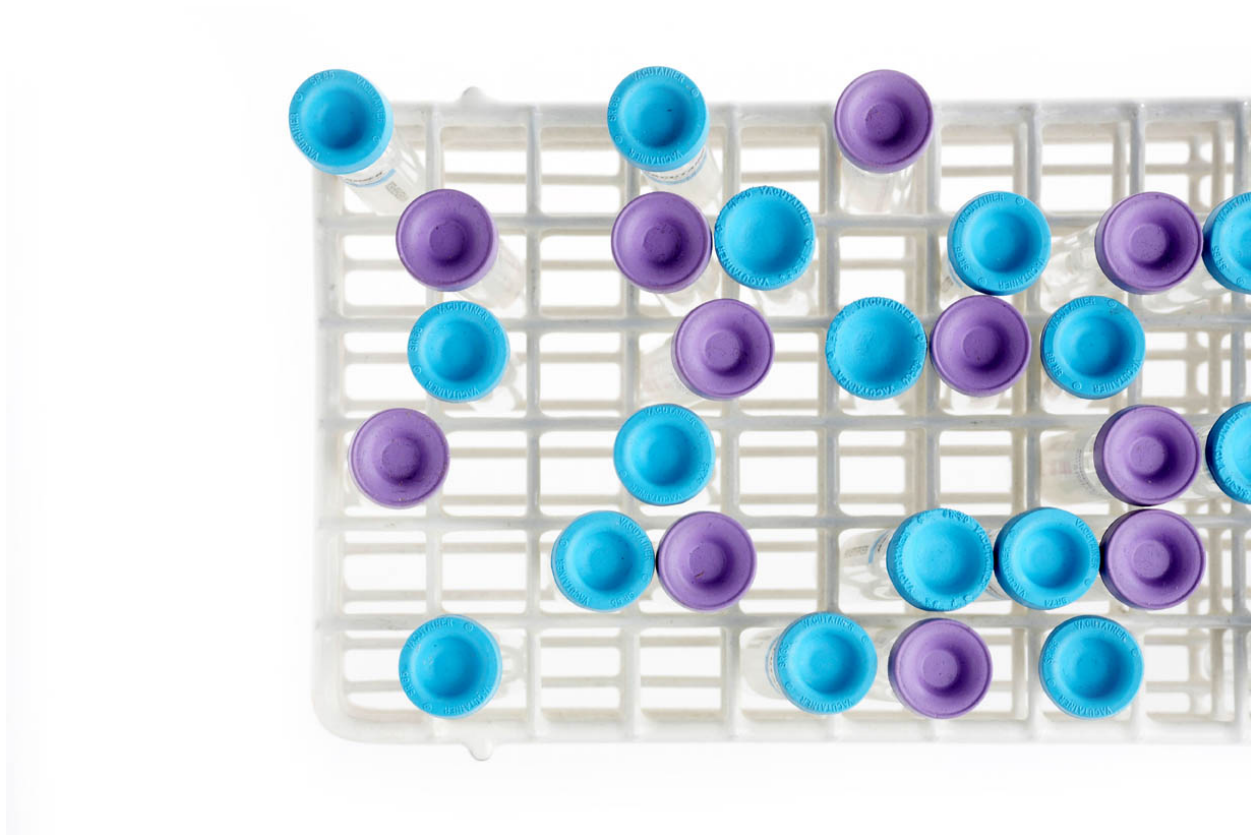


Ministry of Health

Security enhancement roadmap



June 25, 2013

Table of contents

Enhancement roadmap overview	1
Introduction	1
Objectives and scope	1
Approach	2
Summary of recommended enhancement opportunities	2
Next steps	4
Appendix A – Project summaries	5

Enhancement roadmap overview

Introduction

In May, 2012 the Ministry of Health (MoH or the Ministry) initiated an investigation related to contracting irregularities and inappropriate research grant processes. One component of this investigation involved reviewing data management practices of ministry employees, researchers and contractors. The investigation is still underway.

In September, 2012 the Ministry engaged Deloitte to support it in developing a roadmap to enhance data management practices, specifically with respect to security and privacy. This work was conducted independent of any investigation the Ministry may have been carrying out. This work did not constitute an audit or assessment. Rather, the purpose of this project was to highlight opportunities for improvement with respect to data management across the Ministry, with a focus on the security and privacy of health information, and to build these opportunities into a forward-looking roadmap. This roadmap will enable the Ministry to prioritize and implement enhancement projects to support improved control over health-related information.

This document provides an overview of the objectives of this work, describes the high-level scope and approach, and then summarizes the recommended enhancement opportunities included in the roadmap.

Objectives and scope

The objectives of this engagement were to work with MoH to:

1. Understand, at a high level, current processes related to information use and sharing across the Ministry
2. Conduct an inventory of key data sources and flows within the Ministry
3. Identify opportunities for improvement of information management for health information across the Ministry based on accepted standards (with a focus on security and privacy)
4. Based on the above, develop a series of recommendations in the form of an “enhancement roadmap” outlining enhancement opportunities related to business processes, controls and technology where appropriate

As noted above, the Ministry was interested in understanding opportunities for improvement for the organization as a whole. Due to the scale and complexity of the Ministry and the volume of information it collects, manages and shares, the project was scoped to provide a broad view across the Ministry rather than conducting a detailed and exhaustive assessment of one area, system or set of systems. Additional information regarding the scope of the project is summarized in Table 1 below.

Table 1 - Summary of scope by scope element

Scope element	In-scope description
Types of information	Personal health information, with a focus on secondary uses.
Processes	Selection of current state processes related to: • Access • Use • Disclosure • Security • Privacy • Logging and monitoring
Organization	Ministry of Health, with a primary focus on Divisions that manage, store and disclose personal health information

Approach

A phased approach to the project was undertaken in order to ensure that recommendations were based on an understanding of the current state. The key phases in the project are outlined in Figure 1 below.



Figure 1 - Summary of phased approach

Initially, an understanding of the current state was obtained through interviews and review of relevant documentation to identify opportunities for improvement. Standard frameworks (Generally Accepted Privacy Principles (GAPP) for privacy-related risks and ISO 27001 for technology-related risks) were inputs used as a basis for establishing the scope of this work. Based on this, a series of recommendations was developed and these were then structured into a number of projects designed to address these recommendations. These projects were validated with Ministry subject matter experts, and an initial estimate of effort and required skill sets was developed in order to support preliminary planning. These projects were then incorporated into a high-level enhancement roadmap. This preliminary roadmap is intended to support the Ministry as it delivers these projects (for those that are underway) and as it embarks on detailed project planning, phasing and execution for those that are not yet started.

Summary of recommended enhancement opportunities

Based on the recommendations, a series of projects was developed. These projects (summarized in Table 2, below) were recommended to support the consistent enhancement of business process and technical controls related to personal health information across the Ministry. Additional details regarding these projects are provided in “Appendix A – Project Summaries”.

Table 2- Summary of project categories, recommendations and projects.

#	Categories	Recommendations	Projects
1	Information Governance	Develop and implement a formal information governance program	1.1 Enhance components of Governance model
2	Data Management	Enhance data management practices and consider changes to the technology environment to support a consistent level of control over sensitive information	2.1 Complete information inventory 2.2 Develop and implement a secure data environment
3	Transition Condor Environment	Transition the Condor environment to new infrastructure and updated applications, with consideration for key functional, security and privacy requirements	3.1 Actions to mitigate risk in specific legacy systems 3.2 New data warehouse design, implementation & data migration 3.3 Web application environment design, implementation & transition 3.4 SAS enterprise environment design, implementation & transition plan
4	Education & Awareness Program	Develop and implement a formal, mandatory and targeted training and awareness program for information governance, security and privacy	4.1 Deliver immediate training to key staff and supervisors across the Ministry 4.2 Develop an enhanced training and awareness program
5	Access Management & Administration	Enhance and standardize internal processes across the Ministry for management and administration of access to health information	5.1 Enhance approval & granting process 5.2 Enhance transfers process 5.3 Enhance terminations process 5.4 Enhance access review process 5.5 Enable a role-based access approach
6	Information Sharing Agreements	Centrally coordinate and streamline information sharing agreements and related data access processes	6.1 Update inventory of existing information sharing agreements 6.2 Create a centralized repository of existing agreements 6.3 Standardize processes and templates for information sharing agreements
7	Logging & Monitoring	Enhance logging and monitoring practices and capabilities across key systems	7.1 Evaluate existing logging capabilities and enable or enhance where appropriate 7.2 Design and implement a logging solution to support the long-term secure analysis environment
8	Security Management Practices	Enhance IT operational practices for maintaining a secure technology environment	8.1 Consolidate additional enhancement opportunities and address them on a priority basis 8.2 Define the Security Management role responsible for the secure data environment 8.3 Develop and maintain security reference architecture
9	Policies & Standards	Develop key Ministry-specific policies and guidelines.	9.1 Develop a ministry-specific privacy policy 9.2 Develop Ministry-specific guidance for key topics
10	Compliance Monitoring	Implement a compliance-monitoring function to regularly assess compliance against Ministry and third-party requirements with respect to data.	10.1. Implement an enhanced compliance monitoring function

Next steps

The Ministry is in the process of implementing these recommendations.

Appendix A – Project summaries

This appendix contains project summaries for each of the 25 projects included in the enhancement roadmap. These projects are organized into the 10 Project Categories. For each of the 25 projects, a project purpose is provided and this is followed by guidance that is intended to describe the desired outcomes and/or key considerations for each of the initiatives.

1. Information governance

Project overview

Project purpose Develop and implement a formal information governance¹ program.

1.1. Enhance Components of Governance model

Sub-project purpose	The purpose of this project is to enhance components of the existing governance model at the Ministry, in order to provide clarity regarding accountabilities and decision-making processes related to information across the Ministry in the short term. This will enable the development of a longer-term governance model while also supporting critical short-term decision-making related to information governance and technology issues as the longer-term model is developed.
----------------------------	---

Guidance	• Discussions with all of the divisions should be facilitated to discuss the information governance model and to identify the key principles for its development. • The development and implementation of the information governance model should be a shared responsibility across all of the divisions. • Establish Senior Leadership buy-in for a formal Information Governance program. This will include defining an Executive Sponsor and clearly defining, communicating and gaining consensus on: – The scope and mandate of the program (Charter) – The key issues it is meant to address (in terms of risk management and value creation) • Once executive support is obtained (and the proposed model adjusted as required based on input), define the foundational components of the program, including: – Agreed-upon information governance principles (based upon regulatory and contractual obligations with respect to information management and information sharing) – Roles, responsibilities and accountabilities, with a focus on key roles in the short term, potentially including: • Data Stewards • Data Owners • Data Custodians • Data Users – Key structures and associated mandates (Executive Committee, Working Committee, etc.) – Key processes to support the operation of the governance model • Leverage historical efforts related to information governance within the Ministry, with a focus on identifying key governance components to be incorporated into the short-term model.
-----------------	---

¹ There are numerous definitions for information governance. These definitions typically refer to the decision rights, processes, standards, technologies and roles and responsibilities required to manage, maintain and effectively use information in a manner that aligns with security and privacy requirements.

- Once the enhanced model is agreed-upon and established, regular assessment of performance, effectiveness and opportunities for improvement should be conducted to ensure it is meeting the agreed-upon objectives defined by stakeholders
-

2. Data management

Project overview

Project purpose Enhance data management practices and consider changes to the technology environment to support a consistent level of control over sensitive information.

2.1 Complete Information Inventory

Project purpose This project will build upon recent efforts to develop an inventory of information assets and data flows, with the objective of creating a regularly updated repository for the Ministry. This project also involves reviewing this inventory to identify those dataset extracts and other sensitive information assets that can be archived or deleted.

Guidance

- Define roles and responsibilities for the maintenance of the inventory (to include representation from Divisions and HSIMIT).
- Consider working with SSBC to generate inventories of dataset extracts within each division.
- Assign ownership for updating of inventories to division representatives, and where appropriate, update as required.
- Within each Division, utilize the inventories to identify the location of sensitive information
- Review dataset extracts and other sensitive information assets to identify those to retain vs. those that can be archived. Consider including the following criteria in the review:
 - Are the data still in use?
 - Are the employees with access appropriate?
- Identify opportunities for limiting access to shared LAN folders and remediate where possible.
- Within each Division, identify high-level information sharing needs to inform business requirements for the Secure Data Environment (2.2)
- Document where sensitive information resides and consider options for enhanced logging where appropriate.
- Review of access rights to LAN folders containing sensitive information should be coordinated with the access review performed in Project 5.5.
- Once this exercise is complete, update information asset inventories as required

2.2 Develop and implement a secure data environment

Project purpose The purpose of this project is to design and implement a secure environment that enables access to and sharing of sensitive information while at the same time supporting a consistent level of control over this information across the Ministry. Recognizing that there are numerous options regarding the design of the environment, the selected design should enable access to sensitive information by authorized users while supporting a consistent level of control over this information. It should also support the ability to log and monitor access and usage to enable compliance management.

Guidance

- The design process should take into account the following:
 - Requirements for the secure environment should address the Ministry's agreed-upon information management principles (see Project 1.0 – Information Governance), and existing regulatory and contractual obligations associated with the data currently collected and maintained by the Ministry.
 - Business requirements of key stakeholders across the Ministry (business users and HSIMIT) should be developed, validated and approved through a cross-Ministry team to ensure needs of all stakeholders are understood and addressed.
 - The design of the new environment should align with the overall Enterprise Architecture of the Ministry, as well as requirements outlined in the government Information Security Policy
- The user community should also be involved in the development of the test plans, test scripts and key stages of the testing processes.
- The project plan should also include a process to review and onboard future data sets on an ongoing basis.
- Representatives from each Division should be provided with guidance on relevant data retention standards to enable decisions for archiving vs. deleting.
- A risk-based and prioritized data migration strategy should be developed
- When reviewing data sets for migration, consider including the following criteria:
 - Is the dataset actively in use?
 - Are there defined data retention requirements?
 - Is there an ongoing business need for retaining and migrating the data?

- Is the authority under which the data was originally obtained and used still in place?
 - Are there sufficient controls in place to manage the sensitive information contained within the data set
 - Does the dataset exist elsewhere? If so, consider rationalizing datasets in the new environment if possible.
 - When reviewing the scripts used to generate analysis and reports, the following should be considered:
 - Development of an approach to migrating scripts and data (e.g., move all existing scripts “as-is” or review, update and cleanse prior to migration)
 - Ensure hardcoded references in existing scripts are identified and updated as required
 - Ensure updated scripts are working as expected (testing)
 - Consider removal of intermediary products where possible
 - An archive strategy should be defined for all data sets which will not be transitioned.
 - As soon as practical and once all data sets have been transitioned to the new environment or archived, legacy systems should be decommissioned.
-

3. Transition Condor environment

Project overview

Project purpose Transition the Condor environment to new infrastructure and updated applications, with consideration for key functional, security and privacy requirements.

3.1 Actions to Mitigate risk in specific legacy systems

Project purpose The purpose of this project is to perform specific activities that could reduce the risks within the Condor environment in the short term while the new environment is under development.

Guidance

- A review of data sets should be performed to identify inactive data sets which are no longer in use.
- Access to inactive data sets should be revoked for all users and a process implemented to review and approve all access requests to these data sets.
- A user access review should be performed to ensure only approved users with a business need have access to Condor (Manager to approve access).
- Managers of Condor users should be notified that they are responsible to provide prompt notification of termination or changes of access rights.
- An interim access policy should be developed to ensure only approved users with a defined business need are granted access to Condor.

3.2 New data warehouse design, implementation and data migration

Project purpose The purpose of this project is to design and implement a replacement for the legacy Condor data warehouse environment within the Secure Data Environment (sub-project 2.2) that addresses the security and privacy requirements of the Ministry. This sub-project is likely to be integrated into the development and transition to the new Secure Data Environment (sub-project 2.2) and represents an example of legacy systems that will be transitioned to the new environment. The project will ensure that all required data is transferred to the new environment on a priority basis in a secure manner and that data quality and integrity are retained. Finally, the legacy Condor data warehouse environment will be decommissioned.

Guidance

- The new design should address at a minimum:
 - Role based access²
 - Logging of user access and activity
 - The restriction of downloading of data to local computers
- A risk and controls review should be conducted as part of the design to ensure key security and privacy requirements are addressed.
- The new design should follow all relevant OCIO guidance and should go through the PIA & STRA processes.
- The new design should ensure the solution is robust and scalable enough to meet the current and future business needs of the MoH.
- When reviewing data sets for migration, consider including the following criteria:
 - Is the data set actively in use?
 - Is the appropriate authorization for use of data in place?
 - Is there an ongoing business need for retaining and migrating the data?
 - Does the dataset exist elsewhere? If so, consider avoiding duplication in the new environment if possible
- An agreed-upon priority ordering of data sets for migration should be developed with input from data users and owners.
- An archive strategy should be defined for all data sets which will not be transitioned.
- As soon as practical and once all data sets have been transitioned to the new environment or archived, decommission the legacy Condor environment.

3.3 Web application environment design, implementation & transition³

² Role-based access is a method of managing access to computers or networks. It allows the regulation of access based on the job function (role) of users within an organization. In this context, "access" is the ability of an individual user to perform a specific task, such as view, create, or modify a file. Roles are defined according to job competency, authority, and responsibility within the organization. This approach helps to ensure that users have appropriate access and also supports the efficient administration of access rights.

Project purpose The purpose of this project is to design and implement a replacement for the legacy Condor web applications environment within the Secure Data Environment (sub-project 2.2) that addresses the security and privacy requirements of the Ministry. This sub-project is likely to be integrated into the development and transition to the new Secure Data Environment (sub-project 2.2) and represents an example of legacy systems that will be transitioned to the new environment. The legacy Condor web applications environment will be decommissioned once complete.

Guidance

- The new design should address at a minimum:
 - Role based access
 - Logging of user access and activity
 - The restriction of downloading of data to local computers
- A risk and controls review should be conducted as part of the design to ensure key security and privacy requirements are addressed.
- The new design should follow all relevant OCIO guidance and should go through the PIA & STRA processes.
- The new design should ensure the solution is robust and scalable enough to meet the current and future business needs of the MoH.

3.4 SAS enterprise environment design, implementation & transition plan

Project purpose The purpose of this project is to design and implement a replacement for the legacy Condor SAS⁴ environment within the Secure Data Environment (sub-project 2.2) that addresses the security and privacy requirements of the Ministry. This sub-project is likely to be integrated into the development and transition to the new Secure Data Environment (sub-project 2.2) and represents an example of legacy systems that will be transitioned to the new environment. The project will ensure that all required code and SAS libraries are transferred to the new SAS Enterprise environment on a priority basis. Finally, the legacy Condor SAS environment will be decommissioned.

Guidance

- The new design should address at a minimum:
 - Role based access
 - Logging of user access and activity
 - The restriction of downloading of data to local computers
- A risk and controls review should be conducted as part of the design to ensure key security and privacy requirements are addressed.
- The new design should follow all relevant OCIO guidance and should go through the PIA & STRA processes.
- The new design should ensure the solution is robust and scalable enough to meet the current and future business needs of the MoH.
- Conduct a review of SAS code and libraries for migration and consider including the following criteria:
 - Is the code and/or library actively in use?
 - Does an ongoing business need exist for the code and/or library?
 - Based on the business need, is the effort and cost to migrate to the new environment justified?
 - Is the need addressed by other similar libraries or sets of SAS code?
- A priority ordering of SAS libraries to be transitioned should be developed based on input from key business users and owners.
- An archiving strategy should be defined for all SAS libraries which will not be transitioned.
- A code migration process should be developed to port required legacy SAS code to the new environment.
- As soon as practical and once all SAS libraries have been transitioned to the new environment or archived, decommission the legacy Condor environment.

³ The “web applications environment” allows users to access the analytics component of Condor using a web browser.

⁴ In this instance, “Condor” refers to the environment used for data linkage and analysis and “SAS” refers to a commercial off-the-shelf application used for statistical analysis (among other activities).

4. Education and awareness program

Project overview

Project purpose Develop and implement a formal, mandatory and targeted education and awareness program for information governance, security and privacy.

4.1 Deliver immediate foundational training to key staff and supervisors across the Ministry

Project purpose While the enhanced education and awareness program is in development (Activity 4.2), deliver foundational training to appropriate users across the Ministry.

Guidance

- Training should address key questions and concerns of Ministry staff to ensure staff can perform their duties with an understanding of appropriate information sharing.
- A target list of attendees should be developed.
- Management should be informed of training attendance.
- Training should reference key support material (Policies, procedures, etc.).
- Training should be augmented with FAQs and guidance that address the most common questions received from across the Ministry.
- Key training messages should be reinforced through targeted awareness campaigns (e.g., Intranet site updates, emails, posters, etc.)

4.2 Develop an enhanced education and awareness program

Project purpose The purpose of this project is to develop MoH-specific information management security & privacy education that is tailored to needs of divisions and specific roles, and is mandatory, ongoing & updated and reinforced with periodic sign-off by employees.

Guidance

- A foundational information management security & privacy education course should be mandatory as part of onboarding for all new staff and yearly for all existing staff.
- Graduated education should be developed and delivered to address specific needs of different roles (such as all new staff, executives, advanced data users, etc.)
- Staff with access to sensitive information should have additional mandatory training which details their responsibilities and references appropriate policies & procedures.
- Training should address key information management privacy & security risks associated with each role.
- Consider developing guidance around retention and archiving of information.
- The training and awareness program should be reviewed and revised periodically to ensure continuous improvement and alignment with updated policies, legislation and MoH obligations.
- FAQs and guidance should address common question and be reviewed and revised periodically.
- Annual acknowledgment of training and sign-off on responsibilities should be implemented.
- Subject Matter Experts from each business division should be involved in updating training materials and in training sessions.
- Feedback from sessions should be continuously updated in training materials
- Ad-hoc workshops should be developed based on specific needs of branches, new legislation and incidents.

5. Access management and administration

Project overview

Project purpose Enhance and standardize internal processes across the Ministry for management and administration of access to health information.

5.1 Enhance approval & granting process

Project purpose The purpose of this project is to ensure roles and responsibilities related to access management (request, approvals, etc.) are clearly defined and understood across the ministry (DSAM, Authentication Services, Connections, Divisions, etc.).

Guidance

- Enhance and clearly document access administration procedures to enable consistent decision-making for access requests.
 - Document current informal access decision making criteria for applications and data sets.
 - Over time, move to a role based model with pre-defined access usage roles for each application and groups of data sets.
 - A prioritization process should be defined to address critical or urgent requests in a timely manner.
 - Integration should be improved between the contracting process (for all contracts with a data component) and the access management process
- Roles and responsibilities with respect to access control, including requestors (supervisors & managers), approvers (data & system owners), and provisioning should be defined and communicated.
- Approval process and requirements for approval should align to the type of access requested (e.g., Public vs. Personally Identifiable) in order to expedite low-risk requests and ensure sufficient review of higher-risk requests. For example, consider pre-approval of access requests related to standard, low-risk datasets to streamline the approval process.
- Physical access for guests should be restricted to the area or division they are visiting and approved by an MoH employee.
- The concept of segregation of duties should be considered when granting access to employees, contractors, researchers, etc.
- Options to improve the efficiency and effectiveness of access administration processes should be considered. For example, consider automated workflows and a centralized provisioning solution.

5.2 Enhance transfers process (for access changes)

Project purpose The purpose of this project is to clearly define and communicate roles and responsibilities related to access changes (removals, additions, etc.) to ensure access changes are defined, communicated and implemented in a timely manner and that updates regarding access changes are provided to requestors once completed.

Guidance

- Enhance and clearly document access change procedures.
- Supervisor's and manager's responsibilities and accountability with respect to notification and follow up should be clearly defined (e.g., outlined in their job description). For example, notification of staff role changes should be mandatory from the individual's supervisor or manager.
- The procedures for changes to user access should require that all existing access be removed.
- Granting and approval of access required for new roles should follow the access approval process (Activity 5.1)
- Managers or supervisors should be notified once access updates are completed and a description of the access granted.
- Process changes should be communicated to all supervisors and managers.

5.3 Enhance terminations process

Project purpose The purpose of this project is to implement a clearly defined and communicated process for access termination that ensures that all access is removed in a timely manner and that the appropriate supervisors are updated of access removals once complete.

- Guidance**
- Enhance and clearly document access removal procedures.
 - Notification of staff terminations should be driven either automatically from a system of record (e.g., payroll) or incorporated into the HR terminations process.
 - Managers or supervisors should be notified once access is removed.
-

5.4 Enhance access review process

Project purpose The purpose of this project is to design and implement a process for regular reviews of user access rights to key information systems and data sets across the Ministry. This is a detective control that supports the access change and termination processes (described above) and will serve to ensure that only the appropriate individuals have access to sensitive systems and information.

- Guidance**
- For systems and data sets containing personal health information or other sensitive information, access reviews should be conducted immediately to identify users who should be removed or have excessive access rights.
 - Enhance and clearly document access review procedures.
 - Roles and responsibilities with respect to access reviews, including access management staff (generate & supply access lists), and reviewers (confirm access is appropriate) should be defined and communicated.
 - Review process and frequency should vary depending on sensitivity of the data within systems and the volume of user access changes.
 - Supervisors and managers responsibility with respect to access reviews should be a requirement within their job description.
-

5.5 Enhance role based access approach

Project purpose The purpose of this project is to enhance the current role-based access model to support efficient and effective access administration processes. It includes reviewing and rationalizing current roles in HealthIdeas and, over the long term, enhancing the role-based access model to include other key systems and datasets within the Ministry.

- Guidance**
- HealthIdeas access roles should be reviewed and rationalized. Where possible access roles should be aligned to Ministry job roles and new roles should be created on an exception basis as required.
 - Implementation of role based access should be considered for other key MoH information systems and data sets beyond HealthIdeas.
 - A clear definition of the access granted by each role and the intended job descriptions to be granted each role should be provided to access provisioning staff.
 - Roles and responsibilities with respect to defining and approving roles and handling the exception process for none standard roles should be defined and communicated.
-

6. Information sharing agreements

Project overview

Project purpose Centrally coordinate and streamline information sharing agreement and related data access processes.

6.1 Update inventory of existing information sharing agreements

Project purpose The purpose of this project is to compile an inventory of agreements related to information sharing between the Ministry and third parties. This will provide a single view of Ministry and third-party commitments related to information sharing that could ultimately support MoH and third party monitoring and enforcement.

Guidance

- Appropriate stakeholders should define the type of agreements to be included in the inventory
- Conduct an inventory of the types of agreements determined to be in-scope
- Consider conducting a review of key existing contracts/master agreements to ensure appropriate data sharing provisions are in place.
- Data sharing with third-parties, where a data sharing agreement is not in place, should be identified
- Representatives from each division should identify the agreements within their divisions.

6.2 Create centralized repository of existing agreements

Project purpose This project involves the creation of a central repository of Ministry agreements with respect to information sharing with third parties. This will provide one central inventory of such agreements and enable employees responsible for releasing information to access data sharing agreements to determine what is appropriate for release.

Guidance

- One central repository should be created for all agreements that provides a single view of the Ministry's commitments with respect to data sharing with third parties.
- Agreements which cannot be stored in the central repository should have a reference to where they are stored
- Consider coordination with Contract Services and their repository.
- Agreements should be easily accessible to appropriate staff.
- An owner should be defined for the repository.
- An owner or sponsor (role or person) should be assigned for each agreement.

6.3 Standardize processes and templates for information sharing agreements

Project purpose This project will provide a standardized approach and template for data sharing agreements to ensure consistent review and approval processes for all agreements with third parties (inbound and outbound).

Guidance

- The policy should outline accountabilities and acceptable criteria for all agreements with third parties.
- Agreements should include standard clauses, terms & provisions.
- Agreements should have an appropriate level of approval and decision making regarding agreements with third parties to ensure consistency.
- There should be appropriate notification to all relevant parties of new agreements.
- An owner or sponsor (role or person) should be assigned for each agreement.
- Standardized processes and templates, with an exception process for non-standard agreements, should be developed for information sharing agreements.
- Ensure central coordination does not increase processing time and pursue opportunities to improve efficiency (through LEAN initiative).

7. Logging and monitoring

Project overview

Project purpose Enhance logging and monitoring practices and capabilities across key systems.

7.1. Evaluate existing logging capabilities and enable or enhance where appropriate

Project purpose The purpose of this project is to enable logging in the short term on existing applications and systems where possible and appropriate based on a risk based analysis. Additionally, monitoring processes should be defined to review log files and escalate issues identified.

Guidance

- Critical logging requirements should be developed above and beyond those currently supported (i.e., logging of user activities beyond log-on and log-off) for investigative and exception reporting purposes. Consider starting with the HealthIdeas environment and then enhancing logging in other systems (e.g., SAS, databases, applications, network layers, operating systems, etc.), where technically feasible, based on level of risk (sensitivity of information, amount of data, number of users, etc.)
- These additional logging capabilities can support:
 - Sample-based periodic compliance monitoring (see Project 10.0 – Compliance Monitoring)
 - Preliminary investigations triggered by complaints
 - Comprehensive investigations when a known breach has occurred
 - Targeted auditing based on established rules (VIP lists, etc.) to detect inappropriate activity
- Recognizing that manual log reviews are time consuming and can be labour intensive, the above are recommended where logging capabilities and resource availability permit
- Where manual log reviews can be implemented, this program should be communicated to the user community to raise awareness of the monitoring program.

7.2. Design and implement a logging solution to support the longer-term needs of the secure data environment

Project purpose The purpose of this project is to design and implement a long-term logging and monitoring solution for key systems and applications in the Ministry. The logging solution will provide a consistent and efficient means for capturing, and securely retaining a sufficient level of logging data for Ministry systems. This project does not include the implementation of the chosen solution (the time and capital expenditure required will depend on the solution chosen, and has therefore not been included in the estimate below).

Guidance

- To ensure the system is right-sized and meets Ministry requirements, the Ministry should focus initially on clear definition of functional requirements (based on policies and regulatory and contractual obligations).
- Based on system and functional requirements, a formal evaluation process should be initiated to select an appropriate tool.
 - Lessons learned should be identified from successful implementations elsewhere in Government and/or within Health Authorities
 - Consider solutions where licensing agreements within Government may be leveraged
- The requirements and infrastructure should be mapped against a chosen solution to develop a prioritized implementation plan.
- Consider a phased approach to address critical requirements first and to increase functionality over time (e.g., expanding from basic logging to dashboarding, log correlation, alerts and triage, etc.)
- Consider leveraging automation of logging and event correlation technologies where possible, in order to reduce manual effort.
- The system should be tuned over time to balance sensitivity with the follow up required for false positives.
- Procedures should be documented to support maintenance, monitoring, notification, escalation and remediation processes, and continuous improvement of procedures.
- Roles and responsibilities required to support operation and maintenance of the solution should be defined.
- A regular reporting strategy should be developed to support system tuning internally, but also to communicate key results to the Ministry as part of the ongoing awareness program.
- Technical and business process training requirements should be identified and a training plan should be developed.

8. Security Management & Operational Practices

Project overview

Project purpose Enhance security management practices for maintaining a secure technology environment.

8.1. Consolidate additional enhancement opportunities and address them on a priority basis

Project purpose The purpose of this project is to rationalize IT security-related risks and issues identified through internal Ministry reviews as well as this review. These enhancement opportunities should be identified and implemented on a priority basis (based on risk).

Guidance

- This initiative should collect and rationalize a list of enhancement opportunities in order to support continual improvement of security controls within the IT environment. Items for consideration include:
 - Review the patch management procedure at the OS and application layers to ensure that patches are applied in a timely manner following a defined process.
 - Periodic reviews of MoH applications to ensure resources are in place to upgrade and patch applications as necessary.
 - Review security services performed by each service provider to ensure a consistent level of security practices are performed
 - Where possible, require mandatory secure communication to and from all health data systems (e.g., HealthIdeas)
- Projects to address these and related enhancement opportunities should be scoped and prioritized based on risk and alignment to other strategic initiatives
- Consider incorporating enhancement opportunities into other projects where appropriate, or creating new projects as required.

8.2. Clearly define the security management and operational roles responsible for the secure data environment

Project purpose The purpose of this project is to clearly define the operational and management roles to ensure clear accountability for all security aspects associated with the secure data environment. This will also ensure that a clear standard and strategy for security is in place across all infrastructure, networks and applications that are managed by the Ministry as well as those managed by third parties.

Guidance

- Clear ownership and accountability for security should be driven from the executive level.
- Centralized roles responsible and accountable for ensuring coordination of security management practices should be defined and empowered.
- Security management responsibilities should align with Government's Information Security Policy, but address specific requirements related to sensitive health information
- Responsibilities to consider for Security Management include:
 - Monitoring of security infrastructure and the tracking, follow up and closure of incidents and events.
 - Responding to issues identified through scanning and risk assessments performed by the program areas.
 - Ensuring STRAs & PIAs are built into the SDLC process
 - Providing direction for the completion of Security Threat Risk Assessments for new projects
 - Ensuring contracts with service providers contain the appropriate clauses and provisions to ensure compliance MoH security and privacy policies.
 - Acting as a key resource for the Ministry on Security-related topics, and representing the security perspective of the organization at senior levels.
- Once responsibilities have been clarified, the appropriate job description(s) should be created and/or updated to ensure they are formally recognized and assigned.
- The security management function should serve a consultative role while the compliance function should be responsible for assuring compliance.
- Responsibilities & accountability related to the security program may span several roles, but clear accountability should be defined and agreed upon.
- The security management function will work with other functions or branches within the Ministry (e.g., the Compliance Monitoring function and the Health Information Privacy, Security and Legislation Branch) and service providers (e.g., SSBC). Clear division of accountabilities should be in place and agreed to and should be reflected in related procedures.

8.3. Develop and maintain security reference architecture

Project purpose The purpose of this project is to design and maintain a security reference architecture that describes the minimum functional and architectural security standards of the IT environment. This includes all security aspects of the environment, with particular reference to the access model, user provisioning and logging and monitoring.

Guidance

- The security reference architecture should describe clearly defined design principles and should be based upon accepted industry standards such as TOGAF (The Open Group Architecture Framework).
- The architecture should define the minimum standards to which all key components of the environment must comply in order to ensure a consistent level of control and risk management
- The architecture should consider key components:
 - Conceptual architecture
 - Functional architecture
 - Physical architecture
- The architecture should align with the overall Ministry Enterprise Architecture as well as the requirements outlined in Government's Information Security Policy, as appropriate.

9. Ministry-specific policies and guidelines

Project overview

Project purpose Develop a Ministry-specific privacy policy

9.1. Develop a ministry privacy policy

Project purpose The purpose of this project is to develop and implement a Privacy Policy that is specific to the Ministry of Health. This policy will provide a single point of reference regarding privacy matters including obligations, authorities and roles and responsibilities.

Guidance	• Develop a single overarching Ministry Privacy Policy. This policy should include/address the following information: – Privacy principles – appropriate situations where information can be collected. – Requirements for collection, use & disclosure of personally identifiable information – Requirements for privacy considerations in data sharing agreements, STRAs, Contracts, and PIAs – Outline employee roles and responsibilities with respect to privacy; including completing privacy training and a periodic acknowledgement sign-off – Requirement for annual signoff of Privacy and Confidentiality acknowledgement. – Describe roles and responsibilities for key Privacy resources within the Ministry, including the most senior leader with accountability for privacy, compliance monitoring function and other privacy resources – Describe how MoH monitors and enforces employee compliance with its privacy policy and consequences for non-compliance • The Privacy Policy should be reviewed at least annually. This review should address any changes to relevant legislation or policy and should also incorporate lessons learned from any breaches or similar incidents.
-----------------	---

9.2. Develop Ministry-specific guidance for key topics

Project purpose The purpose of this project is to augment existing guidance for key information security & privacy topics and ensure that the guidance is communicated to all relevant MoH employees.

Guidance	• Input should be solicited from representatives of each Division regarding requirements for guidance on information privacy and security topics. This should include input regarding how best to communicate this information to support effective understanding and usage. • Specific topics to consider for targeted, Ministry-specific guidance include: – Decision making support for sharing of sensitive information. Define the spectrum of data between personally identifiable information and open data and the considerations for use and disclosure across this spectrum. – Acceptable use of sensitive information within the Ministry and with third parties – Incident management process with respect to information privacy and security • Consider updates to guidance documents to include appropriate use of portable media. • Integrate key support materials into the Training & Awareness Program where possible to support adoption of, and familiarity with, these materials. • Utilize the Awareness program to communicate regularly to employees regarding available materials, new materials that are created and updates to existing materials • To facilitate use of reference materials, consider rationalizing key reference documents where possible. Some examples for consideration include: – Computer and Technology Acceptable Use Policy/Procedure (e.g. disposal of assets, appropriate use of information systems, internet, software, communicating via email) – Standard Operating Procedures for the Secure Transfer, Storage, Retention, and Disposal of Personal Identifiable Information (e.g. retention schedule, approved areas for storage, destruction of paper documentation, portable media devices) • To support continual improvement, a process should be defined to regularly review and update key guidance documents and policies to ensure they remain current and incorporate lessons learned (including innovative practices from across the Ministry as well as results from compliance monitoring)
-----------------	--

10. Enhanced compliance monitoring function

Project overview

Project purpose Implement an enhanced compliance monitoring function at the Ministry.

10.1. Implement an enhanced compliance monitoring function

Project purpose The purpose of this project is to review the current compliance monitoring function at the Ministry, and implement enhancements to that function.

Guidance	• In developing the scope of the compliance monitoring function, the following should be considered: – Internal access, use & disclosure of data (Ministry compliance with Ministry policy and legislation) – Internal access, use & disclosure of data (Ministry compliance with obligations to third parties that provide data to the Ministry) – External access, use & disclosure of Ministry data by third parties (third party compliance with obligations defined by Ministry ISAs) • Once the mandate is endorsed by Management, the team structure should be defined to ensure it has the capacity and capabilities to deliver on this mandate. • Consider making acknowledgement and response to audit & review findings mandatory. • Roles and responsibilities with respect to appropriately responding to audit & review findings should be defined and communicated. • Consider defining policies outlining penalties for non-compliance with audit & review findings. • In developing the audit & review plan for the first year, ensure that it is risk based and takes into account the key findings of this and other reviews • Look to leverage other monitoring/audit activities that are underway or planned (either within the Government or by third party auditors). • Consider utilizing self-certification for entities that the Ministry provides data to, in order to support third party compliance monitoring. • Support efficiency, effectiveness and consistency by utilizing existing industry accepted frameworks and auditing standards and practices. • Communicate role, mandate, audit & review plan and results across the Ministry and to relevant stakeholders. • Regular risk assessments on the existing environment should be performed, addressing remediation requirements and incorporating lessons learned into the overall security program. • The compliance function should be positioned to be independent of the groups audited and should report to a senior leader within the Ministry as defined in the Governance model. • Consider piloting of audit & review process on a sample of issues to ensure viability of model and obtain feedback from the divisions on the evaluation process and results.
-----------------	---

www.deloitte.ca

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte operates in Quebec as Deloitte s.e.n.c.r.l., a Quebec limited liability partnership.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

© Deloitte LLP and affiliated entities.