Santé et Services sociaux Québec

Outils d'aide au développement d'application

Introduction

Pour aider au développement des applications et permettre aux entreprises de concevoir et développer des systèmes respectant les critères de certification, le Bureau de Certification et d'Homologation du Ministère de la Santé et des Services sociaux rend disponible la liste non exhaustive des critères utilisés pour Trousse Globale de Vérification (Certification TGV).

Cette liste représente l'ensemble des aspects couverts pendant le processus de certification pour tous les types d'applications confondues. Selon les situations, cette liste est modifiée et adaptée soit en retirant, ajoutant ou modifiant les critères. Les fournisseurs d'applications doivent donc se servir du présent document comme un outil d'informations et non comme une garantie de passer la certification TGV.

Lors du processus d'audit, le fournisseur d'applications doit démontrer la conformité aux différents critères. Cette démonstration peut être effectuée de différentes façons :

1. Documentations utilisateurs, administrateurs ou autres.
2. Impressions d'écrans, exemples de rapports, etc.
3. Démonstrations du logiciel à un auditeur.

Il est donc fortement suggéré au fournisseur d'applications de préparer les justifications tout en vérifiant la conformité aux différents critères.

Listes des critères

Les critères dépendent des applications à certifier et varient selon les descriptions fournies. Pour permettre une revue préliminaire de la conformité, vous trouverez des listes de critères basées sur quatre scénarios ou types d'applications les plus probables. Comme mentionné précédemment, ces listes pourraient différer de ce qui sera audité suite à l'évaluation de votre application.

Les critères sont regroupés par volet. Les deux volets principaux sont : Protection des Renseignements Personnels (PRP) et Sécurité.

Dans chacune des listes de critères suivantes, vous retrouverez les indications de colonnes suivantes :

1. ***L'actif traite des données cliniques*** : les données cliniques sont tous les types de données de nature médicale ou en rapport avec la santé d'un patient.
2. ***L'actif traite des données personnelles*** : les données personnelles sont tous les types de données permettant d'identifier un individu, un employé ou un patient.
3. ***L'actif traite des données RH (ressources humaines)*** : les données RH sont tous les types de données attachés à un employé d'un établissement de santé.
4. ***L'actif traite des données financières ou d'une autre nature*** : les données sont de type financier d'un établissement de santé ou tout autre type de données qui ne relève pas des catégories précédentes.

Pour la grille sécurité seulement, une cinquième colonne (#5) ajoute certains critères concernant l'hébergement de l'application en mode « fournisseur d'applications hébergées » à l'extérieur du RITM et chez un tiers commercial. Ces critères s'appliquent si l'application ne réside pas à l'intérieur d'un établissement du MSSS.

Volet PRP

Définitions :

- Projet : Applicatif ou service fourni.
- Service : Projet hébergé dans un environnement externe au MSSS, service de support sur place, ou offre de services de téléassistance (via connexion par poste distant par exemple).

Référence :

- http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html
- http://www.cai.gouv.qc.ca/documents/CAI_G_dev_syst_info_pub.pdf

Note : La mention « Vrai » dans la colonne indique que le critère s'applique dans cette situation. La mention « Faux » indique que le critère ne devrait pas s'appliquer.

	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	
No.					**Libellé du Critère**
1					**Assumer ses responsabilités face aux renseignements personnels**
					Contexte (articles 8 et 59) : Chaque organisme public a la responsabilité d'assurer le caractère confidentiel des renseignements personnels qu'il détient. D'office, la loi va même jusqu'à conférer les fonctions de protection des renseignements personnels à la personne ayant la plus haute autorité au sein de votre organisme. Votre organisme dispose d'une somme de renseignements personnels qui constituent un capital informationnel à haut risque. Toute fuite ou tout mauvais usage de ceux-ci risque de porter atteinte à leur intégrité et à leur confidentialité, en plus de nuire à la personne concernée. Pour contrer cette éventualité, des mesures de protection adéquates doivent être implantées, lesquelles supposent l'adoption et l'application de politiques de confidentialité évolutives et en constant raffinement. À cette fin, le responsable de la protection des renseignements personnels joue un rôle prépondérant dans la promotion et l'application des dispositions de la Loi sur l'accès au sein de votre organisme, appuyé dans sa démarche par ceux et celles qui recueillent, conservent, communiquent, traitent ou détruisent ces renseignements.
P01001	VRAI	FAUX	FAUX	FAUX	Les outils et le support sont en place pour permettre les analyses de risques axés spécifiquement sur la protection des renseignements personnels.
P01002	VRAI	FAUX	FAUX	FAUX	Le responsable de la protection des renseignements personnels de votre organisme est mis à contribution dans le développement de votre projet.
P01003	VRAI	FAUX	FAUX	FAUX	La protection des renseignements personnels est encadrée au sein de votre organisme par des politiques, directives, normes, procédures et autres instructions (accès distant, messagerie électronique, Internet, etc.). Vous êtes en mesure de dresser la liste des documents pertinents et d'indiquer la date de leur dernière révision.
P01004	VRAI	FAUX	FAUX	FAUX	Votre organisme dispose d'une politique de confidentialité.

	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	
No.					**Libellé du Critère**
P01005	VRAI	FAUX	FAUX	FAUX	Le personnel de votre organisme est sensibilisé et formé à la protection des renseignements personnels. Votre organisme dispose d'un programme de formation et de sensibilisation à la confidentialité explicitant les responsabilités de l'organisme, ses obligations, les règles d'éthique au travail, etc.
P01006	VRAI	FAUX	FAUX	FAUX	Votre organisme s'acquitte de ses obligations à l'égard des renseignements personnels en mettant à la disposition de son personnel les mécanismes de protection requis.
P01007	VRAI	FAUX	FAUX	FAUX	Si des tierces parties interviennent dans le projet, elles respectent les mêmes exigences de confidentialité que celles qui prévalent au sein de votre organisme.
P01008	VRAI	FAUX	FAUX	FAUX	Votre projet comporte des mécanismes en vue de gérer les plaintes ou les questions relatives à la protection des renseignements personnels.
2					**Déterminer les fins de la collecte de renseignements personnels**
					Contexte (article 64) : Avant d'entreprendre toute collecte d'information, vous devez définir les raisons pour lesquelles vous comptez recueillir et utiliser un renseignement personnel. Ces motifs doivent être en accord avec les mandats, attributions et programmes relevant de votre organisme. La mise en œuvre de ce principe constitue un préalable incontournable à l'application des autres principes. L'obligation d'identifier les raisons qui conduisent à une collecte de renseignements personnels permettra par la suite : • de délimiter le type et le nombre de renseignements personnels à recueillir; • d'informer la personne concernée des raisons qui justifient la collecte de renseignements; • de déterminer la fréquence de leur mise à jour; • de limiter leur utilisation; • de fixer, à terme, le moment de leur destruction.
P02001	VRAI	FAUX	FAUX	FAUX	Les dispositions particulières des lois, règlements ou programmes légitimant votre collecte de renseignements personnels sont identifiées et les outils sont en place pour permettre leurs respects lors du déploiement et de l'opération de votre projet.
P02002	VRAI	FAUX	FAUX	FAUX	Vous destinez chaque renseignement personnel à un usage déterminé et vous reliez cet usage aux fonctionnalités ou services offerts par votre projet.
P02003	VRAI	FAUX	FAUX	FAUX	Chaque renseignement personnel est utilisé pour une finalité autorisée.
P02004	VRAI	FAUX	FAUX	FAUX	Chaque fichier de renseignements personnels est créé ou maintenu pour une finalité autorisée.
P02005	VRAI	FAUX	FAUX	FAUX	Si vous confiez la collecte des renseignements personnels à une tierce partie externe à votre organisme, vous vous assurez que ce tiers respectera les fins de collecte établies.

	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	
No.					**Libellé du Critère**
P02006	VRAI	FAUX	FAUX	FAUX	Si votre projet constitue une refonte de systèmes existants, vous vous assurez que : • la finalité de chacun des systèmes antérieurs soit connue; • le nouveau système reconduise la finalité des systèmes antérieurs; • toute collecte d'information additionnelle respecte la finalité des systèmes antérieurs.
P02008	VRAI	FAUX	FAUX	FAUX	Si vous créez un entrepôt de données à partir notamment de fichiers de renseignements personnels, vous vous assurez de respecter le cloisonnement des fichiers qui comportent des finalités distinctes.
P02009	VRAI	FAUX	FAUX	FAUX	En complément au critère P02003, il est sous-entendu que l'utilisation secondaire des données est aussi couverte par la protection des renseignements personnels. Ainsi, un fournisseur ne peut créer, exporter, conserver et/ou distribuer des informations (même si les données sont anonymisées, résultats d'analyses statistiques ou sous forme de mégadonnées) obtenues à partir des données personnelles des patients. Le terme « utilisation secondaire » désigne « l'utilisation des renseignements sur la santé à toute autre fin que la prestation de soins et de traitement directs ».
3					**Limiter la collecte de renseignements personnels**
					Contexte (article 65) : Vous ne pouvez recueillir que les seuls renseignements personnels nécessaires à l'exercice des attributions de votre organisme ou à la mise en œuvre d'un programme dont il a la gestion. Il vous incombe de démontrer explicitement en quoi les renseignements visés par la collecte revêtent un caractère indispensable. Votre regard doit porter ici sur le type et le nombre des renseignements personnels colligés. Vous devez justifier la nécessité de les recueillir, interroger leur provenance, anticiper les conséquences de leur détention, etc.
P03001	VRAI	FAUX	FAUX	FAUX	Les renseignements personnels recueillis par le projet sont indispensables à l'exercice des attributions de l'organisme acquéreur ou à sa mise en œuvre d'un programme dont il a la gestion.
P03002	VRAI	FAUX	FAUX	FAUX	Les fins visées par la collecte ne peuvent être atteintes sans l'obtention de chacun des renseignements personnels.
P03003	VRAI	FAUX	FAUX	FAUX	Les actions, décisions ou recommandations qui découlent des renseignements personnels recueillis sont documentées, facilement accessibles et communiquées à l'acquéreur.
P03004	VRAI	FAUX	FAUX	FAUX	La quantité de renseignements personnels à recueillir ne peut être réduite sans compromettre la finalité du fichier qui les contient.
P03005	VRAI	FAUX	FAUX	FAUX	La lise des fichiers où sont versés les renseignements personnels recueillis, y compris ceux contenant des données de journalisation ou de surveillance, est documentée et disponible.
P03006	VRAI	FAUX	FAUX	FAUX	Les recours à des identifiants généraux, tels le numéro d'assurance sociale, le numéro d'assurance maladie, le numéro de permis de conduire, le certificat d'identité électronique ou autre, sont recueillis en vertu de dispositions légales ou d'ententes spécifiques, et l'acquéreur est informé de ceux-ci.

No.	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	Libellé du Critère
P03007	VRAI	FAUX	FAUX	FAUX	Des outils doivent permettre à l'acquéreur d'identifier, d'autoriser, de justifier et de tracer les renseignements personnels fournis par l'intermédiaire de tierces personnes. Entre autres ou à titre d'exemple, l'outil devrait demander une confirmation ou une justification de l'impossibilité de les obtenir directement de la personne concernée.
P03008	VRAI	FAUX	FAUX	FAUX	Lors de la collecte de renseignements personnels, des outils doivent être fournis par le projet pour permettre de valider avec une assurance suffisante l'identité de la personne concernée, qu'elle soit physiquement présente ou non, sans pour autant recueillir ou permettre la communication de renseignements additionnels.
P03009	VRAI	FAUX	FAUX	FAUX	Si le projet recueille de l'information sur le poste informatique des internautes (témoins ou cookies, fichiers temporaires, pixels invisibles ou bogues web, etc.), vous êtes en mesure d'en démontrer la nécessité.
4					**Informer la personne concernée**
					Contexte (article 65) : Vous avez l'obligation d'informer adéquatement la personne concernée avant qu'elle vous fournisse les renseignements personnels attendus. Vous devez faire preuve de transparence à son égard en lui communiquant les raisons de la collecte et les traitements accordés aux informations demandées. Quel que soit le moyen technologique par lequel vous comptez joindre les personnes concernées, votre choix doit faire en sorte que toutes reçoivent facilement une information compréhensible. Le recours accentué aux applications web comme outils de collecte d'information ne vous soustrait pas à l'obligation d'expliquer clairement les raisons de votre démarche. Au contraire, il requiert que vous communiquiez à vos informateurs les risques associés à la transmission de renseignements sensibles sur le réseau Internet et vous oblige à de nouvelles précautions en matière de sécurité – l'authentification des parties dans la communication, l'intégrité des renseignements communiqués, la validité des consentements électroniques, etc. Article 65 : Quiconque, au nom d'un organisme public, recueille un renseignement nominatif auprès de la personne concernée ou d'un tiers doit au préalable s'identifier et l'informer : 1. du nom et de l'adresse de l'organisme public au nom de qui la collecte est faite; 2. de l'usage auquel ce renseignement est destiné; 3. des catégories de personnes qui auront accès à ce renseignement; 4. du caractère obligatoire ou facultatif de la demande; 5. des conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande; 6. des droits d'accès et de rectification prévus par la loi.

No.	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	Libellé du Critère
					Toutefois, une personne dûment autorisée par un organisme public qui détient des dossiers ayant trait à l'adoption de personnes et qui recueille un renseignement relatif aux antécédents d'une personne visée dans l'un de ces dossiers ou permettant de retrouver un parent ou une personne adoptée, n'est pas tenue d'informer la personne concernée ou le tiers de l'usage auquel est destiné le renseignement ni des catégories de personnes qui y auront accès. Les règles suivant lesquelles la collecte de renseignements nominatifs doit être faite sont prescrites par règlement du gouvernement. Le présent article ne s'applique pas à une enquête de nature judiciaire, ni à une enquête ou à un constat fait par une personne qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois.
P04001	VRAI	FAUX	FAUX	FAUX	Lors du déploiement ou de la formation, vous informez l'acquéreur de ses responsabilités en regard aux éléments prévus à l'article 65 de la Loi sur l'accès, en prenant soin d'utiliser des termes simples et usuels.
P04003	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir les outils pour permettre à une personne concernée d'accéder ou rectifier un renseignement personnel la concernant.
P04004	VRAI	FAUX	FAUX	FAUX	Le projet doit demander une autorisation avant de permettre la collecte par un intermédiaire mandataire. Cette autorisation doit permettre de valider que l'intermédiaire maintient les obligations de l'acquéreur relativement à l'article 65 de la Loi sur l'accès.
P04005	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir un outil pour conserver que l'acquéreur a informé la personne concernée que ses renseignements personnels ne seront utilisés que pour l'usage projeté et les finalités recherchées.
P04006	VRAI	FAUX	FAUX	FAUX	Si le projet recueille des renseignements personnels par le biais d'un formulaire électronique ou d'un autre document comparable, les informations requises par l'article 65 y sont prioritairement et préalablement affichées à toute collecte de renseignements personnels.
P04007	VRAI	FAUX	FAUX	FAUX	Le projet avise clairement les internautes de l'usage fait des témoins (cookies) et autres traitements similaires effectués à leur insu, en indiquant quelles informations sont recueillies. Cet avis doit utiliser un langage simple et usuel.
P04008	VRAI	FAUX	FAUX	FAUX	Par l'entremise de son site web, le fournisseur affiche de manière évidente le contenu de sa politique de confidentialité. L'acquéreur devrait être invité à faire référence ou intégrer cette politique à son site web.
5					**Limiter l'accès aux renseignements personnels**
					Contexte (articles 62 et 76) : La loi prévoit qu'un renseignement personnel ne sera accessible qu'aux seules personnes ayant la qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de leurs fonctions. Partant du fait qu'un renseignement personnel est confidentiel, il vous revient d'élaborer les mécanismes internes appropries afin d'éviter que tous aient accès sans restriction à l'ensemble des renseignements disponibles.

No.	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	Libellé du Critère
					Vous devez déterminer quels renseignements sont jugés indispensables au regard des taches et des fonctions à accomplir par chaque membre de votre personnel. Ces privilèges d'accès sont identifiés de façon conjointe par les autorités, les gestionnaires et les ressources humaines en fonction des renseignements et des dossiers spécifiques auxquels chaque employé doit référer dans l'exécution de ses tâches. Rappelons que la nécessité d'accès vise à éviter que des personnes, étant par ailleurs habilitées à prendre connaissance d'un renseignement personnel, ne le fassent à titre gratuit ou par simple curiosité. En se rappelant que... 1. En dépit du mouvement de concentration des traitements et des données qui s'opère au sein des organisations publiques, la gestion des renseignements personnels ne doit pas s'opposer à l'idée du cloisonnement de l'information qui sous-tend la Loi sur l'accès comme moyen privilégié de garantir la confidentialité des renseignements personnels. 2. Une utilisation conséquente des technologies de l'information doit, par le biais d'une analyse de risques, contrôler la facilité avec laquelle elles permettent la dissémination, la duplication ou le partage des renseignements personnels, multipliant par le fait même les probabilités d'accès non autorisés aux données confidentielles, les risques de mauvais usages, de fuites ou de péremption de l'information.
P05001	VRAI	FAUX	FAUX	FAUX	Vous inscrivez dans *l'inventaire* de fichier correspondant aux catégories d'employés (médecins, personnels soignants, agents de bureau, agents de recherche, conseillers, analystes en informatique, etc.) qui doivent recourir aux renseignements personnels.
P05002	VRAI	FAUX	FAUX	FAUX	La documentation doit informer des mandats, tâches ou fonctions accomplis par ces catégories d'emploi au sein de l'organisme et les justifications qui rendent indispensable l'utilisation de chaque renseignement personnel.
P05003	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir des outils pour permettre de gérer ou visualiser la fréquence d'utilisation des renseignements personnels correspondant aux mandats attribués à ces catégories d'employés.
P05004	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir des outils pour gérer ou restreindre dans le temps aux seuls moments requis l'accès aux renseignements personnels.
P05005	VRAI	FAUX	FAUX	FAUX	Le projet doit limiter la portée des privilèges d'accès (lecture, écriture, suppression, etc.) selon la définition de tâches des employés.
P05006	VRAI	FAUX	FAUX	FAUX	Les renseignements personnels destinés à des fins d'usage interne à votre entreprise (voir PO2008) ne sont accessibles qu'aux seules personnes ayant la qualité pour les recevoir, au moment où ces renseignements leur sont nécessaires.
P05007	VRAI	FAUX	FAUX	FAUX	Vous construisez des jeux de données fictives ou anonymes lors de la formation des nouveaux employés.
P05008	VRAI	FAUX	FAUX	FAUX	Vous construisez des jeux de données fictives ou anonymes dans les environnements de développement (unitaire, fonctionnel, intégration, etc.) ou d'entretien d'un système.

	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	
No.					**Libellé du Critère**
P05009	VRAI	FAUX	FAUX	FAUX	Vous imposez aux informaticiens (administrateurs de réseau, administrateurs de base de données, libraires, etc.) un accès limité aux stricts renseignements personnels nécessaires.
P05010	VRAI	VRAI	VRAI	VRAI	Des clauses spécifiques dans le contrat entre le fournisseur et ses employées, le contrat entre le fournisseur et des tiers, ainsi que dans le contrat entre le fournisseur et ses clients, prévoient la protection des renseignements personnels et la confidentialité.
6					**Requérir le consentement à la communication entre organismes publics**
					Contexte (articles 53 et 59) : Un renseignement personnel demeure inaccessible tant que la personne concernée n'a pas consenti à sa divulgation(*). Par conséquent, seuls les organismes que la personne concernée autorise auront accès à ses renseignements personnels. Le consentement concerne strictement la communication de renseignements personnels; il doit être formulé de manière manifeste, libre, éclairée, spécifique, limitée dans le temps et peut être résilié à tout moment. Le droit à la vie privée sous-entend qu'une personne dispose d'un certain contrôle sur la circulation des renseignements la concernant. Vous devez donc vous assurer qu'une information personnelle ne pourra circuler sans l'autorisation préalable de la personne concernée, en évaluant notamment les moyens par lesquels vous obtenez ce consentement, les limites que vous lui attribuez et l'usage que vous en faites. En se rappelant que... 1. Le consentement à la communication vient autoriser la circulation d'un renseignement personnel entre organismes publics dans la mesure où ce renseignement est nécessaire aux attributions de ces organismes ou à la mise en œuvre d'un programme dont ils ont la gestion. 2. Les principes reprennent à leur manière l'idée que la dispersion des renseignements personnels et le cloisonnement administratif des organismes détenant ces mêmes renseignements représentent les meilleurs gages de confidentialité. Cloisonnement et dispersion évitent que des profils sur les individus ne puissent être dressés par l'État et constituer ainsi une réelle menace à la reconnaissance des droits des individus. Le recours obligatoire au consentement à la communication doit être perçu comme un contrôle favorisant non pas la propagation des renseignements personnels, mais bien le maintien de leur répartition. * Certaines exceptions précisées par la Loi sur l'accès autorisent la communication de renseignements personnels sans le consentement préalable des personnes concernées (voir les articles 59, 59.1, 67, 67.1, 67.2, 68 et 68.1).

	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	
No.					**Libellé du Critère**
P06001	VRAI	FAUX	FAUX	FAUX	Considérant que le consentement à la communication des personnes concernées est : • Manifeste — attesté par un document (technologique ou papier); • Libre — exprimé sans conditions, contraintes, menaces ou promesses; • Éclairé — formulé en ayant conscience de sa portée; • Spécifique — autorisant la communication d'un renseignement personnel donné, à des personnes données, à des fins données et à un moment donné; • Limité dans le temps — valide pour la durée requise à la réalisation des fins pour lesquelles il est demandé. Le projet doit offrir des outils pour : • conserver l'attestation du consentement par la personne concernée; • permettre de spécifier les personnes ou organismes où seront communiqués les renseignements; • permettre de définir une durée de validité; • permettre à la personne concernée de révoquer en tout temps les communications.
P06002	VRAI	FAUX	FAUX	FAUX	Le projet doit identifier les différentes façons d'obtenir le consentement à la communication auprès de la personne concernée : en sa présence, par Internet, par la poste ou par d'autres voies.
P06003	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir les outils pour confirmer que le consentement à la communication provient directement de la personne concernée.
P06004	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir les outils pour consigner les preuves de consentement à la communication et les échanger entre parties communicantes.
P06007	VRAI	FAUX	FAUX	FAUX	Le projet doit fournir les outils pour déterminer ou gérer les circonstances et la manière de communiquer un renseignement personnel à un autre organisme.
P06008	VRAI	FAUX	FAUX	FAUX	Si le projet a recours à des services externes pour la gestion spécifique de renseignements personnels, vous vous assurez que la protection des renseignements personnels chez ce prestataire de services répondra aux exigences de l'acquéreur, qu'il y ait ou non communication de renseignements au sens de l'article 67.2 de la Loi sur l'accès.
P06009	VRAI	FAUX	FAUX	FAUX	Le projet doit consigner (et permettre d'identifier) toutes les communications de renseignements personnels sans consentement, incluant celles effectuées dans le cadre de mandats à l'externe et pour lesquels une entente écrite précise les dispositions légales et les mesures qui s'appliquent aux renseignements personnels communiqués (article 67.2).

	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	
No.					**Libellé du Critère**
7					**Assurer la qualité des renseignements personnels**
					Contexte (article 72) : Un renseignement personnel doit être maintenu à jour, être exact et complet afin de servir adéquatement aux fins pour lesquelles il a été recueilli. Vous devez donc identifier préalablement les renseignements personnels devant être mis à jour et consigner par la suite les dernières dates auxquelles ils auront été rectifiés. De cette manière, les renseignements personnels évolueront tout au long de leur cycle de vie conformément à la situation des personnes concernées. Du fait des décisions que vous êtes appelés à prendre au sujet des personnes, il importe que la détention de renseignements personnels au sein de votre organisme respecte certaines obligations particulières. En outre, la collecte de tout nouveau renseignement personnel, rendue nécessaire pour des raisons de mise à jour, doit être conforme au principe sur la limitation de la collecte énoncée antérieurement.
P07001	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir les outils pour déterminer depuis combien de temps chaque renseignement personnel a été recueilli.
P07002	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir les outils pour déterminer la fréquence d'utilisation de chaque renseignement personnel.
P07003	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir les outils pour identifier les renseignements personnels qui nécessitent une mise à jour.
P07004	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir les outils pour établir des mécanismes pour gérer les mises à jour d'un renseignement personnel au cours de son cycle de vie.
P07005	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir les outils pour établir des mécanismes pour gérer les mises à jour d'un renseignement personnel dupliqué ou répliqué (p. ex. sites miroirs).
P07006	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir les outils pour déterminer la fréquence des mises à jour des renseignements personnels basée sur leur fréquence d'utilisation (p. ex. un traitement annuel unique ne justifierait pas a priori des mises à jour mensuelles).
P07007	VRAI	FAUX	FAUX	FAUX	Le projet doit permettre la mise à jour d'un renseignement personnel à des d'employés possédant les privilèges d'accès appropriés.
P07008	VRAI	FAUX	FAUX	FAUX	Des outils doivent permettre à l'acquéreur d'identifier, d'autoriser, de justifier et de tracer les mises à jour par échange de renseignements personnels sans consentement, préalablement autorisées par la Commission (par des ententes ou par des dispositions légales particulières).
P07009	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir les outils pour confirmer qu'une demande de modification d'un renseignement personnel proviendra bien de la personne concernée.

	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	
No.					**Libellé du Critère**
8					**Garantir la sécurité des renseignements personnels**
					Contexte (articles 53, 69 et 76) : Des mesures de protection appropriées doivent assurer efficacement la sécurité d'un renseignement personnel, autant lors de sa mise en circulation que pendant toute la durée de sa détention. Vous devez préserver simultanément la confidentialité, la disponibilité et l'intégrité d'un renseignement personnel par le biais de moyens proportionnels aux conséquences possibles de sa divulgation. Protection des renseignements personnels et sécurité informatique ne s'avèrent pas synonymes. D'une part, si certaines mesures de sécurité contribuent au respect de la confidentialité, d'autres en revanche constituent de véritables intrusions dans la vie privée des personnes. Il vous revient de déterminer au préalable si les contrôles que vous envisagez s'accordent avec le droit à la vie privée des utilisateurs. D'autre part, une mesure de sécurité efficace peut être insuffisante pour assurer la protection des renseignements personnels. Une transmission électronique, par exemple, peut être sécurisée de façon à préserver le caractère confidentiel de son contenu, mais être acheminée à une personne non autorisée à accéder aux renseignements qui y figurent. D'où le besoin d'évaluer la pertinence et l'efficacité des moyens de sécurité mis en œuvre afin de réserver aux renseignements personnels un usage qui respecte la finalité de leur collecte. En se rappelant que... 1. Le cryptage ou chiffrement constitue une mesure de sécurité particulière pour préserver temporairement la confidentialité d'un renseignement personnel durant sa transmission ou son entreposage. Un renseignement personnel crypté demeure confidentiel du fait que sa transformation reste passagère et réversible. 2. Un fichier ne peut être qualifié d'anonyme lorsqu'il est possible par un moyen ou un autre d'identifier une personne, lorsqu'un moyen de déduction logique permet de reconstituer une identité à partir de plusieurs renseignements anonymes, lorsque le mécanisme d'anonymisation est réversible ou lorsqu'un pseudonyme remplace un identifiant. Faute d'anonymat, les obligations de protection conférées par la loi aux renseignements personnels demeurent applicables.
P08001	VRAI	FAUX	FAUX	FAUX	Pour tous les types de services offerts par le projet : Vous établissez des mesures de sécurité applicables tout au long du cycle de vie d'un renseignement personnel, de sa collecte à sa destruction en passant par ses différentes utilisations. À titre indicatif : • Mesures physiques : contrôles d'accès aux salles de serveurs, aux ordinateurs de support, aux salles de câblage, au système d'alarme, etc. • Mesures technologiques : identifiants et mots de passe, chiffrement, coupe-feu, anonymisation, pseudonymisation, etc. • Mesures administratives : autorisations sécuritaires, accès sélectif, formation des employés, ententes de non-divulgation, etc.

	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	
No.					**Libellé du Critère**
P08002	VRAI	FAUX	FAUX	FAUX	Tous les membres de votre personnel pouvant accéder aux renseignements personnels doivent être informés de façon complète et non ambiguë des mesures de surveillance et de contrôle dont ils font l'objet et vous leur indiquez l'identité des personnes autorisées à accéder aux informations issues de ces mesures, en précisant les circonstances dans lesquelles elles y accèderont.
P08003	VRAI	FAUX	FAUX	FAUX	La documentation du service doit être en mesure d'expliquer les mesures de sécurité inhérentes à votre prestation électronique de services en regard des risques encourus par les renseignements personnels.
P08004	VRAI	FAUX	FAUX	FAUX	Des mesures de contrôle a priori touchant l'accès aux fichiers informatisés contenant des renseignements personnels sont en place.
P08005	VRAI	FAUX	FAUX	FAUX	Les accès à distance pouvant conduire à l'accès à des renseignements personnels sont gérés et contrôlés.
P08006	VRAI	FAUX	FAUX	FAUX	L'information sur les renseignements personnels qui circule par le biais des ordinateurs portables de votre personnel est gérée et contrôlée.
P08007	VRAI	FAUX	FAUX	FAUX	Vous contrôlez par des mesures particulières la sécurité des extrants : extractions, copies, impressions, copies de sécurité, notes personnelles.
P08008	VRAI	FAUX	FAUX	FAUX	Le projet crypte d'une manière sûre les renseignements personnels qui doivent être communiqués.
P08009	VRAI	FAUX	FAUX	FAUX	Si le projet requiert une identification à distance, votre procédé d'authentification vous permet de valider avec une assurance suffisante l'identité de la personne avec qui vous communiquez, ainsi que la validité de l'instance d'authentification considérant la sensibilité des renseignements personnels engagés tout au long de la communication.
P08010	VRAI	FAUX	FAUX	FAUX	Le projet comporte des mécanismes garantissant l'intégrité des renseignements personnels communiqués.
P08011	VRAI	FAUX	FAUX	FAUX	Vous vous assurez que tout prestataire de services agissant à titre d'intermédiaire dans une communication de renseignements personnels fournira un niveau de sécurité égal ou supérieur au vôtre à l'égard des supports, de la technologie et du lieu d'entreposage des renseignements personnels.
P08012	VRAI	FAUX	FAUX	FAUX	Le projet journalise tous les accès aux renseignements personnels afin d'être en mesure d'identifier, si nécessaire, quels utilisateurs y ont eu accès pendant une période déterminée. Des mécanismes de contrôle rigoureux pour l'accès aux fichiers de journalisation sont en place pour en garantir l'intégrité et l'inviolabilité.
P08013	VRAI	FAUX	FAUX	FAUX	Lors de prestation de services (hébergement, téléassistance, etc.), vous analysez les fichiers de journalisation de manière anonyme et à intervalles réguliers, en vous souciant d'ajuster et de varier les critères d'analyse.
P08014	VRAI	FAUX	FAUX	FAUX	Vous vous parez aux cyberattaques provenant tant de l'interne que de l'externe autant dans vos infrastructures de développements que de services.

	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	
No.					**Libellé du Critère**
P08015	VRAI	FAUX	FAUX	FAUX	Pour toutes les prestations de services, l'information sur les patients devant être protégé par les lois de la province en matière de confidentialité peut être conservée conformément aux lois et aux lignes directrices du Collège des médecins du Québec.
P08016	VRAI	FAUX	FAUX	FAUX	Le fournisseur d'application doit s'assurer que tous les tiers impliqués dans la conservation des renseignements personnels soient au Canada et soumis aux lois canadiennes, et inclure cette garantie dans une clause du contrat signé avec ses fournisseurs et ses clients. En particulier les centres de traitement et d'hébergement, les centres de relève en cas de sinistre, et les entreprises qui entreposent les copies de sauvegarde. A priori, une solution basée sur une approche infonuagique n'est pas admissible. Cependant, si un fournisseur peut démontrer que dans l'approche infonuagique proposée les données sont hébergées dans des centres de traitement au Canada que l'ensemble des données hébergées ou en transits sont cryptées et que les meilleures pratiques de gestion de centre de traitement sont appliquées, le service pourra être considéré acceptable. Dans le cadre du chiffrement des données, le fournisseur doit démontrer qu'il utilise les meilleures pratiques de l'industrie et que les clés de chiffrement sont rangées dans des modules cryptographiques FIPS 140-2 level 3 qui sont en permanence sous le contrôle du fournisseur.
9					**Assurer les droits d'accès et de rectification**
					Contexte (articles 83, 84 et 89) : Un renseignement personnel doit pouvoir être accessible et rectifié. Vous devez informer toute personne qui en fait la requête de l'existence des renseignements personnels qui la concernent et de la possibilité de les consulter ou d'en obtenir copie, quel que soit le support. Vous devez identifier quels dispositifs ont été prévus pour répondre adéquatement aux demandes formulées par les personnes concernées relativement à l'accès aux renseignements personnels, de même qu'à leur rectification.
P09001	VRAI	FAUX	FAUX	FAUX	Le projet doit offrir des outils pour rendre facilement accessibles à une personne tous les renseignements personnels la concernant, de façon à lui permettre de les consulter et de les corriger dans la mesure prévue par la loi.
P09002	VRAI	FAUX	FAUX	FAUX	Si les demandes peuvent être effectuées à distance par la personne concernée, le projet offre des mécanismes pour efficacement valider l'identité du requérant.
P09003	VRAI	FAUX	FAUX	FAUX	Le projet peut rendre disponibles les renseignements personnels sur des supports facilitant leur obtention (papier ou technologique).
P09004	VRAI	FAUX	FAUX	FAUX	Le projet s'assure de propager dans les fichiers concernés (p. ex. dupliqua) toute rectification apportée à un renseignement personnel.

No.	1-L'actif traite des données cliniques.	2- L'actif traite de données personnelles	3- L'actif traite des données RH (ressources humaines).	4- L'actif traite de tout autre type de données	Libellé du Critère
10					**Limiter la durée de conservation des renseignements personnels**
					Contexte (articles 73 et 102.1) : Vous êtes tenus de détruire irréversiblement tout renseignement personnel lorsque l'objet pour lequel il a été recueilli est accompli. Cette obligation, qui vise à réduire la probabilité que des renseignements personnels soient utilisés à des fins autres que celles auxquelles ils étaient destinés, est assortie d'une réserve importante : la Loi sur les archives, et plus précisément, le calendrier de conservation de l'organisme. Un organisme ne peut conserver les renseignements personnels qu'il détient au-delà des délais prescrits par le calendrier de conservation, quel que soit le support utilisé. Vos échéances de conservation doivent tenir compte des demandes d'accès que pourrait invoquer la personne concernée à la suite des décisions prises à son sujet, mais se limiter cependant au strict intervalle de temps requis pour que le renseignement personnel puisse jouer le rôle auquel il est destiné.
P10001	VRAI	FAUX	FAUX	FAUX	Le projet permet de fixer un calendrier de conservation à tous les renseignements personnels qu'il détient, quels que soient leurs supports.
P10002	VRAI	FAUX	FAUX	FAUX	La destruction d'un renseignement personnel par le projet entraîne celle de toutes ses copies.
P10003	VRAI	FAUX	FAUX	FAUX	La destruction des renseignements personnels est effectuée de manière irréversible.
P10004	VRAI	FAUX	FAUX	FAUX	Même si les renseignements personnels sont versés dans un fichier de conservation distinct (p. ex. un entrepôt de données), vous les soumettez à un calendrier de conservation et les détruisez à terme.
P10005	VRAI	FAUX	FAUX	FAUX	Durant leur conservation, le projet préserve les renseignements personnels de façon anonyme ou masqués par un pseudonyme pour mieux en préserver la confidentialité.

Volet Sécurité

Note : La mention « Vrai » dans la colonne indique que le critère s'applique dans cette situation. La mention « Faux » indique que le critère ne devrait pas s'appliquer.

	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	
No.						**Libellé du critère**
3 Gestion de l'exploitation et de télécommunication						
3.1.1 Procédures d'exploitation documentées						
S03001	FAUX	FAUX	FAUX	FAUX	VRAI	Un guide de l'utilisateur ou une aide contextuelle DOIT être disponible. Cette documentation DOIT être suffisante pour permettre à un utilisateur ou à un pilote de bien comprendre les éléments nécessaires à l'utilisation du système d'information.
S03057	FAUX	FAUX	FAUX	FAUX	VRAI	Lorsque le système est offert en mode « fournisseur d'applications hébergées », un guide d'opération DOIT être disponible. Ce guide doit détailler, entre autres, les éléments suivants : • Description de la configuration des postes de travail typique du système d'information pour un déploiement sécuritaire. • Configuration des privilèges (répertoires, bases de données, etc.). • Configuration de sécurité du navigateur si des éléments particuliers doivent être modifiés à ce niveau. • Foires aux questions. • Limitations connues (IE v5+…).
S03003.b	FAUX	FAUX	FAUX	FAUX	VRAI	Une liste complète des équipements requis DOIT être disponible. Il faut indiquer les exigences matérielles minimales et optimales pour chacun des composants du système d'information : • Poste client. • Routeur. • Service internet. • Etc.
S03004	FAUX	FAUX	FAUX	FAUX	VRAI	Une architecture de déploiement détaillée DOIT être produite pour démontrer la redondance matérielle et logicielle ainsi que les calculs et les hypothèses permettant de démontrer que le système peut être disponible à 99,999 %. Note : Une évaluation indépendante par un organisme reconnu par le MSSS pourrait être souhaitable en cas de doute.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
3.1.2 Gestion des modifications						
S03005	FAUX	FAUX	FAUX	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre d'identifier la version du système d'information utilisée. Une méthode fréquente est l'utilisation d'un menu contextuel « Aide --> À propos de ».
S03006	FAUX	FAUX	FAUX	FAUX	VRAI	Un document d'architecture détaillée du système d'information et de ses composantes DOIT être disponible.
3.1.3 Séparation des tâches						
S03009	FAUX	FAUX	FAUX	FAUX	VRAI	Un utilisateur non authentifié (anonyme) NE DOIT PAS être en mesure de créer et d'activer lui-même son compte utilisateur.
S03010	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT fournir un module de pilotage. Note : Il est recommandé que ce module de pilotage soit totalement indépendant du système d'information plutôt que d'effectuer l'affichage ou non des fonctionnalités de pilotage selon les privilèges de l'utilisateur en cours.
S03011	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT être suffisamment modulaire pour permettre d'assurer la séparation des tâches. Par exemple, le système d'information DOIT permettre d'assurer que le pilote ne possède pas les mêmes privilèges qu'un administrateur du ou des serveurs. Également, comme il est mentionné dans la section « Procédures d'exploitation documentées », le guide d'opération DOIT expliquer la configuration des privilèges. Note : Cette séparation des tâches prévient un utilisateur mal intentionné de supprimer toutes les traces de ses actions.
S03013	FAUX	FAUX	FAUX	FAUX	VRAI	Le compte pilote NE DOIT PAS être considéré comme un utilisateur normal dans le système d'information. Exemples : • Le compte pilote DOIT seulement permettre de configurer des options reliées à la gestion du système d'information telles que l'ajout, la modification ou la suppression d'un identifiant ou à la gestion des configurations relatives à la sécurité telles que la journalisation, les mots de passe complexes exigés, etc. • Un compte utilisateur DOIT uniquement être en mesure d'effectuer des transactions tel un utilisateur.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
3.1.4 Séparation des équipements de développement, de test et d'exploitation						
S03014	FAUX	FAUX	FAUX	FAUX	VRAI	Une fonctionnalité DOIT permettre d'indiquer si le système d'information est dans un environnement de production ou dans un autre environnement. Exemples : Une variable de configuration, champ de BD, portion d'URL, etc. : • Il est possible d'indiquer l'environnement mentionné dans la barre de titre. • Il est possible de modifier les couleurs, permettant ainsi de distinguer un environnement de production d'un autre.
3.2 Prestation de service						
S03060	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT permettre d'effectuer le support à distance en utilisant les services communs en place. La description des outils ainsi que le mode de communication DEVRAIENT être inclus dans les contrats de service. Voici la liste des exigences du logiciel de support. Celui-ci doit être évalué en rapport à la fonctionnalité de support à distance et non aux autres fonctionnalités disponibles dans l'outil. • Authentification sécurisée. • Autorisation de la session par l'utilisateur « hôte » (aucun mécanisme d'accès sans supervision), voir critère S03016. • Possibilité pour l'utilisateur « hôte » d'arrêter une session. • LOGIN de contexte non limité au login de l'utilisateur « hôte » (le fournisseur doit s'identifier avant de pouvoir utiliser l'outil de support à distance). • Profile d'accès du personnel de support : différents mots de passe, permission granulaire (aucun compte générique, un compte pour chaque membre du personnel au support). • Changement forcé du mot de passe, soit par le système d'exploitation (OS) ou l'outil. • Journalisation des interventions et des accès à ces journaux. • Chiffrement des communications à l'intérieur ou à l'extérieur du RITM. • Passage sécuritaire à travers un ou des routeurs et un ou des coupe-feu (identification du port utilisé par l'outil, aucun requis de configuration particulière du réseau pour l'acquéreur). • La version utilisée ne doit pas avoir de vulnérabilité déclarée sur les bases de données CERT/CC et SANS institute. De plus, veuillez noter que tous les fournisseurs doivent toujours utiliser la méthode du « jeton » ou du « service F » afin de se connecter au RITM.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S03060	FAUX	FAUX	FAUX	FAUX	VRAI	D'autre part, ces exigences concernent les logiciels de support distant qui seront utilisés dans le RITM. Pour les logiciels de supports distants utilisés à l'intérieur du réseau même de l'établissement, il en est de ce dernier d'établir ses propres critères.
3.3.1 Mesures contre les codes malveillants						
S03059	FAUX	FAUX	FAUX	FAUX	VRAI	Le fournisseur s'engage à fournir un système d'information compatible avec la présence d'antivirus commerciaux reconnus.
S03019	FAUX	FAUX	FAUX	FAUX	VRAI	Le fournisseur s'engage à fournir un système d'information sans aucune porte dérobée (backdoor).
3.3.2 Mesures contre le code mobile						
S03020	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT permettre de vérifier l'authenticité d'un exécutable externe à l'aide d'une signature numérique. Exemples : • Applets Java. • Contrôles ActiveX. • Etc. Pour plus de détails sur la signature numérique, il est possible de consulter la section « 8.1.3 Réglementation relative aux mesures cryptographiques ».
3.4 Sauvegarde des informations						
S03021	FAUX	FAUX	FAUX	FAUX	VRAI	Les fonctionnalités de la base de données du système d'information DOIT permettre d'effectuer des prises de sauvegarde en temps réel ou quasi réel sans interrompe le fonctionnement du système.
S03047	FAUX	FAUX	FAUX	FAUX	VRAI	Effectue la sauvegarde des données / bases de données de façon à permettre, à partir des copies de sécurité, la récupération de tous les systèmes d'opération et applicatifs et de toutes les données utilisateurs.
S03048	FAUX	FAUX	FAUX	FAUX	VRAI	La sauvegarde des données / bases de données peut fonctionner en mode de sauvegarde complète ou incrémentale.
S03049	FAUX	FAUX	FAUX	FAUX	VRAI	Les applications et procédures de sauvegarde permettent une récupération complète et/ou partielle des données (par exemple une fiche, une plage de temps, etc.).
S03050	FAUX	FAUX	FAUX	FAUX	VRAI	Le programme de récupération de données est en mesure de récupérer les métadonnées s'appliquant aux données récupérées. En particulier, il récupère l'information de contrôle d'accès.
S03051	FAUX	FAUX	FAUX	FAUX	VRAI	Les applications et procédures de sauvegarde permettent une récupération jusqu'au point de défaillance.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S03052	FAUX	FAUX	FAUX	FAUX	VRAI	Dans le cas où des sauvegardes quotidiennes partielles sont effectuées, le programme de copies de sécurité intégrera plusieurs sauvegardes incrémentales pour récupérer les données jusqu'à un point donné dans le temps.
S03053	VRAI	VRAI	VRAI	FAUX	VRAI	Les copies de sécurité contenant des informations de nature hautement sensible sont conservées dans des locaux extérieurs au site d'origine de ces informations.
S03054	FAUX	FAUX	FAUX	FAUX	VRAI	Les copies de sécurité et les mécanismes de récupération des informations sont vérifiés régulièrement.
S03055	VRAI	VRAI	VRAI	FAUX	VRAI	La circulation des copies doit être contrôlée et l'accès aux copies de sécurité, restreint aux seules personnes autorisées.
3.5 Politiques et procédures d'échange des informations						
S03058	FAUX	FAUX	FAUX	FAUX	VRAI	Les communications entre les composants du système d'information et avec l'utilisateur DOIVENT pouvoir être chiffrées de bout en bout. Pour plus de détails sur le chiffrement, il est possible de consulter la section « 8.1.3 Réglementation relative aux mesures cryptographiques ». Note : Le « Cadre global de la gestion des actifs informationnels appartenant aux organismes du RSSS (CGGAI) - volet Sécurité » exige également le chiffrement de bout en bout.
3.6.1 Rapport d'audit						
S03027	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information DOIT permettre de journaliser tous les évènements significatifs : • Ouverture de session. • Fermeture de session. • Tentatives d'accès réussies ou avortées (données ou systèmes). • Activation ou désactivation de fonctionnalités par le pilote. • Toutes les activités qui affectent les privilèges sont journalisées et vérifiables. Il faut également indiquer si la journalisation s'effectue au niveau de l'application, la base de données, ces deux (2) derniers, le système d'exploitation ou tout autre composant.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S03029	VRAI	VRAI	VRAI	FAUX	VRAI	Un outil flexible de recherche (critères paramétrisables) DOIT être disponible au pilote pour consulter l'historique des activités du système d'information. Exemples : • Pour consulter l'historique des transactions, à un moment spécifique, par une personne spécifique, sans lui permettre de consulter des informations nominatives. • Pour consulter la liste des utilisateurs, les profils ainsi que les privilèges associés. • Pour consulter la liste des utilisateurs actifs. • Etc.
S03030	VRAI	VRAI	VRAI	FAUX	VRAI	Possibilité de générer des rapports d'audit définis par les utilisateurs. (Par exemple Rapports d'audit par médecin/utilisateur, par usager, par date).
3.6.2 Surveillance de l'exploitation du système						
S03032	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information DOIT fournir un système d'alertage afin d'envoyer des courriels au(x) pilote(s) lors de la détection d'erreurs ou d'anomalies. Exemples : • l'envoi des messages par courriel ; • l'envoi des messages à l'aide du protocole « syslog ». Voici une liste non exhaustive des erreurs ou anomalies intéressantes : • problème de connexion ; • description précise des erreurs applicatives ; • pages non trouvées ; • services non disponibles ; • tentatives échouées d'authentification ; • Ou autres évènements exceptionnels. À noter que le système d'alertage devrait être en mesure de prévenir l'envoi massif de messages lors d'erreurs similaires. Par exemple, un message d'erreur applicatif devrait être envoyé à toutes les minutes plutôt qu'à chaque occurrence, l'objectif étant de prévenir les dénis de services. Dans le cas de l'utilisation d'un système d'alertage par courriel, le système d'information DOIT utiliser un service de relais administrateur (ex : relaisapp.rtss.qc.ca) plutôt que le service de relais utilisateur (relais.rtss.qc.ca).

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S03033	VRAI	VRAI	VRAI	FAUX	VRAI	Possibilité de surveiller les événements d'accès « inhabituels » et de produire des rapports d'alerte pour la surveillance du respect de la conformité. Par exemple : Événements inhabituels, tels que : • Recherche sur le même nom de famille. • Individus identifiés par le prestataire de soins comme « proéminents » ou sensibles. • Toute situation où un individu a accédé à l'information de plus de « x » patients en « y » heures [par ex. volume inhabituel basé sur la valeur moyenne]. Le but de ce critère est de s'assurer que le personnel de la clinique n'utilise pas le système pour d'autres fins que celles requises par sa fonction dans cette clinique. Il s'agit donc d'imaginer des scénarios d'utilisation inappropriée des informations contenues dans le système. L'allusion au nom de famille fait référence au nom de famille des employés qui chercheraient, par exemple, de l'information sur leur propre dossier ou ceux de leur famille. Des individus « proéminents ou sensibles » sont des personnes connues, du public en général ou de l'environnement de la clinique, et qui sont effectivement des patients de cette clinique; la liste de ces personnes pourrait alors être fournie par la clinique elle-même.
S03034	VRAI	VRAI	VRAI	FAUX	VRAI	Des systèmes de prévention des intrusions (SPI) et systèmes de détection des intrusions (SDI) sont intégrés à la solution et journalisés.
S03035	VRAI	VRAI	VRAI	FAUX	VRAI	La solution utilise une approche systématique en matière de verrouillage du système (renforcement de la sécurité [hardening]). La solution présente une sécurité renforcée selon les meilleures pratiques pour les systèmes d'opération et les applicatifs. L'approche est extensible et s'adaptera aux nouvelles technologies et à l'évolution des besoins.
3.6.3 Protection des informations journalisées						
S03037	VRAI	VRAI	VRAI	FAUX	VRAI	La configuration par défaut du système d'information DOIT permettre la protection adéquate des journaux afin d'empêcher toutes altérations des journaux de tous les composants du système d'information. Ces configurations DOIVENT également être documentées dans le guide d'opération (voir la section « 3.1.1 Procédures d'exploitation documentées »).

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S03037	VRAI	VRAI	VRAI	FAUX	VRAI	Exemples : • Les privilèges sur les répertoires DOIVENT être configurés adéquatement afin d'assurer que seule une personne autorisée (ex. : administrateur du serveur) puisse y accéder. Par exemple, il est nécessaire d'enlever tous les privilèges de type « Écriture pour tous ». Tous les composants du système d'information DOIVENT posséder les privilèges suffisants pour journaliser toutes les actions. • Les privilèges sur les tables, au niveau des bases de données, DOIVENT être configurés adéquatement afin d'assurer que seule une personne autorisée puisse y accéder. Par exemple, seul un compte de journalisation DOIT avoir les privilèges nécessaires afin de journaliser toutes les actions. Un compte de pilotage DOIT pouvoir accéder à la journalisation en mode lecture seulement, alors qu'un compte utilisateur NE DOIT disposer d'AUCUN privilège aux tables destinées à la journalisation. • Utilisation d'un outil de rotation des journaux.
S03039	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information DOIT permettre la séparation des tâches, comme il est indiqué dans la « section 3.1.3 Séparation des tâches ». Dans le cas de la protection des informations journalisées, il faut s'assurer que le pilote du système d'information n'ait pas, également, le contrôle sur les journaux, lui permettant ainsi de masquer de possibles actions malintentionnées.
S03040	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre la consolidation des journaux de tous les composants du système d'information afin d'être en mesure d'identifier et de comprendre la séquence des évènements à travers la multitude de journaux.
S03044	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information DOIT permettre uniquement la consultation des journaux en mode lecture aux utilisateurs autorisés.
S03056	VRAI	VRAI	VRAI	FAUX	VRAI	Le calendrier de conservation de la journalisation doit être établi en fonction des lois, normes et règlements en vigueur.
3.6.4 Journal administrateur et journal des opérations						
S03045	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information DOIT permettre de journaliser les actions du pilote et de l'administrateur du serveur. Par exemple, une fonctionnalité utilisant des protocoles tels que « syslog » permet de recevoir les journaux sur un autre serveur, lequel est administré par un administrateur distinct.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
3.6.5 Synchronisation des horloges						
S03046	VRAI	VRAI	VRAI	FAUX	VRAI	Les composants du système d'information DOIVENT permettre d'être synchronisés sur les horloges du RITM (ntp.rtss.qc.ca) afin de faciliter la corrélation des journaux. Cette fonctionnalité peut être utilisée au niveau du système d'information ou au niveau du système d'exploitation.
4 Contrôle d'accès						
4.1.1 Enregistrement des utilisateurs						
S04001	VRAI	VRAI	VRAI	FAUX	VRAI	Les fonctionnalités de gestion du système d'information DOIVENT permettre au pilote de gérer les utilisateurs. Il faut inclure les fonctionnalités typiques telles que : • ajouter, modifier, activer ou désactiver un utilisateur ; • modifier un mot de passe ; • saisir toutes informations pertinentes qui permettent d'identifier ou de communiquer avec un utilisateur. Également, le système d'information DOIT : • empêcher l'enregistrement d'identifiants identiques ; • empêcher la suppression d'un compte utilisateur ; • empêcher la suppression de tous les comptes de type pilote.
S04004	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT afficher un message de confirmation lors de l'ajout, la modification, l'activation ou la désactivation d'un identifiant. Par exemple, une méthode fréquente est l'utilisation d'un message « Vous êtes sur le point de modifier le compte XX, désirez-vous continuer ? Oui / Non ».
S04005	FAUX	FAUX	FAUX	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre d'activer ou désactiver un identifiant ainsi que de permettre d'inscrire une date de début et une date de fin.
4.1.2 Gestion des privilèges						
S04006	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information DOIT permettre : • d'associer un ou plusieurs rôles à un identifiant ; • la gestion des privilèges par rôle ; • par fonction de l'application ; • par secteur d'activité ; • selon l'endroit du poste de travail ; • en mode urgence ; • d'empêcher l'assignation de privilèges contradictoires. Également, le système d'information DOIT permettre l'utilisation d'un seul rôle à la fois.

	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	
No.						**Libellé du critère**
S04006	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité du système d'information DOIT afficher tous les rôles disponibles à l'utilisateur et lui permettre de sélectionner le rôle approprié à son contexte. Exemple : Un contrôle d'accès pour des profils d'accès (utilisateurs et administrateurs) basés sur le rôle de manière à favoriser la séparation des tâches et responsabilités (par ex. : médecin vs administrateur de base de données [DBA] vs MOA, etc.).
S04010	VRAI	VRAI	VRAI	FAUX	VRAI	Les mécanismes de contrôle du système d'information DOIVENT vérifier les privilèges d'un utilisateur avant toute transaction. Ces mécanismes de contrôle NE DOIVENT PAS être utilisés au niveau du tiers client, car il peut être possible de contourner la validation au niveau du client.
S04011	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information DOIT empêcher un utilisateur d'assigner des privilèges supérieurs ou égaux aux siens, à lui-même ou à un autre utilisateur.
S04013	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information DOIT utiliser des identifiants de base de données différents selon les types d'activités. Exemples : Un identifiant est disponible pour : • les activités normales ; • le mode lecture seulement ; • le mode lecture/écriture ; • les activités d'administration ; • chaque utilisateur. Ou • l'utilisation d'une queue de connexion avec une connexion persistante. Également, les privilèges DOIVENT être configurés au niveau des tables de la base de données, selon les identifiants déterminés pour chacun des types d'activités mentionnés ci-haut. Par exemple, le compte « lecture seulement » doit avoir seulement accès aux tables déterminées en lecture seulement.
S04014	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information NE DOIT PAS utiliser un compte administrateur ou un compte privilégié pour se connecter à la base de données ou à tout autre composant du système d'information.
4.1.3 Réexamen des droits d'accès utilisateur						
S04019	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité DOIT permettre de désactiver un identifiant qui n'a pas été utilisé pendant un maximum d'un an.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
4.2.1 Utilisation du mot de passe						
S04020	FAUX	FAUX	FAUX	FAUX	VRAI	Les mots de passe DOIVENT être conservés dans un format protégé. Il faut utiliser des mesures cryptographiques adéquates comme il est mentionné dans la section « 15.1.6 Réglementation relative aux mesures cryptographiques ». En aucun moment, le mot de passe ne doit être stocké en clair. Ceci s'applique dans tous les contextes : • les tables de bases de données ; • les registres ; • les scripts ; • les variables de sessions ; • les fichiers de configurations ; • etc. Dans l'impossibilité de répondre à ce critère, il est nécessaire de bien détailler les raisons.
S04021	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information NE DOIT PAS utiliser un mot de passe dans : • les scripts automatisés ; • les macros ; • le code source ; • ou toute autre utilisation pouvant rendre complexes les mises à jour des mots de passe. Dans le cas contraire, une demande d'exception doit être effectuée (voir MSSS04-026).
4.2.2 Matériel utilisateur laissé sans surveillance						
S04022	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité de déconnexion DOIT être disponible. Lors de la déconnexion, toutes les sessions DOIVENT être réinitialisées afin d'empêcher la réutilisation de cette session. La méthode la plus fréquente est l'utilisation d'un lien « Déconnexion » ou « Se déconnecter » dans le haut de la page de l'écran.
4.3 Authentification de l'utilisateur pour les connexions externes						
S04023	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT être fonctionnel lorsque celui-ci est utilisé à travers le « Service F » ou le service de télé-accès, pour assurer le support à distance.
4.4.1 Ouverture de sessions sécurisées						
S04024	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre de désactiver un identifiant automatiquement après un maximum de cinq tentatives de connexion échouées, comme il est exigé dans le « Cadre global de la gestion des actifs informationnels appartenant aux organismes du RSSS (CGGAI) - volet Sécurité ». Une notification automatique doit informer l'utilisateur du verrouillage de l'identifiant.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S04025	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre d'envoyer un message au pilote ou aux responsables de la surveillance après cinq tentatives de connexion échouées pour les informer de la situation.
S04028	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information NE DOIT PAS transmettre les mots de passe en clair sur le réseau. Par exemple, une méthode fréquente de chiffrement est d'utiliser des connexions avec SSL (ex. : https://votresite.com). Ceci est applicable autant au niveau de : • l'application ; • la base de données; • l'application cliente ; • ou de tout autre composant. Donc, cela signifie que l'authentification de l'application envers la base de données DOIT également être chiffrée.
S04029	VRAI	VRAI	VRAI	FAUX	VRAI	La conservation des mots de passe DOIT être dans un format chiffré (ex. : chiffrement à 256 bits).
S04030	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information NE DOIT PAS spécifier les champs invalides lors de l'authentification. Par exemple, si le mot de passe est invalide pour un identifiant, le système d'information NE DOIT PAS spécifier que c'est le mot de passe qui est invalide. La méthode la plus fréquente est d'afficher un message général indiquant que l'authentification a échoué.
4.4.2 Identification et authentification de l'utilisateur						
S04037	VRAI	VRAI	VRAI	FAUX	VRAI	Le fournisseur s'engage à fournir un système d'information dont le module d'authentification est indépendant du reste du système d'information, permettant ainsi d'utiliser le système d'information avec un module d'authentification externe.
S04038	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information NE DOIT PAS utiliser des comptes génériques. Dans le cas contraire, une demande d'exception doit être effectuée (voir MSSS04-026).
4.4.3 Système de gestion des mots de passe						
S04040	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre de forcer un utilisateur à choisir un mot de passe complexe tel qu'exigé dans le « Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux (CGGAI) - Volet sécurité ». Un minimum de huit (8) caractères dont : • un mixte de lettres et de chiffres ; • un mixte de lettres et de caractères spéciaux ; • un mixte de lettres et de chiffres et de caractères spéciaux.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S04040	VRAI	VRAI	VRAI	FAUX	VRAI	La saisie du mot de passe DOIT également être sensible aux minuscules et majuscules. Exemple : Un paramètre dans le module de pilotage permet d'indiquer le nombre de caractères minimum désirés, ainsi que le type de caractères utilisés.
S04042	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre à l'utilisateur de modifier son mot de passe à tout moment.
S04043	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre d'imposer à un utilisateur de changer son mot de passe lors de la première connexion.
S04044	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité DOIT permettre de désactiver un identifiant si le mot de passe temporaire n'a pas été modifié dans les cinq jours suivants.
S04046	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité DOIT permettre d'exiger la modification des mots de passe par défaut lors de son déploiement. Par exemple, lors de l'installation ou le déploiement, un message exige la modification de tous les mots de passe pour tous les comptes existants par défaut.
S04047	VRAI	VRAI	VRAI	FAUX	VRAI	Le mot de passe NE DOIT PAS être affiché en clair à l'écran lors de la saisie. La méthode appropriée est généralement l'affichage du caractère « * » afin de remplacer le vrai caractère utilisé.
S04049	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre d'imposer le changement du mot de passe après un maximum de 90 jours, tel qu'exigé dans le « Cadre global de la gestion des actifs informationnels appartenant aux organismes du RSSS (CGGAI) - volet Sécurité ». Exemple : Un paramètre dans le module de pilotage permet d'indiquer le nombre de jours maximum avant que le mot de passe n'expire. Conditions d'assignation : Il est acceptable d'utiliser un annuaire (Ex. : Active Directory) pour cette fonctionnalité.
S04050	FAUX	FAUX	FAUX	FAUX	VRAI	La solution peut réutiliser l'authentification du poste de travail Windows lorsque ce dernier est en domaine et lorsque la solution a été intégrée à un Active Directory

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S04051	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité DOIT permettre de désactiver un identifiant automatiquement après un maximum de six semaines de non-activité, tel qu'exigé dans le « Cadre global de la gestion des actifs informationnels appartenant aux organismes du RSSS (CGGAI) - volet Sécurité ». Il serait acceptable d'utiliser une désactivation manuelle si un message est envoyé (à l'aide d'un système d'alertage) au pilote mentionnant qu'un compte doit être désactivé. Exemple : Un paramètre dans le module de pilotage permet d'indiquer le nombre de jours maximum d'inactivité avant que l'identifiant soit désactivé.
S04053	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre d'empêcher la réutilisation d'un mot de passe lors de sa modification. Le « Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux (CGGAI) - Volet sécurité » spécifie que les 10 derniers mots de passe doivent être conservés. Exemple : Un paramètre dans le module de pilotage permet d'indiquer le nombre de mots de passe qui sont retenus par le système d'information afin d'empêcher la réutilisation de ceux-ci. Conditions d'assignation : Il serait acceptable d'utiliser un annuaire (Ex. : Active Directory) pour cette fonctionnalité.
4.4.4 Emploi des utilitaires systèmes						
S04054	FAUX	FAUX	FAUX	FAUX	VRAI	Les utilitaires du système d'information DOIVENT utiliser des privilèges restreints à l'usage prescrit. Par exemple, un compte administrateur NE DOIT PAS être nécessaire pour exécuter un utilitaire. Un utilitaire du système peut être : • des scripts d'automatisation ; • des commandes propres au système d'exploitation (Ex. : cp, top, rm ou autres commandes disponibles pour administrateur) ; • ou tout autre outil complémentaire.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
4.5.2 Isolement des systèmes sensibles						
S04063	FAUX	FAUX	FAUX	FAUX	VRAI	Les locaux où se trouvent les ordinateurs centraux, les mini-ordinateurs, les serveurs des réseaux locaux, le matériel de télécommunications et autres actifs informationnels doivent mettre en place des moyens de protection : • sécurité physique ; • sécurité logique ; • sauvegarde des données ; • outils de surveillance. À titre d'exemple : • être situés dans des endroits protégés contre les catastrophes naturelles (ex. : verglas, inondations) ou accidentelles (ex. : bris d'aqueduc ou de tuyauterie, surchauffe, déclenchement de gicleurs); • être protégés par des mécanismes de contrôle d'accès; • être munis de systèmes de chauffage, de ventilation et de climatisation conformes aux normes recommandées par les fournisseurs; • être munis d'un système d'alimentation électrique sans interruption et d'un système de protection contre les incendies; • permettre de voir les faits et gestes du personnel autorisé présent à l'intérieur du local (aire ouverte).
S04064	FAUX	FAUX	FAUX	FAUX	VRAI	Les équipements pouvant présenter des informations confidentielles, ce qui comprend les imprimantes, les photocopieurs et les télécopieurs, doivent être placés de façon à éviter toute utilisation et observation non autorisées. Par exemple, les équipements utilisés par les équipes de télé-support.
S04065	FAUX	FAUX	FAUX	FAUX	VRAI	L'accès aux locaux où se trouvent les ordinateurs centraux, les mini-ordinateurs, les serveurs des réseaux locaux, le matériel de télécommunications et autres actifs informationnels doit être limité au strict minimum et réservé aux personnes autorisées uniquement.
S04066	FAUX	FAUX	FAUX	FAUX	VRAI	Une liste des personnes autorisées à accéder à ces locaux doit être constituée. Outre le nom de ces personnes, la liste comporte l'énumération des tâches autorisées pour chacune d'entre elles et la durée habituelle de leur intervention ; cette liste doit être mise à jour périodiquement.
S04067	FAUX	FAUX	FAUX	FAUX	VRAI	Un mécanisme de contrôle de l'entrée et de la sortie des personnes qui accèdent aux locaux sécurisés doit être mis en place.
S04068	FAUX	FAUX	FAUX	FAUX	VRAI	Le personnel externe (ex. : fournisseurs, consultants, tiers n'étant pas des employés) chargé de l'entretien et de la réparation des équipements ou de tout autre type d'intervention permise doit être accompagné par une personne autorisée.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S04084	FAUX	FAUX	FAUX	FAUX	VRAI	Tous les postes de travail du centre informatique (télé-support, administration des systèmes, etc.) ayant accès aux renseignements personnels des patients ET à Internet ou aux courriels DOIVENT enregistrer toutes les activités d'accès. Tous les enregistrements comprennent l'heure, la date, l'ID utilisateur et les données relatives à l'accès (par exemple, site Web et adresse IP, adresse de courriel, en-tête de courriel, objet de courriel, ID terminal et ID transaction).
S04085	FAUX	FAUX	FAUX	FAUX	VRAI	En plus des mesures du critère S04084, le fournisseur DOIT aussi décrire les contrôles de sécurité physique et du personnel utilisés dans les postes de travail.
S04069	FAUX	FAUX	FAUX	FAUX	VRAI	Un mécanisme d'identification et d'autorisation doit être mis en place afin de limiter aux seules personnes autorisées l'accès aux actifs informationnels.
S04070	FAUX	FAUX	FAUX	FAUX	VRAI	Les privilèges d'accès accordés aux utilisateurs doivent être inscrits dans un registre maintenu à jour. L'utilisateur qui a accès à des données personnelles ou sensibles signe un formulaire par lequel il s'engage à en respecter la confidentialité.
4.5.4 Gestion des équipements						
S04071	FAUX	FAUX	FAUX	FAUX	VRAI	L'inventaire des équipements, précisant la localisation et l'assignation principale de ces équipements doit être constitué et tenu à jour.
S04072	FAUX	FAUX	FAUX	FAUX	VRAI	La configuration de base des équipements installés doit être définie et tenue à jour.
S04073	FAUX	FAUX	FAUX	FAUX	VRAI	Le registre de l'entretien des équipements doit être constitué et tenu à jour.
S04074	FAUX	FAUX	FAUX	FAUX	VRAI	Les équipements déclarés en surplus ou mis au rebut doivent être exempts d'information électronique avant leur abandon.
S04077	FAUX	FAUX	FAUX	FAUX	VRAI	Des procédures ou des mécanismes de protection contre l'utilisation non autorisée et le vol des équipements doivent être mis en place.
S04078	FAUX	FAUX	FAUX	FAUX	VRAI	L'organisme doit instaurer une procédure obligatoire pour autoriser la sortie d'équipements hors de ses installations.
S04079	FAUX	FAUX	FAUX	FAUX	VRAI	Le calendrier des tâches assurées par le service de l'exploitation informatique quant à l'installation, à l'entretien et à la mise à jour de chaque logiciel et application doit être établi en fonction des besoins définis par le détenteur de l'actif informationnel.
S04080	FAUX	FAUX	FAUX	FAUX	VRAI	Le fournisseur doit faire des mises à jour constantes de son application et de ses composantes (ex. : Oracle, librairies externes, etc.) pour corriger ou prévenir les problèmes de sécurité.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S04082	FAUX	FAUX	FAUX	FAUX	VRAI	Pour les solutions en mode « fournisseur d'applications hébergées », la communication entre le service hébergé de la solution et le terminal d'affichage est mutuellement authentifiée et sécurisée.
S04083	FAUX	FAUX	FAUX	FAUX	VRAI	Permet l'accès sécuritaire à l'application, incluant l'utilisation des ports courants pour faciliter l'accès à travers les pare-feux des établissements (ex : hôpitaux, CLSC).
5 Acquisition, développement et maintenance de SI						
5.1 Analyse et spécification des exigences de sécurité						
S05001	FAUX	FAUX	FAUX	FAUX	VRAI	Le fournisseur s'engage à fournir un système d'information conforme aux meilleures normes de programmation en place ou toutes autres normes jugées acceptables. Ces normes mentionnent des éléments tels que : • les exigences de qualité de code ; • la nomenclature des variables ; • la présence des commentaires ; • des fonctionnalités interdites (ex. : fonction d'exécution de type système telle que « Exec() », « System() » ; • l'utilisation de liens absolus pour les répertoires et les fichiers ; • etc.
S05002	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT être complètement fonctionnel lors de son exécution avec un compte non privilégié. Par exemple, le démarrage du système d'information NE DOIT PAS exiger des privilèges administrateurs pour son utilisation.
S05003	FAUX	FAUX	FAUX	FAUX	VRAI	Le fournisseur s'engage à fournir un système d'information développé selon les ISO 27001 de programmation sécuritaire. Par exemple, Microsoft et Sun Microsystems publient de l'information spécifique à leurs plates-formes de développement. Aussi, des organismes indépendants comme l'OWASP publient de l'information concernant les failles les plus fréquentes auxquelles il est nécessaire de porter attention (« Les dix vulnérabilités de sécurité applicatives Web les plus critiques »).
S05004	FAUX	FAUX	FAUX	FAUX	VRAI	Le fournisseur s'engage à fournir un système d'information empêchant un utilisateur d'accéder à des fonctionnalités non autorisées même si l'utilisateur connaît le lien direct. Par exemple, dans le cas d'une application Web, supposons « https://un_site.rtss.qc.ca/ », il faut empêcher un utilisateur d'accéder au répertoire « https://un_site.rtss.qc.ca/admin/ ».

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
5.2.1 Validation des données d'entrée						
S05005	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information DOIT valider les données en entrées au niveau du serveur et non au niveau du client. Par exemple, les mécanismes de contrôle de type « Javascript » NE DOIVENT PAS être utilisés comme unique mécanisme de validation, car l'utilisation de type « Javascript » peut être facilement contournée.
S05006	VRAI	VRAI	VRAI	FAUX	VRAI	Une fonctionnalité du système d'information DOIT permettre de valider les fichiers téléversés (upload) en limitant les types de fichier acceptés ainsi que la taille du fichier. Par exemple, si le fichier téléversé (upload) attendu par le système d'information doit être un rapport PDF, celui-ci DOIT refuser tous les fichiers qui ne sont pas considérés être un « PDF ». Note : 3. La validation unique des extensions n'est pas une méthode efficace de validation du type de fichier, puisqu'il est possible de renommer un fichier « *.exe » par un fichier « *.pdf ». 4. La limitation du type et de la taille des fichiers téléversés permet d'empêcher le téléversement d'un code malveillant ou l'insertion de fichiers multimédias non désirés.
S05007	VRAI	VRAI	VRAI	FAUX	VRAI	Le fournisseur s'engage à fournir un système d'information qui vérifie et valide toutes les données en entrée, afin d'effectuer toute manipulation ou action à partir de celles-ci, particulièrement lors d'interactions avec des tiers hors confiance. Par exemple, il faut valider : • selon la longueur d'une chaîne de caractères attendue ; • le type de données attendues (Ex. : caractères numériques entre 0 et 9) ; • les champs de type « hidden » (fréquents dans les systèmes d'information de type web) ; • etc.
5.2.3 Mesure relative au traitement interne						
S05011	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT permettre d'utiliser un encodage de données reconnu tel qu'UTF8 afin d'assurer que les données ne seront pas corrompues. Cet encodage DOIT être utilisé au niveau de tous les composants du système d'information afin d'assurer l'intégrité des données à tous les niveaux.
5.2.4 Intégrité des messages						
S05012	FAUX	FAUX	FAUX	FAUX	VRAI	Un message DOIT permettre de confirmer à l'utilisateur le succès ou l'échec de sa transaction. Par exemple, une méthode fréquente est d'afficher un message « Les données ont été sauvegardées ».

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
5.3.2 Gestion des clés						
S05015	VRAI	VRAI	VRAI	FAUX	VRAI	Le système d'information DOIT empêcher l'exportation ou la prise de copie d'une clé privée. Par exemple, la clé privée d'un certificat. La clé privée DEVRAIT être sécurisée à l'aide de la configuration des privilèges (similaire aux sections 3.6.3, 5.2.3 et 5.4).
S05016	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT utiliser des certificats émis par des entités de confiance telles que : • Entrust • Verisign • ou une autorité émise par le Technocentre national (TCN). Il faut mentionner le type de certificat utilisé, l'émetteur du certificat ainsi que l'utilisation prévue. Exemples : Certificat SSL de type serveur : • Nom de domaine : www.un_nom.rtss.qc.ca. • Émetteur : Entrust. • Clé RSA 2048 bits. • Algorithme de signature : SHA-1 (SHA-1 pour des raisons de compatibilité). • Utilisation : Chiffrement et intégrité pour le site https://www.un_nom.rtss.qc.ca. À noter que pour enregistrer des noms de domaine se terminant par « .rtss.qc.ca », il est nécessaire de faire une demande de certificat à 00 SOG Centre de services.
S05017	FAUX	FAUX	FAUX	FAUX	VRAI	S'assurer que les certificats et clés de chiffrement utilisés par l'application ou l'infrastructure qui la supporte, sont gérés et entreposés de façon sécuritaire selon des bonnes pratiques reconnues. Par exemple, les applications Java utilisent normalement un keystore Java. En particulier, si les données sont chiffrées dans la base de données, une attention particulière doit être portée à la gestion des clés de chiffrement.
5.4 Contrôle d'accès au code source du programme						
S05019	FAUX	FAUX	FAUX	FAUX	VRAI	Le fournisseur s'engage à transmettre toute modification ou graduation au système d'information de manière structurée et sécuritaire basée sur les meilleures pratiques. Exemples : • l'envoi d'un cd-rom original ; • l'ajout dans un répertoire de fichiers national ; • le chiffrement lors de l'envoi via les services de télécommunications ; • les méthodes de vérification contre les virus ou les programmes malicieux ; • la vérification de la signature du code ; • la vérification de l'empreinte numérique ; • etc. Il faut expliquer les méthodes de distributions utilisées.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S05020	FAUX	FAUX	FAUX	FAUX	VRAI	S'assurer que l'environnement de développement du fournisseur est protégé par des moyens de sécurité qui respectent les bonnes pratiques généralement reconnues (sécurité physique, sécurité réseau, sécurité logique, entente de confidentialité, anti-virus, etc.). S'assurer que des moyens de sécurité sont en place pour assurer l'intégrité du code source, des documents d'architecture et de spécifications, des fichiers de configuration, des images ou répliques du code déployé chez les clients, des copies de sécurité, etc. S'assurer que des moyens sont en place pour assurer l'intégrité du code déployé chez le client. S'assurer que les développeurs n'ont pas accès à des données personnelles réelles. S'assurer de pouvoir rendre compte aux clients ou à un auditeur de la mise en place adéquate de ces mesures.
S05027	FAUX	FAUX	FAUX	FAUX	VRAI	Les originaux des logiciels et des applications doivent être conservés sous clé et n'être accessibles qu'aux personnes autorisées.
5.5 Mesure relative aux vulnérabilités techniques						
S05022	FAUX	FAUX	FAUX	FAUX	VRAI	Le fournisseur s'engage à fournir un système d'information développé, selon les recommandations des principales autorités en la matière telles que : OWASP ; NIST ; DoD/DISA ; SANS ; CERT ; FrSIRT.
6 Gestion des incidents liés à la sécurité de l'information						
S06003	FAUX	FAUX	FAUX	FAUX	VRAI	Toute information portant sur des processus ou des mesures touchant la sécurité des actifs informationnels doit être gérée de façon confidentielle par l'organisme.
S06004	FAUX	FAUX	FAUX	FAUX	VRAI	Les accès non autorisés doivent être vérifiés. Des mesures préventives ou correctives doivent être appliquées pour les éviter.
S06005	FAUX	FAUX	FAUX	FAUX	VRAI	Un processus d'escalade en cas d'attaque doit être établi et éprouvé ; ce processus comprend notamment les actions permettant la reconstitution de la preuve.
S06006	FAUX	FAUX	FAUX	FAUX	VRAI	Le fournisseur doit élaborer et tenir à jour les trois registres de sécurité suivants : • Le registre des autorités, contenant le nom des différents acteurs impliqués dans la gestion des actifs informationnels ainsi que leurs rôles et responsabilités. • Le registre des incidents où sont consignés les événements ayant pu mettre en péril la sécurité des actifs informationnels. • Le registre des actes de gestion de la sécurité, contenant tout renseignement obtenu dans le cadre du processus de gestion de la sécurité ainsi que les documents, décisions ou directives rédigés par un acteur dans le cadre de ses fonctions en matière de sécurité.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S07002	FAUX	FAUX	FAUX	FAUX	VRAI	Un plan de reprise après sinistre (en cas de sinistre, de panne, d'intrusion, etc.) des systèmes en activité doit être mis par écrit et éprouvé régulièrement au moyen d'exercices de récupération des informations. Ce plan doit préciser, entre autres, le seuil de tolérance à l'interruption de chaque actif ainsi que les processus de relocalisation et les façons de revenir à la normale. Il doit également consigner l'historique des événements.
S07003	FAUX	FAUX	FAUX	FAUX	VRAI	Tous les documents à jour relatifs au plan de reprise après sinistre doivent être conservés à l'extérieur du site.
8 Conformité						
8.1.1 Droits de propriété intellectuelle						
S08001	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT utiliser un code de programmation dont le fournisseur peut garantir les droits de propriété intellectuelle conformément à la Loi sur les droits d'auteurs. Dans le cas contraire, le fournisseur DOIT préciser clairement les limitations (ex. : type de licence). Note : Dans le cas d'utilisation de logiciel libre ou de code libre, le fournisseur DOIT démontrer que la licence permet l'utilisation de ceux-ci dans le contexte. Par exemple, les licences LGPL et GPLv3. Il est recommandé de consulter le site suivant : http://www.gnu.org/licenses/gpl-faq.html.
8.1.2 Protection des données et confidentialité des informations relatives à la vie privée						
S08007	FAUX	FAUX	FAUX	FAUX	VRAI	Le mot de passe DOIT être chiffré ou haché lors de la période de stockage. Pour plus de détails sur les algorithmes cryptographiques, il est possible de consulter la section « 8.1.3 Réglementation relative aux mesures cryptographiques ».
8.1.3 Réglementation relative aux mesures cryptographiques						
S08009	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information NE DOIT PAS reposer sur le chiffrement au niveau des couches OSI 3 et moins (ex. : IPSEC) à l'intérieur du RITM, conformément à la norme « MSSS04-002 - Principes directeurs de sécurité pour les télécommunications ». À titre d'information, rappelons que les couches OSI sont les suivantes : 7 Application 6 Présentation 5 Session 4 Transport 3 Réseau 2 Liaison de données 1 Physique Au besoin, il est possible de consulter le site http://www.frameip.com/osi/.

No.	1- L'actif traite des données cliniques.	2- L'actif traite de données personnels	3- L'actif traite des données RH (ressources humaines)	4- L'actif traite de tout autre type de données	5- L'actif est hébergé par le fournisseur	Libellé du critère
S08010	FAUX	FAUX	FAUX	FAUX	VRAI	Le système d'information DOIT utiliser des algorithmes cryptographiques et protocoles reconnus. Exemples : • AES (128, 192, 256 bits) • RSA (1024 bits et plus) • DSA (1024 bits et plus) • SHA1 (selon pour des besoins de compatibilités), SHA-256, etc. Le centre de la sécurité des télécommunications du Canada (CST) est la référence pour le Canada à ce niveau. https://www.cse-cst.gc.ca/fr/publication/list/Cryptography À noter que les protocoles TLS et SSH/SSLv3 sont également acceptés.
8.2.1 Conformité avec les politiques et les normes de sécurité						
S08011	VRAI	VRAI	VRAI	VRAI	FAUX	Le système d'information DOIT respecter la Charte de la langue française, autant au niveau de la documentation que du système d'information.
S08012	VRAI	VRAI	VRAI	VRAI	FAUX	Le fournisseur s'engage à respecter les normes du MSSS et du « Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux (CGGAI) - Volet sécurité » et d'effectuer des mises à jour au système si des modifications y sont apportées (au CGGAI).
S08058	VRAI	VRAI	VRAI	VRAI	VRAI	Le fournisseur doit mettre en place des programmes de sensibilisation et de formation du personnel de manière à favoriser le développement des compétences relatives à la sécurité des actifs informationnels, à l'application de la politique de sécurité adoptée par l'organisme et au Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité. Par exemple : Formation de l'équipe de support.
S08061	VRAI	VRAI	VRAI	VRAI	VRAI	Le fournisseur doit réévaluer périodiquement, et particulièrement au moment de l'intégration de nouveaux employés, de nouveaux systèmes, de nouveaux développements ou de nouvelles technologies, les besoins du personnel en ce qui concerne la sensibilisation et la formation en matière de sécurité.