Purpose:	Information and Data only have value if they are Fit for Purpose and used to achieve desired outcomes.

The purpose of this policy is to:

- Define how Island Health manages Information and Data across the organization and throughout its Lifecycle to ensure it is Fit-for-Purpose, understandable, and available to meet the organization's business, accountability, transparency, legal, ethical, Risk and regulatory obligations.
- Facilitate compliance with the BC Freedom of Information and Protection of Privacy Act (FIPPA) and regulations, and the BC Information Management Act.
- To meet Accreditation Standards[1]:

  11. Information management policies and systems meet current information needs, take into consideration future information needs, and enhance organizational performance.

  11.5 The organization's leaders manage access to and support and facilitate the flow of clinical and administrative information throughout the organization, to the governing body, across departments, sites, or regional boundaries, and to external partners and the community.

  11.7 The quality and usefulness of the organization's information are regularly assessed, and the assessment results are used to improve the information systems.

Scope:	

- Applies to all Information and Data in the Custody and/or Control of Island Health at any given time, whether in verbal, paper, film or any of the range of electronic forms including audio, video, SMS text message, email, images, scanned (imaged) documents, analog, digital and qubit forms of Data encoding.
- Applies to all Staff and Medical Staff.

Note: capitalized terms can be found in Section 3.0 Definitions

1.0   Policy

1.1 Governance

- Island Health Information and Data will be managed with an organization-wide approach, throughout its Lifecycle, so it is Fit for Purpose, available to contribute to the realization of strategic and operational goals, and Handled in a manner that is transparent and promotes confidence amongst its various stakeholders.
- Information and Data will be managed in accordance with the Island Health Information Governance Framework.
- All Information and Data should be associated with a designated Information Steward.

---

[1] Leadership Standards for Small, Community-based Organizations. March 31, 2016 Ver.11. page 51 Accreditation Canada Qmentum

Maintained by:	Information Governance Council					
Issuing Authority:	Vice President Strategy & Chief Information Officer					
Last Revised:	2021-APR-15	Last Reviewed:	2021-APR-09	First Issued:	2009-MAR-12	Page 1 of 12

1.2 Access and Use Privileges
- Access to and use of Information and Data is a privilege and not a right.
- Staff and Medical Staff will be provided with timely access to Information and Data that is necessary and required to legitimately carry out their Permitted Work Purposes, while abiding by the principles of 'Need to Know' and 'Least Privilege'.
- Researchers and third parties who have been authorized to receive Island Health Information and Data will be provided access to the authorized Information and Data in a timely and secure manner.

1.3 Quality
- Information and Data will be monitored for Quality across its Lifecycle.
- Information and Data Quality and Quality assurance processes will be documented and auditable.
- Persons using Information and Data will ensure it is of sufficient Quality for the purposes for which it is used.
- Information and Data anomalies, inaccuracies or errors will be reported in a standardized manner to the person responsible for the Information or Data.

1.4 Classification – for Information Sensitivity
- Information and Data will be classified and Handled according to Information sensitivity Standards and Classification policy.

1.5 Compliance
- Information and Data will be Handled in compliance with applicable laws, regulations, Standards and organizational policies.

1.6 Protection
- Information and Data and the Systems within which they reside will be categorized, inventoried and regularly updated to support organizational awareness of and accountability for all such assets.
- Any collection of Information and Data containing Personal Information will be registered as a Personal Information Bank (PIB) and all PIBs will have an identified Information Steward.
- Information and Data will be secured with the appropriate levels of protection from breach, corruption and loss (recognizing the challenge posed by rapidly changing technology).
- Supporting policies and procedures, setting out specific direction and guidance, will be in place to ensure the appropriate Handling and security of Information and Data throughout its Lifecycle.
- The Canadian Standards Association Model Code for the Protection of Personal Information, along with relevant legislation, regulatory guidance and case law will provide further guidance to procedure development appropriate to the Sensitivity level and Information Management (IM) activity.

1.7 Metadata
- Information and Data will be understood by a common vocabulary, approved definitions, and Metadata;
- Information and Data will be supported by documented descriptions, definitions, calculations, lineage, flow, Data Quality profiles and cautions, and location(s).

Maintained by:	Information Governance Council				
Issuing Authority:	Vice President Strategy & Chief Information Officer				
Last Revised:	2021-APR-15	Last Reviewed:	2021-APR-09	First Issued:	2009-MAR-12

Page 2 of 12

1.8 Standards
- Information and Data will be Handled in alignment with federal, provincial, and local Information and Data Standards.

1.9 Source of Truth
- There should be identified Sources of Truth or Systems of Record for Information and Data used for making decisions.

1.10 Technology
- Information and Data will be enabled and enhanced by efficient, effective, legally compliant Information architectures, technologies, and procurement and usage processes.

1.11 Issue Resolution
- Governance, management and use of Information and Data will be enabled with clearly defined and consistent issue resolution processes.

1.12 Communication
- Governance, management, and use of Information and Data will be enabled by communication of: what is available; where it can be found; how it can be accessed; as well as relevant policies, procedures, Standards, processes and resources.

1.13 Accountabilities and Responsibilities (with respect to this policy)

Chief Information Officer (CIO)	The CIO is responsible for the overall operational management of Enterprise Information, Access & Privacy, and Information Systems. The CIO will allocate and manage all physical, human and financial resources for the introduction and sustainment of Information Management and Information technology, anticipating future changes that will affect service delivery.[2] The CIO is accountable for this policy, and may delegate responsibilities for its implementation and monitoring.
Chief Technology Officer (CTO)	The CTO is responsible for: the overall management and evolution of the regional, integrated technology infrastructure; the strategic vision and operational framework for provision of secure technologies and services; and for planning, allocation and management of all physical, human and financial resources for the introduction, sustainment and support of Information technology infrastructure.[3] The CTO has responsibility for implementing this policy.
Information Governance (IG) body	An IG body may be delegated by the CIO to fulfill an IG role as described in that body's terms of reference, including establishing policies, procedures, processes, Standards, accountabilities and responsibilities, to ensure compliance with the IG Framework and IG policies.

---

[2] Chief Information Officer job description – excerpted from role summary.
[3] Executive Director Technology Innovation and Client Services job description – excerpted from role summary.

Maintained by:	Information Governance Council					
Issuing Authority:	Vice President Strategy & Chief Information Officer					
Last Revised:	2021-APR-15	Last Reviewed:	2021-APR-09	First Issued:	2009-MAR-12	Page 3 of 12

Template V02 | This material has been prepared solely for use at Island Health. Island Health accepts no responsibility for use of this material by any person or organization not associated with Island Health. A printed copy of this document may not reflect the current, electronic version on the Island Health Intranet.

Executive Leadership	Executive leadership has responsibility to champion IG and IM, and to promote compliance with the Island Health IG Framework and Island Health IG and IM policies.
Information Stewards	Information Stewards have responsibility to take care of organizational Information and Data that reside in their business area(s) and/or to which they have been designated Information Steward. Taking care of Information and Data includes and is not limited to monitoring and improving Data Quality, protecting privacy, and overseeing appropriate Handling. Information Stewards are responsible to ensure the implementation and application this policy. See Appendix A for the full list of Information Steward responsibilities. An Information Steward is a designated Island Health program leader who is assigned responsibility to take care of the Information and Data within the scope of their organizational role. These individuals are typically at a Director, or higher, organizational level.
Technical Stewards	Technical Stewards have responsibility to manage and steward the technology or Systems that holds the Information and Data.
Privacy lead	The Privacy lead has responsibility to promote and influence the responsible, transparent and lawful stewardship and Handling of Information and Data. The Privacy lead provides advice, oversight, education, compliance monitoring, Risk assessment and management of Island Health Information and Data Access and privacy protection practices, policies, procedures, processes and Standards in compliance with related legislation and regulations.
Information and Data Managers	Information/Data Managers have responsibility to implement and apply this policy as delegated by their supervisors and Information Stewards.
Information and Data Users	Information and Data Users have responsibility to comply with this policy.

2.0   Monitoring and Evaluation

Program Directors/Information Stewards will monitor compliance with this policy in their respective areas, and report opportunities for improvement to the IG body.

The IG body will develop and monitor key performance metrics for this policy. The metrics can be found on the Information Governance intranet pages.

Maintained by:	Information Governance Council					
Issuing Authority:	Vice President Strategy & Chief Information Officer					
Last Revised:	2021-APR-15	Last Reviewed:	2021-APR-09	First Issued:	2009-MAR-12	Page 4 of 12

Template V02 | This material has been prepared solely for use at Island Health. Island Health accepts no responsibility for use of this material by any person or organization not associated with Island Health. A printed copy of this document may not reflect the current, electronic version on the Island Health Intranet.

3.0   Definitions (for the purposes of this policy)

Access
'Access' means the ability or opportunity to view, study or obtain a copy the Data or Information. (Source: BC FOIPPA Policy & Procedures Manual, accessed 14Sep2020)

Accountability
The condition wherein, there is answerability to senior staff (or body), and that the senior staff (or body) ensures the task or function will be completed. (Source: Island Health Policy Framework).

Classification
Classification for Information Sensitivity is a system for determining the sensitivity of personal and health Information and for establishing priorities for Information security and privacy protection. (Source: COACH: Canada's Health Informatics Association (2014). Privacy & Security for Patient Portals, 2014 Guidelines for the Protection of Health Information, Special Edition. Toronto, Ontario: National Office. p. 95)

Control
Control of Data or Information means the power or authority to manage the record throughout its Lifecycle, including restricting, regulating and administering its use or Disclosure. (Source: BC FOIPPA Policy & Procedures Manual, accessed 14Sep2020)

Custody
Custody of Data or Information means having physical possession of a record, even though the public body does not necessarily have responsibility for the record. Physical possession includes responsibility for Access, managing, maintaining, preserving, disposing, and providing security. (Source: BC FOIPPA Policy & Procedures Manual, accessed 14Sep2020)

Data
An individual fact (datum) or multiple facts (Data) or a value, or set of values, that is not significant in and of itself. Data is the raw material stored in a structured manner that, given context, turns into Information. Data includes numbers, text, images and sounds, which are created, generated, sent, communicated, received by and/or stored. Data does not include hardware, platforms, software, applications or middleware.

Decision Rights
'Decision Rights' means cataloging critical decisions and documenting who will ultimately be accountable for the decisions that are made.

Delegate
'Delegate' is the act of committing or entrusting authority to an agent or deputy. (Source: BC FOIPPA Policy & Procedures Manual, accessed 14Sep2020)

Disclose
'Disclose' or 'disclosure' means to reveal, show, expose, provide copies of, sell, give or tell (personal or non-personal Information or records). (Source: BC FOIPPA Policy & Procedures Manual, accessed 14Sep2020)

Fit for Purpose
Appropriate, and of a necessary Standard, for its intended uses. (Source: https://en.wiktionary.org/wiki/fit_for_purpose)

Governance
Governance is: defining accountabilities, responsibilities and decision rights; establishing policy; defining processes; and monitoring performance. (Source: The Data Warehouse Institute – Data Quality Fundamentals)

Handle/Handling Information	Any act, activity, operation or operations performed on Information including accessing, viewing, searching for, collecting, creating, obtaining, receiving, organizing, structuring, adapting, altering (e.g. anonymization, pseudonymization), using, applying, sharing, disclosing, retaining, storing, deleting, disposing of, discarding, transmitting, disseminating, copying, exporting, transferring, combining, or in any other way engaging with or processing Information. (Sources: Island Health Confidential Information Management Code of Practice Policy, and ISO/IEC 29100:2011,2.23)
Information	Data that have been recorded, classified, organized, related, synthesized, derived, or interpreted within a framework so that meaning emerges. Information remains Information regardless of storage medium (e.g. paper, CD, electronic System, Cloud) and regardless of form (e.g. text, voice, video Data). Metadata is a subset of Information.
Information Governance (IG)	Information Governance (IG) realizes the value of Information and Data assets by: defining accountabilities, responsibilities and decision rights; establishing policy; defining processes; and monitoring performance; related to managing Information and Data throughout its Lifecycle. IG promotes objectivity through robust, repeatable processes insulated from individual, organizational, political, or other biases. (Source: Island Health IG Framework)
Information Management (IM)	Information Management (IM) embraces all the generic concepts of management, including the planning, organizing, structuring, processing, controlling, evaluation and reporting of Information activities. It concerns Information and Data across its Lifecycle. The Lifecycle of Information and Data involves a variety of stakeholders, including those who are responsible for assuring the Quality, accessibility, protection, and utility of Information and Data and those who need it for providing care and making decisions. (modified from: Wikipedia – Information Management accessed 14Sep2020)
Least Privilege	A security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error or unauthorized use. (Source: BC Core Policy & Procedure Manual chapter 12 definitions)
Lifecycle	The Lifecycle is the sequence of stages that a particular unit of Information or Data goes through from its initial generation or capture to its eventual archival and/or deletion at the end of its useful life. • Planning • Collection, capture, receipt • Organization • Access, use, disclosure • Maintenance, retention and protection • Disposition, destruction • Evaluation (Source: The Canadian Health Information Management Lifecycle ©CHIMA 2016)
Medical Staff	The physicians, dentists, midwives and nurse practitioners who have been appointed to the medical staff, and who hold a permit to practice medicine, dentistry, midwifery, or nursing as a nurse practitioner in the facilities and programs operated by the Vancouver Island Health Authority. (Source: Island Health Policy Framework)

Metadata	Metadata is Information about Information or Data. There are many kinds of Metadata: • Descriptive metadata is Information about a Information or Data resource. It is used for discovery and identification. It includes elements such as title, abstract, author, and keywords. • Structural metadata is Information about containers of Information or Data, and indicates how compound objects are put together, for example, how pages are ordered to form chapters. It describes the types, versions, relationships and other characteristics of digital materials. • Administrative metadata is Information to help manage a resource, like resource type, permissions, and when and how it was created. • Reference metadata is Information about the contents and Quality of Information or Data. • Statistical metadata, also called process Information or Data, may describe processes that collect, process, or produce Information and Data. (Source: modified from Wikipedia – Metadata accessed 14Sep2020)
Need to Know	A privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office. (Source: BC Core Policy & Procedure Manual chapter 12 definitions)
Permitted Work Purpose	Duties, activities and responsibilities that are ethically and legally permitted at Island Health to support day-to-day care, service, clinical governance, organizational governance, Quality improvement, service planning, research, evaluation and communication needs and that are explicitly identified, or directly related to those explicitly identified, in the individual's job or position description, or pursuant to a legal agreement, and, as required, as directed by the individual's Accountable Person. Specific permitted purposes are set out in Island Health's "Patient, Client and Resident" and "Employee" Notices, and are collectively called "a Permitted Care or Service Activity" of Island Health. (Source: Island Health Confidential Information Management Code of Practice Policy)
Personal Information	Verbal or recorded Information in any form about an identifiable individual, other than business contact Information, including, but not limited to: • The individual's name, address or telephone number, • The individual's race, national or ethnic origin, colour, or religious or political beliefs or associations, • The individual's age, sex, sexual orientation, marital status or family status, • Identifying number, symbol, image, audio recording or other particular assigned to the individual, • The individual's fingerprints, blood type or inheritable characteristics, • Information about the individual's health care history, including a physical or mental disability, • Information about the individual's education, financial, criminal or employment history, • Anyone else's opinions about the individual, and • The individual's personal views or opinions, except if they are about someone else; (Source: Island HealthConfidential Information Privacy Rights of Personal Information Policy, and Confidential Information Management Code of Practice Policy)

Maintained by:	Information Governance Council
Issuing Authority:	Vice President Strategy & Chief Information Officer

Personal Information Bank (PIB)	Any collection of records containing Personal Information, that is organized or retrievable by a name or an identifier, and is searchable or indexed, as required under the BC Freedom of Information and Protection of Privacy Act, [RSBC 1996].
Quality	Information and Data are regarded as high Quality if they are well suited to the purposes for which the Information or Data are needed. Suitability of purpose must consider all of the purposes for which the Data are used, ranging from business transactions and operational reporting, to business intelligence and analytics. Quality criteria will vary among the different uses.
Record	'Record' includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which Information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records. (Source: BC Freedom of Information and Protection of Privacy Act, [RSBC 1996]. Accessed 14Sep2020)
Responsible	Obligation to perform a particular task; one is responsible for the actual carrying out of the task or function. (Source: Island Health Policy Framework)
Risk	An uncertainty affecting planned goals or objectives. The occurrence of risk could interfere with the ability to meet our annual goals or deliverables (Source: Island Health Risk Management Glossary https://intranet.viha.ca/departments/risk_management/Documents/risk-management-glossary.pdf)
Sensitivity of Information	Is related to the potential for harm or stigma that might attach to the identification of an individual because of the nature of the Information exposed about that individual. Sensitivity can range from very low to extremely high depending on the type of Information and the context of its use or sharing - either alone or in combination with other Information. Information considered to be sensitive includes sexual attitudes, practices and orientation; use of alcohol, drugs or other addictive substances; illegal activities, suicide, sexual abuse, sexual harassment; an individual's psychological well-being or mental health; types of genetic Information (e.g., Information that predicts future illness or disability and raises concerns around future employability or insurability); certain financial Information such as Social Insurance number and any other Information that might lead to social stigmatization, discrimination, threats or blackmail of an individual. (Source: COACH: Canada's Health Informatics Association (2014). *Privacy & Security for Patient Portals, 2014 Guidelines for the Protection of Health Information, Special Edition*. Toronto, Ontario: National Office. p. 106)

Maintained by:	Information Governance Council					
Issuing Authority:	Vice President Strategy & Chief Information Officer					
Last Revised:	2021-APR-15	Last Reviewed:	2021-APR-09	First Issued:	2009-MAR-12	Page 8 of 12

Template V02 | This material has been prepared solely for use at Island Health. Island Health accepts no responsibility for use of this material by any person or organization not associated with Island Health. A printed copy of this document may not reflect the current, electronic version on the Island Health Intranet.

Source of Truth	A trusted and identified Information or Data source that gives a complete picture of the Information or Data object as a whole. (Source: Island Health IG Framework)
	Also note Island Health's Health Records Policy and the definition of 'Original Record'. Original Record: means the first complete record capable of reaching the purposes for which it was intended (i.e., "effective"). An Original Record has three characteristics: primitiveness (i.e., the first to be generated); completeness; and effectiveness. Please note, a draft document is not considered an Original Record as it is not considered complete nor to have effectiveness (i.e., it is not capable of reaching the intended purpose). For example, a dictated report is not considered an original but a draft whereas the transcribed and signed report which is uploaded to PowerChart is considered the Original Record. The Original Record in Health Care is typically also referred to as the "Source of Truth" record.
Staff	For the purpose of policy, 'Staff' refers to all employees (including management and leadership), health care professionals, students, volunteers, contractors, and other service providers. (Source: Island Health Policy Framework)
Standards	Standards are a formula that describes the best way of doing something. It could be about making a product, managing a process, delivering a service or supplying materials – standards cover a huge range of activities. Standards are the distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent – people such as manufacturers, sellers, buyers, customers, trade associations, users or regulators. (https://www.iso.org/Standards.html)
System (Information System)	'System' refers to any electronic device or equipment used to support the electronic storage, transfer, or access of information. (Source: Island Health Acceptable Use of Assets and Resources Policy)
System of Record	The identified authoritative source for a given Data element or piece of Information; the repository where the Data element or piece of Information, as a whole or specific attributes, is created, updated, modified and deleted. (Source: Island Health IG Framework)

4.0   Related Island Health Policies

- Island Health Policy 1.5.1: Confidential Information - Privacy Rights of Personal Information
- Island Health Policy 1.5.2: Confidential Information-Third Party, VIHA Business and other Non-Personal Information
- Island Health Policy 1.5.3 Release of Patient Information to Law Enforcement
- Island Health Policy 1.5.4 Privacy and Related Information Security Breaches: Reporting and Investigation Management.
- Island Health Policy 16.2.1 Health Records
- Island Health Policy 16.4.2.1: Security of Electronic Information
- Island Health Policy 16.4.2.2: Security of Health Records
- Island Health Policy 16.4.2.3: Acceptable Use of Assets and Resources
- Island Health Policy 16.4.2.4 Remote Access
- Island Health Policy 16.4.2.5 Mobile Computing
- Island Health Policy 16.4.2.6 Remote Assistance and Session Sharing for Support Purposes

Maintained by:	Information Governance Council					
Issuing Authority:	Vice President Strategy & Chief Information Officer					
Last Revised:	2021-APR-15	Last Reviewed:	2021-APR-09	First Issued:	2009-MAR-12	Page 9 of 12

Template V02 | This material has been prepared solely for use at Island Health. Island Health accepts no responsibility for use of this material by any person or organization not associated with Island Health. A printed copy of this document may not reflect the current, electronic version on the Island Health Intranet.

- Island Health Policy 16.6.1 Photography and Recording by Staff and Physicians
- Island Health Policy 16.6.2: Confidential Information Management Code of Practice
- Island Health Policy 16.6.6 Recording (photographing, videotaping or audio recording) by Clients and Visitors
- Island Health Procedure 1.5.4 Privacy and Information Security Breaches Information Breaches: Risk Assessment
- Island Health Policy 19.1 Service Contract Management

5.0   References

- Accreditation Canada Required Organizational Practices (ROP) Handbook Version 14
    https://intranet.viha.ca/departments/quality/Accreditation/Documents/2019%20ROPs%20and%20Standards/2019%20ROP%20Handbook.pdf
- BC Core Policy & Procedures Manual Policy Chapter 12: Information Management and Information Technology Management
    https://www2.gov.bc.ca/gov/content/governments/policies-for-government/core-policy/policies/im-it-management/
- BC Freedom of Information and Protection of Privacy Act (FIPPA)
    https://www.bclaws.gov.bc.ca/civix/document/id/consol26/consol26/96165_00
- BC Information Management Act
    https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/15027
- FIPPA Policy & Procedures Manual
    https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual/policy-definitions
- Island Health Information Governance Framework
    https://intranet.viha.ca/departments/decision-support/Documents/ig-framework.pdf
- Island Health Policy Framework   https://intranet.viha.ca/pnp/Documents/island-health-policy-framework.pdf
- Island Health Risk Management Glossary
    https://intranet.viha.ca/departments/risk_management/Documents/risk-management-glossary.pdf

6.0   Resources

- InfoGovernance@viha.ca
- Information Governance intranet pages
    https://intranet.viha.ca/departments/decision-support/Pages/information-governance.aspx
- BC Information Management & Technology resources
    https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology
- Information Stewardship, Access and Privacy program
    https://intranet.viha.ca/departments/privacy/Pages/default.aspx
- Information Steward Toolkit
    https://intranet.viha.ca/departments/privacy/Pages/Information_Steward_Resources.aspx
- Information Steward learning module
    https://intranet.viha.ca/departments/privacy/Pages/Information_Steward_Resources.aspx

Maintained by:	Information Governance Council					
Issuing Authority:	Vice President Strategy & Chief Information Officer					
Last Revised:	2021-APR-15	Last Reviewed:	2021-APR-09	First Issued:	2009-MAR-12	Page 10 of 12

Template V02 | This material has been prepared solely for use at Island Health. Island Health accepts no responsibility for use of this material by any person or organization not associated with Island Health. A printed copy of this document may not reflect the current, electronic version on the Island Health Intranet.

Appendix A: Information Steward Responsibilities[4]

Information Stewards are responsible for the following, as may be amended from time to time:

1	Governance and Shared Stewardship	• Understanding and defining the scope of Information and Data for which they are an Information Steward. • Collaborating to define the extent of their stewardship at each stage of the Information Lifecycle. • Collaborating to define how stewardship will be handled when Accountabilities are shared or transferred, especially as Information and Data moves through the Lifecycle and from System to System. • Understanding that Information and Data are organizational assets that require management and are not owned by a department or program. • Ensuring that the Information and Data needs of their own program/business are identified, communicated, and where the Information and Data are available, fulfilled. • Ensuring future and downstream user needs are considered when making decisions about the Information and Data. • Ensuring downtime procedures are in place as appropriate.
2	Access and Use	• Ensuring Information and Data are available for authorized users. • Ensuring Risk-proportionate processes and procedures are in place to appropriately control access to Information and Data. • Facilitating understanding and appropriate interpretation of Information and Data. • Adjudicating requests to Access and use Information and Data. • Enabling lawful Access to Personal Information in response to formal requests under FIPPA.
3	Quality	• Ensuring the Information and Data is of sufficient Quality for the need at each stage of the Information and Data Lifecycle. • Ensuring effective controls over Information and Data collection and recording processes. • Ensuring Information and Data remain of appropriate Quality after it has been entered into Systems, through periodic or routine monitoring and testing. • Ensuring controls are in place to monitor the completeness and accuracy of Information and Data as it flows from one System to another. • Ensuring Information and Data Quality processes are documented.
4	Classification	• Classifying the Information and Data they steward in compliance with organizational policies and Standards.
5	Compliance	• Complying with federal, provincial and health authority legislation, regulations, and policies, relevant to Information and Data. • Ensuring Handling of Information and Data, including by authorized service providers or vendors, occurs in compliance with privacy and security policies, legislation, and with the appropriate third party contractual controls in place. • Registering Personal Information Banks (PIBs) in accordance with organizational policy and procedure. • Initiating and completing, in collaboration with the privacy office, Privacy Impact Assessments (PIAs) as required by law and organizational policy.

---

[4] Except for Classification, Technology and Communication, these accountabilities were developed and approved by the Information Governance Council's working group on Information Stewards in 2019. The categories used by the working group have been re-labeled to align with the categories in this policy and the IG Framework principles.

Maintained by:	Information Governance Council				
Issuing Authority:	Vice President Strategy & Chief Information Officer				
Last Revised:	2021-APR-15	Last Reviewed:	2021-APR-09	First Issued:	2009-MAR-12	Page 11 of 12

6	Protection	• Protecting the Information and Data they steward in compliance with organizational policies and Standards. • Supporting staff to fulfill privacy and security training requirements and uphold their privacy and security obligations, including participating as required in the investigation, management, and prevention of privacy breach incidents. • Establishing the appropriate contractual controls and/or agreements with third party service providers and vendors. • Understanding and addressing Risks identified in PIAs provided by the privacy office. • Understanding and addressing Risks identified in Security Threat Risk Assessments (STRAs) provide by the Information security office.
7	Metadata	• Documenting and communicating up-to-date descriptions, definitions, calculations, lineage, flow, Data Quality profiles, and locations of Information and Data to facilitate meaningful interpretation and use.
8	Standards	• Ensuring compliance with Island Health, provincial, and national Standards for capture, collection, definition, calculation, and reporting of Information and Data.
9	Technology	• Ensuring Information technologies used in their business area are compliant with Island Health Standards, policies and procedures.
10	Communication	• Communicating metadata, and changes to the Information and Data they steward, to users and to administrators of downstream Systems.