|  |
| --- |
|  |
| Site Readiness Assessment Toolkit |
| Data, Privacy, and Security Assessment Tools |

|  |
| --- |
| Justin Fyfe  9-13-2019 |

Contents

[1. Document Information 2](#_Toc21433130)

[1.1. Revision History 2](#_Toc21433131)

[1.2. Related Documents 2](#_Toc21433132)

[1.3. Authors & Contributors 2](#_Toc21433133)

[2. Executive Summary 3](#_Toc21433134)

[2.1. Why Privacy and Security are Important to the MPI 3](#_Toc21433135)

[2.2. Evolution of the Toolkit 3](#_Toc21433136)

[2.3. How to Use This Toolkit 3](#_Toc21433137)

[3. Technical Assessment Tools 5](#_Toc21433138)

[3.1. Technical Privacy Assessment Tool 5](#_Toc21433139)

[3.2. Technical Security Requirements 6](#_Toc21433140)

[4. Administrative Assessment Tool 10](#_Toc21433141)

[4.1. Administrative Privacy Assessment Tool 10](#_Toc21433142)

[4.2. Administrative Security Assessment Tool 14](#_Toc21433143)

[5. Data Collection Policy Assessment Tool 20](#_Toc21433144)

[6. Appendices 22](#_Toc21433145)

[6.1. Sample Privacy Impact Assessment 22](#_Toc21433146)

[Good Health Hospital Privacy Impact Assessment 22](https://jfyfe-my.sharepoint.com/personal/justin_fyfesoftware_ca/Documents/Projects/2019/UNOPS/MRE2/MPI%20Readiness%20Assessment.docx#_Toc21433147)

[Executive Summary 22](https://jfyfe-my.sharepoint.com/personal/justin_fyfesoftware_ca/Documents/Projects/2019/UNOPS/MRE2/MPI%20Readiness%20Assessment.docx#_Toc21433148)

[Workflows Concerning MPI 22](https://jfyfe-my.sharepoint.com/personal/justin_fyfesoftware_ca/Documents/Projects/2019/UNOPS/MRE2/MPI%20Readiness%20Assessment.docx#_Toc21433149)

[Workflow 1: Registering a new HIV Patient 22](https://jfyfe-my.sharepoint.com/personal/justin_fyfesoftware_ca/Documents/Projects/2019/UNOPS/MRE2/MPI%20Readiness%20Assessment.docx#_Toc21433150)

[6.2. Sample Consent Form 22](#_Toc21433151)

# Document Information

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Date** | **Changes** | **Version** |
| Justin Fyfe | Feb, 2019 | Initial Draft | 0.75 |
| Justin Fyfe | Sept 13, 2019 | Edits to make document suitable for sharing and review to broader community. | 0.8 |
| Justin Fyfe | March 14, 2022 | Updates to include more instructions – making it a general tool for the SanteDB Community members | 1.0 |

## Related Documents

|  |  |
| --- | --- |
| **Document Link** | **Relevance** |
| https://www.infoway-inforoute.ca/en/component/edocman/resources/technical-documents/389-ehr-privacy-and-security-requirements | Canada Health Infoway Privacy and Security Requirements upon which the requirements in this document are based. |
| Link Needed | Data Protection Impact Assessment |
| [Developing Privacy Impact Assessments - SanteSuite Help Portal](https://help.santesuite.org/installation/installation-1/planning-and-preparation-work/developing-privacy-impact-assessments) | Provides insights and pointers on developing and assessing the privacy impact of your SanteDB deployment |
|  |  |

## Authors & Contributors

|  |  |
| --- | --- |
| **Contributor** | **Organization** |
| Justin Fyfe | SanteSuite |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Glossary of Terms

If your implementation uses country or context specific terms then they should be enumerated here. For example, if your document refers to a national health facility registry (NHFR) it should include this definition in the table.

This provides readers a place to “look-up” what specific terms found in the document mean.

|  |  |
| --- | --- |
| **Term** | **Definition** |
| MPI | Master Patient Index – A solution which is responsible for maintaining and cross referencing the identity of persons/patients within the authority. |
| dCDR | Disconnected Clinical Data Repository – The terms used by SanteDB to describe the offline portion (or client portion) of the clinical data repository (see: [SanteDB Architecture - SanteSuite Help Portal](https://help.santesuite.org/santedb/architecture#dcdr-clients)) |
| iCDR | Integrated Clinical Data Repository – The term used by SanteDB to describe the central, jurisdictional clinical data repository ([SanteDB Architecture - SanteSuite Help Portal](https://help.santesuite.org/santedb/architecture#icdr-server)) |
| PHI | Personal Health Information – Discrete health event information which can be linked to a single patient. PHI could diagnoses, observations, demographics, etc. |
| PII | Personally Identifiable Information – Information which can be used to uniquely identify a person. |

## Document License

This document was original developed under TA agreement and is based on several source documents (linked in the references section). In order to promote sharing and dissemination this document is licensed under the terms of the Creative Commons Attribution + Share-Alike 4.0 License ([Creative Commons — Attribution-ShareAlike 4.0 International — CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)).  
  
A picture containing text, clipart

Description automatically generated

Original Copyright © 2022, SanteSuite Inc.

## Outstanding Issues / Comments

Use this section to collect or enumerate any feedback on the document which has yet to be resolved. The outstanding issues and comments section should be used while the document is being authored, and can be removed prior to publication.

Note: This section is included in the document to provide readers with a reference point within the document (for a specific version of the document they are reading) the issues and active/outstanding issues with the content of this version of the document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Discussion / Issues** | **Resolved** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Executive Summary

This document is intended to serve as a toolkit which may be leveraged by organizations implementing and connecting to your SanteDB project and by software vendors/suppliers integrating their solutions into SanteDB.

While completing this assessment, it is important to remember to assess each requirement truthfully. The primary purpose of this toolkit is to allow partners to identify next steps and procedures required to upgrade their processes and environment to meet some of the best practices in data collection, privacy and security.

**Note:** This document is a template – it is intended to be adapted by those operationalizing SanteDB software for their local use cases. You may think of the requirements listed here as a guideline for good practices which should be implemented, however, not all requirements may be applicable in your deployment.

## Why Privacy and Security are Important

The primary purpose of centralized health infrastructure is to share patient centered data. To accomplish this, SanteDB must collect and disclose personally identifiable health information (PHI) which may be sensitive (like ART/TB registration numbers, names, addresses, and contact details of patients who may be at an elevated risk, etc.). Because of this, organizations deploying or connecting to SanteDB should ensure that, to the best of their ability, they can meet or exceed a minimum set of requirements.

## Using this Toolkit

This toolkit is broken into three sections:

* **Technical Assessment Tools**: This section focuses primarily on technical mitigations/strategies which can be used by vendors of software or IT operations to protect data. This section will help gauge compliance with (and set goals to achieve) best practices for data collection, protection, and management.
* **Administrative Assessment Tools**: This section primarily focuses on organizational or administrative mitigations/strategies to protect data. This section is primarily targeted to organizations seeking to assess their environments adherence to best practices for data sharing.
* **Data Collection Assessment Tools:** This section is primarily concerned with the collection of data by clinicians, administrative staff and other “users” of the system.

It is recommended that the toolkit be used as part of a rollout of SanteDB projects:

1. Adapt the toolkit:
   1. Review the requirements to meet your local context and implementation. Not all requirements are needed or may even be applicable in all contexts.
   2. Prepare a country/context specific version of the assessment toolkit and get consensus from relevant stakeholders that the requirements accurately reflect the project being undertaken.
   3. Integrate the assessment requirements into your training for staff members performing rollout on the importance of security and privacy, data collection and protection.
2. Use the toolkit:
   1. Read the description of the requirement, discuss the requirement with staff, suppliers, contractors, or other actors involved in operating or developing the health solution.
   2. Rank the current implementation/compliance with the requirement:
      1. **Fully Met:** Software and/or organization fully implements all portions of the requirement.
      2. **Partially Met:** Software and/or organization implements some of the requirement however does not fully comply with the complete requirement verbiage.
      3. **Not Met:** Software and/or organization does not comply with any of the requirement.
      4. **Exempt:** Software and/or organization should be exempt from the requirement because it is not applicable in your use case.
   3. Describe why the assessment is justified and/or any initiatives/corrective measures that are underway or will be implemented to increase compliance with the requirement. Where possible, indicate approximate timelines and effort.
3. Address identified gaps from the toolkit assessment for each site
   1. Not all software or sites will perfectly implement all requirements (even SanteDB iCDR and dCDR partially meet some of the requirements)
   2. Gaps should be integrated into a development roadmap for the site, software, or staff.

# Technical Assessment Tools

This section is intended to be completed by technical staff. This could be:

* Software Vendors who are maintaining the computer program code of the health solution
* Operations Staff who are responsible for deployment/maintenance of the operational environment
* Subject matter experts who are performing independent review of a software platform

## Technical Privacy Assessment Tool

| # | Privacy Requirement | Analysis | Description |
| --- | --- | --- | --- |
| TPR1 | **Recordation of Consent**  Where required by law, health systems software storing personally identifiable health information must be able to record a patient/person’s consent including withholding or withdrawal.  Health systems software should also provide a mechanism, where applicable, to prevent data from being shared upon request of the patient. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TPR2 | **Association Consent with PHI**  Where health systems are connected to the centralized infrastructure, the system must be capable of associating the patient/person’s agreement/withdrawal or withholding of consent with the data for which they are consenting. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TPR3 | **Logging Access, Modification, Disclosure**  Health systems must provide a mechanism to record when records are accessed, modified, or disclosed to third parties. These access logs must include:   * The access, modification or disclosure action that occurred * The date/time of the modification, access, or disclosure * The identity of the user or system which modified, accessed, or disclosed the data   Where required by law, health systems should provide a mechanism for the accountable person (see organization Privacy impact assessment requirement APR1). | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TPR4 | **Retaining Records**  Health systems recording personally identifiable health information must retain that health information in accordance with local legislation. The systems should provide mechanism for archiving, destroying, and pruning data following legislated retention periods. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |

## Technical Security Requirements

| # | Security Requirement | Analysis | Description |
| --- | --- | --- | --- |
| TSR1 | **Labelling Personal Health Information as Confidential**  Health Information Systems connecting to shared infrastructure should be capable of informing users of the system of the confidential nature of the information and should either:   1. Append the confidential indication on all printouts or hard copies PHI, and/or 2. Display this labelling to the user upon logging into the system, and/or 3. Requiring the acceptance of an “acceptable use policy”. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR2 | **Preserving the History of PHI**  Health information systems should be capable of displaying the former content of a record at any point in the past (within the scope of applicable retention policies), as well as indicate which user or system was responsible for the changes.  Alternatively, health information systems should keep a record of modifications made to the content of a record over time, such that the content of a particular record can be established. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR3 | **Logging Access to PHI**  Health information systems should be capable of logging all access to personal health information in an audit trail. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR4 | **Minimum Content of Audits**  Health information systems should record, at minimum, in their audit logs:   1. The ID of the user or system which accessed the data 2. The role of that user when they were accessing the data 3. The organization to which the user or system whom accessed the data belongs 4. The ID of the patient to which the personal health information belongs 5. The function performed by the user (query, edit/save, etc.) 6. The date & time that the action occurred 7. In the case that the user was accessing personal information that they would not normally have access to (i.e. an override) the reason for the override. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR5 | **Restricting Access to Users by Role**  All health systems connected to the SanteDB infrastructure must be capable of restricting access to functions based on the current role(s) that the logged in user is assigned. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR6 | **Timely Revocation of Access Privileges** All health systems connected to the SanteDB infrastructure must be capable of revoking access to users in a timely manner (i.e. the system should deny login immediately after a user’s access has been revoked) | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR7 | **Granting Access by Association**  All health systems connected to the SanteDB infrastructure must be capable of granting access to clinical data, based on the patients for which the user is assigned (example: if a system supports both immunizations and HIV care, immunization nurses should not see data for HIV patients).  In such cases where an information system only covers one patient population, the system should provide a mechanism for distinguishing between clinical and non-clinical users of the system (example: administrators) | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR8 | **Robustly Authenticate Users**  All health systems connected to the SanteDB infrastructure must authenticate users using a robust mechanism. For example, requiring each individual user to have their own username and complex password. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR9 | **Restricting Access to Unattended Workstations**  All health systems connected to the SanteDB infrastructure must be capable of expiring sessions after a predetermined amount of time and must restrict any access after the session has expired. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR10 | **Uniquely Identifying Patients**  All health systems connected to the SanteDB infrastructure must be capable of uniquely identifying patients and must   1. Ensure that patients/persons are assigned an identifier (patient ID) that can uniquely identify the patient/person within the scope of that system, and 2. Be capable of merging two or more patients within their own identity domain. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR11 | **Validating Input**  All health systems connecting to the SanteDB infrastructure must be capable, wherever feasible, of validating user inputs in order to safeguard against incorrect and inappropriate data values. The following input validations should be considered:   1. Input checks to detect out of range/bounds values 2. Detect invalid characters in user input fields 3. Missing or incomplete data 4. Nefarious attempts to override security controls (SQL Injection, HTML Injection, etc.) | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR12 | **Provide Digital Signatures**  All health systems storing personal health information, where appropriate, should provide and/or implement a mechanism for digitally signing content authored by users to detect tampering of data. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| TSR13 | **Reporting Security Incidents**  All health systems storing personal health information should provide a mechanism for alerting the accountable person of detected security breaches (if feasible), invalid access attempts, and improper use. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |

# Administrative Assessment Tool

This section is intended to serve as a guidebook for organizations, clinics, hospitals, etc. integrating patient information. The section is primarily intended for:

* Organizational administrators (managers, directors, etc.) to organize their institution’s participation in the shared infrastructure.
* Third parties performing independent assessments of organizations connecting to the central infrastructure.
* IT administrators or Network Operation Center staff deploying health software into their environment.

## Administrative Privacy Assessment Tool

| # | Privacy Requirement | Analysis | Description |
| --- | --- | --- | --- |
| APR1 | **Accountable Person**  Organizations collecting personal health information must publicly name an individual or group who is accountable for facilitating compliance with applicable data protection policies and legislation, and the following of privacy requirements. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR2 | **Third Party Agreements**  Organizations connecting to the SanteDB infrastructure must enter a contractual means to provide a comparable level of privacy protection while exchanging data with the SanteDB infrastructure. The content of such an agreement will need to be negotiated, however usually contains:   1. The purpose(s) for which personally identifiable information is being shared between the organization and SanteDB infrastructure 2. Listing the identifiable information being shared with or used from the SanteDB infrastructure 3. The purposes for which the identifiable information is being disclosed to either the SanteDB infrastructure or to the organization connected to the SanteDB infrastructure 4. Obligations of the organization upon termination of the agreement. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR3 | **Establish a Privacy Policy**  Organizations connecting to the SanteDB infrastructure must implement a privacy and security policy and standard operating procedures, including:   1. Standard procedures to protect identifiable information. 2. Establishing procedures to receive and respond to privacy related complaints and inquiries. 3. Training users and communicating to users information about the organization’s privacy and security policies and practices. 4. Developing communications materials to explain to the general public the organization’s privacy policies and use of identifiable health information. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR4 | **Identify the Purpose of Collection, Use and Disclosure**  Organizations connecting to the SanteDB infrastructure must:   1. Identify all the purposes for which the identifiable information will be collected, used and disclosed at or before the time it will be collected, 2. Make a reasonable effort to inform patients/persons of why data is being collected in a manner understandable to the patient, prior to sharing their information with the SanteDB infrastructure. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR5 | **Limit the Collection, Use or Disclosure to Identified Purposes**  Organizations connecting to the SanteDB infrastructure should ensure that only information required by the SanteDB infrastructure is shared with the SanteDB infrastructure and should limit the collection of additional demographics in their own system unless identified in APR4. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR6 | **Obtain Knowledgeable Consent**  Except where inappropriate (i.e. patient safety, law, or professional code of practice), organizations connecting to the SanteDB infrastructure should obtain the knowledge and consent of each patient/person for the collection, or disclosure of their personal health information, and where required by local law, must obtain the consent of each patient prior to collecting, using or disclosing their personal health information.  For an example of a simple consent form see 6.2. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR7 | **Educating Patients of the Implications of their Consent**  Organizations should make a reasonable effort (for example, by using pamphlets, posters, etc.) to ensure that patients are educated about the implications of their consent. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR8 | **No Coerced Consent**  Organizations should not deny health services to patients who do not consent to their personal health information being collected, used or disclosed by the organization. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR9 | **Collecting Information by Lawful Means**  Organizations connecting to the SanteDB infrastructure must ensure that the personal information collected and shared with the SanteDB infrastructure was obtained following applicable laws and policies and should not deceive providers or patients for which information is being collected. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR10 | **Notifying Patients/Persons of Inappropriate use of Their Information**  Where feasible, organizations should notify patients when inappropriate access or disclosure events are detected. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR11 | **Retaining Records**  Organizations connecting to the SanteDB infrastructure should:   1. Retain personally identifiable health information in accordance with local laws and requirements outlined in any relevant legislation. 2. Should develop guidelines and standard operating procedures related to the retention of health information including:    1. The minimum length of time that personal health information is retained    2. The maximum length of time that personal health information should be retained    3. Appropriate processes for destroying, archiving, or otherwise removing stored health information. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR12 | **Accuracy**  Organizations connecting to the SanteDB infrastructure should take reasonable steps or make a reasonable effort to:   1. Ensure that data collected is accurate, complete and up to date as is necessary for the purposes for which it is to be used to identify patients. 2. Accurately identify a person prior to modifying their health information | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR13 | **Training Users and Raising Awareness**  Organizations connecting to the SanteDB infrastructure must ensure that privacy education, training and regular updates to any organizational policies and procedures are provided to each employee, contractor or third party who has access to any software system within the organization. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR14 | **Openness**  Organizations connecting to the SanteDB infrastructure must make specific information about their policies and practices relating to the use of personal health information available to the public.  At minimum, these organizations should, if feasible, make available the following information:   1. The name, title, and contact information of the accountable group or person whom is held accountable for privacy, 2. A description of the personally identifiable health information which is collected and shared by the organization with the SanteDB infrastructure, the limitations collection, use and disclosure of that data, and the retention of that data within the organization, 3. A general description (at a high level) of the administrative, technical, and physical safeguards in place as it relates to the storage of personally identifiable health information, 4. What patient demographics fields are shared with the SanteDB infrastructure from the organization’s systems, and why. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR15 | **Amending Inaccurate or Incomplete Information**  Organizations connecting to the SanteDB infrastructure should:   1. Amend any personally identifiable health information when a patient successfully demonstrates the inaccuracy of the information (i.e., correcting an address after showing a valid driver’s license) 2. Where applicable, notify the SanteDB infrastructure of the changed information and indicate the modifications 3. If unresolved inaccuracies exist, document them and notify the appropriate accountable person or group of the contested information. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR16 | **Challenging Compliance**  Organizations connecting to the SanteDB infrastructure must allow patients and/or auditors to challenge their compliance to the relevant policies, standards, and legislation. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| APR17 | **Perform a Privacy Impact Assessment**  Organizations connecting to the SanteDB infrastructure must perform a privacy impact assessment (see section 6.1 for an example) with regards to data and workflows for data which they are or plan to send to the SanteDB infrastructure.  See: [Developing Privacy Impact Assessments - SanteSuite Help Portal](https://help.santesuite.org/installation/installation-1/planning-and-preparation-work/developing-privacy-impact-assessments) for guidance on developing privacy impact assessments. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |

## Administrative Security Assessment Tool

| # | Security Requirement | Analysis | Description |
| --- | --- | --- | --- |
| ASR1 | **Perform a Threat Risk Assessment** Organizations connecting to the SanteDB infrastructure should perform a threat risk assessment to assess threats and risks to their software systems. After a careful review of these systems, organizations should put in place mitigation and prevention strategies to prevent potential security complications. Such a TRA should include:   1. An inventory of all IT assets connecting to the SanteDB infrastructure and all assets which may receive or consume data from those systems (i.e. an EMR may consume data from the SanteDB infrastructure, several systems may have access to that EMR) 2. An assessment, for each asset, of how critical it is to the maintain the security, confidentiality, availability and accountability of that asset. 3. Where feasible, a vulnerability analysis including a comprehensive listing of the vulnerabilities identified in the underlying components, 4. A risk analysis that determines the residual risk after mitigation and prevention strategies are put in place.   See: [Develop Threat / Risk Assessments - SanteSuite Help Portal](https://help.santesuite.org/installation/installation-1/planning-and-preparation-work/develop-threat-risk-assessments) for guidance on developing a TRA. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR2 | **Establish a Security Policy**  Organizations connecting to the SanteDB infrastructure must have a written IT security policy that is approved by the management of that organization and published to all employees, contractors and third parties operating within the organization. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR3 | **Allocate Responsibilities for Security and Management of Assets**  Organizations connecting to the SanteDB infrastructure should establish a written list of those persons who are responsible for safeguarding, maintenance and management of assets connected to the MPI and assets which leverage MPI data. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR4 | **Independent Review of Security Policies and Implementation**  Organizations connecting to the SanteDB infrastructure must have the implementation of their security policies either:   1. Reviewed independently, 2. Attested to by a designated IT person and/or management | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR5 | **Address Security in Third-Party Agreements**  Organizations connecting to the SanteDB infrastructure, which share data from the MPI with third parties, must include relevant sections related to appropriate use, security, and privacy in a third party agreement with the third party to which SanteDB infrastructure data will be disclosed. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR6 | **Transmitting Personally Identified Health Information**  Organizations connecting to the SanteDB infrastructure must connect to the SanteDB infrastructure using the secured interfaces provided by the SanteDB infrastructure. Furthermore, organizations which allow third party access to SanteDB infrastructure sourced data must protect the transmission of SanteDB infrastructure data to third parties by either:   1. Physically securing the connection (firewalls on a private network with only third-party systems) 2. Encrypting the data transmission 3. Allowing only access to other local services on the same machine | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR7 | **Addressing User Responsibilities in Job Descriptions**  All organizations connecting to the SanteDB infrastructure should including in relevant job descriptions, employment contracts or other agreements with third parties, the responsibilities of users accessing data from the SanteDB infrastructure. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR8 | **Verifying the Identity of Users**  All organizations connecting to the SanteDB infrastructure must verify the identity of every staff member, contractor, or third party which will be accessing IT systems which store or access SanteDB infrastructure data and must ensure that each individual user of an IT asset is uniquely identified with an appropriate user account and password. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR9 | **Training Users and Raising Security Awareness**  Organizations connecting to the SanteDB infrastructure must provide employees, contractors, and third parties with training which identifies the organization’s security policies, the acceptable use of SanteDB infrastructure data, and general security practices (example: Safe web browsing practices, viruses, etc.) | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR10 | **Terminating User Access when Terminating Employment**  Organizations connecting to the SanteDB infrastructure must terminate the access of a user once the user is no longer an employee, contractor or registered third party of the organization. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR11 | **Physically Securing IT Assets**  Organizations connecting to the SanteDB infrastructure must, where feasible, physically secure any IT assets which access and store SanteDB infrastructure data, and must have identified standard operating procedures for preventing access to the SanteDB infrastructure when/if an IT asset is lost, stolen, or retired. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR12 | **Disposing of IT Assets**  Organizations connecting to the SanteDB infrastructure must establish standard procedures for disposing of IT assets including:   1. The complete removal of all security keys, access tokens, or other protective measures from the IT asset, 2. The complete removal or destruction of all data on the IT asset that was obtained from the SanteDB infrastructure | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR13 | **Removing of IT Assets**  Organizations which connect to the SanteDB infrastructure must ensure that any IT assets which contain personally identifiable SanteDB infrastructure data are not removed from the premises without prior approval of the organization’s management (including for maintenance). | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR14 | **Separation of Production and Testing/Training Environments**  Organizations which connect to the SanteDB infrastructure must ensure that any assets configured or used for training or testing are separate from those used for training and testing purposes. And must ensure that data from production environments is not used for testing and/or training. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR15 | **Protecting Against Malware**  Organizations which connect to the SanteDB infrastructure must ensure that reasonable steps are being taken to prevent malware such as ransomware, viruses, rootkits, and other nefarious software from operating on IT assets storing MPI data. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR16 | **Securely Backing up Data**  Organizations connecting to the SanteDB infrastructure must ensure that any backups of the personally identifiable data obtained from the SanteDB infrastructure is backed up in a secure fashion either by:   1. Physical protection (locked vault) 2. Encryption | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR17 | **Protecting MPI Data on Portable Media**  Organizations connecting to the SanteDB infrastructure must ensure that any data which originated from the SanteDB infrastructure is appropriately protected when/if that data is saved to portable media, such as using encryption. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR18 | **Protecting Data Storage**  All organizations connecting to the SanteDB infrastructure must ensure that any personally identifiable data obtained from the SanteDB infrastructure is stored in an encrypted form. This could include (but is not limited to):   1. Encrypting the entire device (using BitLocker, TruCrypt or similar technology) 2. Encrypting the datafile/database which contains SanteDB infrastructure data | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR19 | **Retaining Audit Logs & Securing Access to Audits**  Organizations connecting to the SanteDB infrastructure should ensure that appropriate audit logs are maintained and access to such audit logs are secured. See TSR4 for more information as to minimum content of audits. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR20 | **Registering Users**  All organizations connecting to the SanteDB infrastructure must subject potential users of IT assets that connect to the SanteDB infrastructure and may potentially come into contact with personally identifiable health information from the SanteDB infrastructure, to a formal user registration process. This process must ensure:   1. The level of user identification provided ensures the appropriate identity of the user (i.e. passport, driver’s license, etc.) 2. Each potential user has a relationship with the organization as either an employee, contractor or registered third party. 3. Each potential user as a legitimate need to access SanteDB infrastructure data (or the system which connects to the SanteDB infrastructure) | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR21 | **Develop an Acceptable Use Agreement**  Organizations connecting to the SanteDB infrastructure must define the responsibilities of a user and must ensure that users are aware of these uses as part of an acceptable use agreement. Such agreements include:   1. Under what conditions the user may collect, use or disclose personal health information to/from the SanteDB infrastructure, 2. Under what conditions the user must not collect, use or disclose personal health information to/from the SanteDB infrastructure, 3. The repercussions of violating the agreement | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ASR22 | **Implementing Regular Software Updates**  Organizations connecting to the SanteDB infrastructure must ensure that appropriate IT procedures are in place to ensure IT assets and software are up to date with the latest security and stability patches. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |

# Data Collection Policy Assessment Tool

Software vendors and organizations connecting to a SanteDB infrastructure should review and complete this assessment together to ensure compliance with best practices.

| # | Requirement | Analysis | Description |
| --- | --- | --- | --- |
| ADR1 | **Collecting Minimum Data Set**  Organizations collecting patient demographics to be shared with the SanteDB infrastructure must collect the minimum dataset for patient demographics specified in the SanteDB infrastructure Conformance Profile. These include:   1. At least one (1) reliable identifier for the patient such as National Health ID, National Citizen ID, Passport Number, Birth Certificate Number or Driver’s License Number. 2. The name of the patient 3. The date of birth of the patient 4. The gender of the patient 5. The address of the patient (to the City level if possible) | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ADR2 | **Verbally Request Information from Patients**  Organizations collecting data that will be shared with the SanteDB infrastructure should ask patients to verbally state their demographics information rather than asking patients yes/no questions. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ADR3 | **Authentication of Patient Identity**  Organizations collecting data that will be shared with the SanteDB infrastructure should ask adult patients to provide valid government photo identification prior to registering a new patient, in order to verify their identity.  Organizations may wish to collect biometric data related to a patient to authenticate the patient on subsequent visits. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ADR4 | **Patient Confirmation of Demographic Data**  Where feasible, organizations collecting data that will be shared with the SanteDB infrastructure should ask the patient to confirm the details of their registration prior to saving the demographic record. If errors are detected by the patient on a subsequent visit, these errors should be corrected according to APR15. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |
| ADR5 | **Photographic Identification of Patients**  Where feasible and applicable, organizations should consider taking photographs of their patient’s face and should include those images in the local registration system, where such a photograph would not compromise patient privacy (i.e. the patient is identified at an elevated risk). These photographs must not be sent to the central SanteDB infrastructure. | * Fully Met * Partially Met * Not Met * Exempted (state why) |  |

# Appendices

## Sample Data Sharing Documentation

Included below is a sample privacy impact assessment. It can be used as a starting point for organizations to assess the data they are collecting and the purpose of such data collection.

Good Health Hospital Data Sharing Documentation

Executive Summary

Good Health Hospital is a 1000 bed hospital located in X, it is responsible for delivery of emergency care….

Describe the business that your organization undertakes, how it uses MPI and what you hope to do with MPI data

Workflows Concerning MPI

Good Health Hospital leverages several electronic medical records systems for HIV, TB, and acute care. Good Health Hospital has a challenge with consistently identifying patients….

Describe the workflows that you hope to leverage MPI for.

Workflow 1: Registering a new HIV Patient

When a new patient presents to the HIV care clinic at Good Health Hospital, the clinician will first search the local database to determine whether the patient exists. If the patient does not exist, we expect the clinician to query the MPI using the patient’s known identifier. When neither the national MPI nor the local system contains the patient demographic we will register the patient.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Element** | **Source** | **Purpose** | **Sensitivity** | **Shared With** |
| ART Number | System | Identify patients in future a visit and correlate their care. | Very High | MPI |
| Name | Patient | Used to verify patient identity. | High | MPI |
| Gender | Patient | Used to classify other risk factors | Low | MPI |

## Sample Consent Form

**Data Collection, Use and Disclosure Form**

By signing this form, I authorize Good Health Hospital to collect, use and eventually share my personal demographics data with the central Patient Index located in City Name. I understand this data is limited to:

- Name - Date Of Birth - Gender

- MRN (Bracelet #) - ART / TB Case Number - Address

All other data will not be shared with the Master Patient Index and will be held at the facility. I understand if I have questions related to the privacy of my data I may contact [complaince@goodhealth.ca](mailto:complaince@goodhealth.ca).

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_