Supporting Requirements

The following tables include a broad set of interoperability and solution requirements for consideration and to support and provide guidance to implementers of the pan-Canadian Patient Summary - Interoperability Specification v1 Trial Implementation.

Note: Some of the supporting requirements may be further developed in future PS-CA Specifications releases and re-categorized as a Testable Requirement.

Business Legal: Requirements for Guidance and Support

BR ID	Description	Type	Subcategory
BR 1-01	A Patient Summary-CA Solution should provide the ability to manage the versioning, storage, preservation, destruction, and archiving of Patient Summaries produced and consumed by authorized users of the system in accordance to jurisdictional policies.	Recommended	Solution
BR 1-02	A Patient Summary-CA Solution should provide a health care provider with the option to review and sign-off the Patient Summary content before it is made available to PS-CA Consumers. Note: If the health care provider determines that changes are required to the Patient Summary prior to sign-off, the HCP will make the updates in the patient's chart. If the changes affect the Patient Summary content, a new Patient Summary will be created for review/sign-off by the HCP.	Recommended	Solution
BR 1-03	A Patient Summary-CA Solution shall provide a healthcare provider with the ability to invalidate a Patient Summary if they determine if it was entered in error or is invalid as required by jurisdictional policy.	Mandatory	Interoperability
BR 1-04	A Patient Summary-CA Solution should adhere to data retention policies set by local/jurisdictional policies and system requirements.	Recommended	Solution
BR 1-06	A Patient Summary-CA Solution may provide the ability to extract and save discrete data from a Patient Summary based on a request by an authorized system user.	Optional	Solution
BR 1-07	A PS-CA Author should reasonably ensure that the health information contained in a Patient Summary-CA is accurate, sufficiently complete and up to date to meet the specified clinical purpose.	Recommended	Solution
BR 1-08	A Patient Summary-CA Solution should be able to comply with a legal hold from an authorized entity based on jurisdictional policies. *Note: Legal hold policies prevent deletion of any electronically stored information on the PS-CA that may be imminent for a legal case.	Recommended	Solution
BR 1-09	A Patient Summary-CA Solution should be able to omit or mask data in a PS-CA in compliance with local /jurisdictional privacy policies.	Recommended	Solution
BR 1-10	A Patient Summary-CA Solution shall have the ability to produce a Patient Summary in compliance with a subject of care's consent directives in accordance to local/jurisdictional standards and/or policies. Note: For example, local/jurisdictional standards may include associating consent directives with PHI in the Patient Summary which cover concepts of maintaining association, processing consent directives, blocking transmission of PHI in Patient summary where consent directives are violated or no exception of a disclosure is outlined by law or by jurisdictional policy, and notifications to requesters when data is blocked due to consent directives	Mandatory	Interoperability
BR 1-12	A Patient Summary-CA Solution shall have the ability to indicate or make the PS-CA Consumer (e.g. a healthcare provider) aware that information about the subject of care has been omitted or masked based on a consent directives and jurisdictional policies.	Mandatory	Interoperability

Technical: Requirements for Guidance and Support

BR ID	Description	Type	Subcategory

BR 3-06	A Patient Summary-CA Solution should adhere to minimum local/jurisdictional industry standards for authentication (e.g., multi-factor authentication) of authorized users.	Recommended	Solution
BR 3-07	A Patient Summary-CA solution should, where feasible, segregate duties and areas of responsibility to reduce opportunities for unauthorized modification or misuse of PHI based on jurisdictional standards. Note: For example, appropriate access-controls should be put in place to segregate duties for authorized actors who have access and or can view hosted components of the Patient Summary in order to reduce opportunities for unauthorized modification or misuse of PHI and security-critical system data according to jurisdictional standards.	Recommended	Solution
BR 3-09	A Patient Summary-CA Solution should adhere to the minimum industry standards for role-based access control and security mechanisms for the Patient Summary, including defining the security level and authorization profile of all authorized actors and mapping each user to one or more roles and each role to one or more system functions, dictated by jurisdictional standards and system requirements. Note: For example, jurisdictional standards for role-based access control should consider the following standards such as ISO 22600-1:2014, which describes the scenarios and the critical parameters in information exchange across policy domains. Another example of a standard is ISO 22600-2:2014, which describes and explains, in a more detailed manner, the architectures and underlying models for privilege management and access control which are necessary for secure information sharing including the formal representation of policies.	Recommended	Solution
BR 3-10	A Patient Summary-CA Solution should adhere to jurisdictional standards for creation of secure audit logs that capture access to, modification or disclosure of Patient Summary-CA information. This includes the activities of PS-CA Producers, Consumers and Requesters. Note: For example, jurisdictional standards for appropriate secure-audit records should log PHI-related events, such as Patient Summary access (including access to confidential data), Patient Summary creation, Patient Summary amendments and changes, traceability of consent, consent directive overrides and more for the Patient Summary.	Recommended	Solution
BR 3-11	The Patient Summary-CA Solution should have the ability to capture secure audit log content as dictated by jurisdictional standards and/or system requirements. Note: For example, jurisdictional standards and/or system requirements for secure audit logs should consider Patient Summary schema and log content such as the user ID of authorized actors, the role the user is exercising, the organization of the accessing user (at least in those cases where an individual accesses information on behalf of more than one organization), the patient ID of the data subject (patient/person), the function performed by the accessing user, a timestamp, in the case of access override to blocked or masked records or portions of records, a reason for the override, and in the case of changes to consent directives made by a substitute decision-maker, the identity of the decision-maker.	Recommended	Solution
BR 3-12	A Patient Summary-CA Solution may provide the capability for a PS-CA to be de-identified, according to local /jurisdictional requirements.	Optional	Solution
BR 3-14	A Patient Summary-CA Solution should retrieve data elements for the PS-CA from the PS-CA Author's local data source.	Recommended	Solution
BR 3-15	A Patient Summary-CA Solution may provide the ability to convert structured documents (e.g. FHIR-based) to unstructured documents (e.g PDF), and make transformations between structured document formats (e.g. CDA).	Optional	Solution
BR 3-17	A Patient Summary-CA Solution should protect health information at rest, adhering to jurisdictional standards for encryption Note: For example, jurisdictional standards for encryption should cover concepts of cryptographic algorithms and protocols, and management of encryption keys to maintain the confidentiality and integrity of the Patient Summary.	Recommended	Solution