

Les orientations technologiques

du réseau sociosanitaire

Pour un accès intégré
et sécurisé à l'information

Québec 

Les orientations technologiques du réseau sociosanitaire

**Pour un accès intégré
et sécurisé à l'information**

Avis aux lecteurs

La cueillette des informations requises pour produire ce document s'est réalisée au cours du premier trimestre de 2001. Aussi les informations propres à l'évolution technologique de l'industrie ou du réseau sociosanitaire risquent de ne plus être à jour au moment de la publication de ce document.

Document produit par :

La Direction des ressources informationnelles du ministère de la Santé et des Services sociaux.

Ce document est disponible en version électronique et peut être consulté à la section Documentation, sous la rubrique Publications du site Web du Ministère de la Santé et des Services sociaux dont l'adresse est : **www.msss.gouv.qc.ca**

Le genre masculin utilisé dans ce document désigne aussi bien les femmes que les hommes.

Dépôt légal

Bibliothèque nationale du Québec, 2003

Bibliothèque nationale du Canada, 2003

Toute reproduction totale ou partielle de ce document est autorisée, à condition que la source soit mentionnée.

© Gouvernement du Québec

MOT DU SOUS-MINISTRE

L'influence des technologies sur l'organisation de notre mode de vie est devenue un sujet de réflexion constant. Les technologies de l'information, nées du traitement logique de l'information rendu possible par le mode numérique, nous ont amenés à constater à quel point la gestion de l'information est un enjeu crucial au sein de nos organisations. Quel que soit le champ d'activité dans lequel elles sont utilisées, les ressources informationnelles alimentent les processus de production et contribuent à en accroître l'efficacité.

Dans le secteur socio sanitaire s'est dessinée la ferme volonté d'assurer l'intégration des services aux usagers dans un continuum de services. Cela implique la mise en relation de personnes qui collaborent entre elles tantôt pour assurer des soins à un usager, tantôt pour mettre sur pied une campagne de vaccination au sein d'une communauté, tantôt pour poursuivre une recherche visant à vaincre une maladie ou encore pour faire face de façon efficace à une problématique sociale. De fait, un réseau intégré de services est à se mettre en place, et tous les acteurs du domaine socio sanitaire sont invités à y participer.

Un tel réseau s'appuie nécessairement sur des mécanismes de communication efficaces entre les différents acteurs. Les ressources informationnelles contribuent directement à cette stratégie. Au cours des dernières années, l'évolution rapide des technologies a modifié la nature même des possibilités offertes, ce qui a incité les organisations à se doter d'infrastructures permettant de tirer profit des ressources informationnelles.

C'est avec grand plaisir que le ministère de la Santé et des Services sociaux vous convie à prendre connaissance des orientations technologiques du réseau sociosanitaire. Ces orientations sont le fruit d'une démarche effectuée en collaboration avec les acteurs concernés par la mise en valeur des ressources informationnelles, au service de leur communauté. Elles ont aussi profité des avis éclairés des fournisseurs qui, à titre de partenaires, s'efforcent avec nous d'inventer des solutions nouvelles susceptibles d'améliorer notre réponse aux besoins de la population québécoise.

En publiant ses orientations technologiques, le Ministère indique clairement ce qu'il entend réaliser et assurer, ce faisant, le leadership que le secteur sociosanitaire attend de lui. Les orientations visent la mise en place d'infrastructures modernes et sécurisées qui serviront d'assise à une utilisation optimale de l'information. Elles invitent les organisations du réseau à tirer pleinement parti des nouvelles technologies de l'information. Elles respectent aussi l'autonomie des partenaires du Ministère qui, nous en sommes convaincus, sauront profiter de la cohésion et de la synergie issue de l'effort commun.

Le sous-ministre,

Pierre Gabrièle

COLLABORATEURS

COMITÉ DIRECTEUR DU PROJET

Jean Asselin (ACJQ)	Roch Beauchemin (MSSS)
Laurent Boisvert (AHQ)	Gabriel Collard (AERDP)
François Dépault (TCR Estrie)	Michel Fortin (Conférence des Régies)
Robert Garon (SOGIQUE)	Jean Houde (MSSS)
Martin Lachance (RAMQ)	Claude Lévesque (MSSS)
Serge Métivier (RAMQ)	Julien Michaud (ACCQ)
Joël Moreau (SOGIQUE)	Alain Ouellet (RR Estrie)
Jean-Louis Pelletier (RAMQ)	

STRUCTURE DE RÉALISATION DU PROJET

CHEF DE PROJET

Lucie Pelletier (MSSS)

ÉQUIPE CHARGÉE DES COMMUNICATIONS

Gilles Dufour (MSSS)

Nicole Lalonde (MSSS)

ÉQUIPE D'INTÉGRATION

Joël Moreau (SOGIQUE)

Patrick Fortin (LGS)

ÉQUIPE DE RÉALISATION (DMR CONSEIL)

André Carette (chargé de projet)

Christian Dion

Jacques Charlebois

André Lemieux

Olivier Lejay

Paul Morin

Michel Morin

Alain Perras

ÉQUIPE DE CONSULTATION (CGI)

Gilles Boivin (chargé de projet)

Guy Tremblay

PARTICIPANTS AUX ATELIERS DE TRAVAIL

ATELIER 1 – SOUTIEN AUX INTERVENANTS

Robert Brochu (SOGIQUE)
Alain Mercier (SOGIQUE)
Richard Vézina (SOGIQUE)

ATELIER 2 – SERVICES INFORMATIONNELS

Alain Dumas (MSSS)
Richard Halley (MSSS)
André Lévesque (MSSS)

ATELIER 3 – TÉLÉSANTÉ

Christine Deschênes (MSSS)
Stéphanie Froissart (MSSS)
Gilles Laberge (MSSS)
Alain Mercier (SOGIQUE)
Denis Poulin (MSSS)

ATELIER 4 – SÉCURITÉ INTÉGRÉE

Claude Bouchard (MSSS)
Robert Brochu (SOGIQUE)
Richard Halley (MSSS)
Denis Poulin (MSSS)
Bernard Roy (MSSS)
Christian Tanguay (MSSS)

ATELIER 5 – CADRE DE RÉFÉRENCE ET PLAN DE MISE EN OEUVRE

Roch Beauchemin (MSSS)
Robert Garon (SOGIQUE)
Jean Houde (MSSS)
Claude Lévesque (MSSS)
Alain Saucier (MSSS)
Michel Verville (MSSS)

PARTICIPANTS À LA CONSULTATION

TABLE DE L'AGIRS

Benoît Bastien	Serge Boileau	Michel Morin	Richard Ouellet
Mario Parent	Denis Pépin	Daniel Sirois	

TABLE DES TECHNOCENTRES RÉGIONAUX

Gilles Blanchette	Raymond Courtois	Pierre Desbiens	François Dépault
Bernard Major	Éric Perron	Gilles Potvin	

TABLE DES INFOCENTRES RÉGIONAUX

Marc Boudreault	Pierre Ferland	Mohamed Jamali	Daniel Larivée
Marie-Hellene Thibault			

TABLE RAMQ

Hugues Beaudoin	Pierre Blais	Jacques Blouin	Danielle Boucher
Philippe Pelletier	Jean-Louis Pelletier	Michelle Quintal	Emile Serinet
Serge Sylvestre	Gaël Ségal	André Vézina	

TABLE DES CHUS

Dr Jeff Barkin	Jean-Pierre Chenel	Marc-André Larose	François Leclerc
Dr Alain Vadeboncoeur			

TABLE DE L'AHQ

Serge Boileau	Laurent Boisvert	Alain Chamoune	Maurice Dupras
Pierre Madore	Dr. Richard Marchand	Dr Christian Obden	Krystina Pecko
Denis Pépin	Dominic Saindon		

TABLE DES CLSC ET DES CHSLD

Guy Deschênes	Gary Furlong	Jean-Guy Lamothe	Jean-Yves Leblanc
Julien Michaud	Can Nguyen-Quang		

TABLE DU FORUM DES RESSOURCES INFORMATIONNELLES

Michel Fortin	Gilles Gauthier	Jean Laterrière	Jacques Longval
Guy Mathieu	Nathalie Simard	Yves Viau	

TABLE DES CENTRES JEUNESSE

Jean Asselin	Pierre Boulianne	Jean Grignon	Sylvain Noury
Yves Provençal	Daniel Robitaille		

TABLE DES CENTRES DE RÉADAPTATION

Gabriel Collard	Michel Dumaine	Michel Fréchette	Guy Gignac
Daniel Héту	Pierre-Paul Lachapelle	Raymond Laforest	Anne Lauzon
Alain Lefebvre	Yves Robitaille		

TABLE DES MATIÈRES

LISTE DES DIAGRAMMES ET TABLEAUX	15
INTRODUCTION	17
1 LE CONTEXTE TECHNOLOGIQUE DU RÉSEAU SOCIO SANITAIRE	19
1.1 LES PROGRÈS DU RÉSEAU SUR LE PLAN TECHNOLOGIQUE.....	19
1.1.1 <i>Rappel des orientations antérieures.....</i>	19
1.1.2 <i>Progrès accomplis.....</i>	21
1.2 L'ÉVOLUTION DE L'INDUSTRIE DES TECHNOLOGIES DE L'INFORMATION ET DES COMMUNICATIONS.....	23
1.3 DE NOUVELLES PERSPECTIVES D'AVENIR POUR LE RÉSEAU.....	27
1.3.1 <i>Contexte gouvernemental québécois.....</i>	27
1.3.2 <i>Plan stratégique ministériel 2001-2004.....</i>	28
1.3.3 <i>Plan d'action en matière de ressources informationnelles</i>	35
1.4 UN MODÈLE DE GESTION DES RESSOURCES INFORMATIONNELLES RENOUVELÉ	38
1.5 LA PORTÉE DES ORIENTATIONS TECHNOLOGIQUES.....	41
2 LES ORIENTATIONS TECHNOLOGIQUES GÉNÉRALES	45
2.1 LES PRINCIPES DIRECTEURS DE GESTION DES TECHNOLOGIES DE L'INFORMATION	46
2.2 LE MODÈLE TECHNOLOGIQUE DE RÉFÉRENCE	52
2.2.1 <i>Prémisses du modèle technologique de référence.....</i>	52
2.2.2 <i>Énoncés généraux de direction</i>	54
2.2.3 <i>Perspectives conceptuelles</i>	57
2.2.4 <i>Règles d'architecture.....</i>	82
3 LES ORIENTATIONS SPÉCIFIQUES.....	87
3.1 LES ORIENTATIONS EN MATIÈRE DE SERVICES ÉLECTRONIQUES AUX INTERVENANTS RELATIVEMENT AUX DOSSIERS DES USAGERS.....	87
3.1.1 <i>Éléments de contexte</i>	89
3.1.2 <i>Principes directeurs concernant les services électroniques aux intervenants relativement aux dossiers des usagers.....</i>	97
3.1.3 <i>Perspectives conceptuelles</i>	98

3.2	LES ORIENTATIONS EN MATIÈRE DE TÉLÉSERVICES.....	103
3.2.1	<i>Éléments de contexte</i>	104
3.2.2	<i>Principes directeurs en matière de téléservices</i>	113
3.2.3	<i>Perspectives conceptuelles</i>	114
3.3	LES ORIENTATIONS EN MATIÈRE DE SERVICES ÉLECTRONIQUES D'INFORMATION SUR LES RESSOURCES ET LES SERVICES.....	119
3.3.1	<i>Éléments de contexte</i>	120
3.3.2	<i>Principes directeurs pour les services électroniques d'information sur les ressources et les services</i>	130
3.3.3	<i>Perspectives conceptuelles</i>	132
3.4	LES ORIENTATIONS EN MATIÈRE DE SERVICES ÉLECTRONIQUES DE GESTION DES RESSOURCES	137
3.4.1	<i>Éléments de contexte</i>	138
3.4.2	<i>Principes directeurs pour les services électroniques de gestion des ressources</i>	140
3.4.3	<i>Perspectives conceptuelles</i>	142
3.5	LES ORIENTATIONS EN MATIÈRE DE SÉCURITÉ ET DE PASSERELLES D'ÉCHANGES ÉLECTRONIQUES.....	147
3.5.1	<i>Éléments de contexte</i>	148
3.5.2	<i>Principes directeurs en matière de sécurité et de passerelles d'échanges électroniques</i>	160
3.5.3	<i>Perspectives conceptuelles</i>	165
3.6	LES ORIENTATIONS EN MATIÈRE DE TÉLÉCOMMUNICATIONS	169
3.6.1	<i>Éléments de contexte</i>	169
3.6.2	<i>Principes directeurs en matière de télécommunications</i>	174
3.6.3	<i>Perspectives conceptuelles</i>	177
4	LA PLANIFICATION DE LA MISE EN ŒUVRE	183
4.1	DES ORIENTATIONS DE TRANSITION POUR LES SYSTÈMES D'INFORMATION	184
4.1.1	<i>Principes d'alignement sur les orientations</i>	184
4.1.2	<i>Modalités de transition</i>	185

4.2	UN MODÈLE DE GESTION DES ORIENTATIONS TECHNOLOGIQUES	187
4.2.1	<i>Description des activités</i>	187
4.2.2	<i>Résultats du processus</i>	189
4.3	LE PLAN DE MISE EN ŒUVRE.....	191
4.3.1	<i>Chaîne de résultats.....</i>	191
4.3.2	<i>Principes de planification de la mise en œuvre.....</i>	195
4.3.3	<i>Approche de mise en œuvre.....</i>	196
4.3.4	<i>Plan d'action.....</i>	198
5.	LES CONTRIBUTIONS ET LES CONSÉQUENCES DES ORIENTATIONS TECHNOLOGIQUES ACTUALISÉES	201
5.1	CONTRIBUTIONS DES ORIENTATIONS TECHNOLOGIQUES	201
5.2	CONSÉQUENCES GÉNÉRALES DES ORIENTATIONS TECHNOLOGIQUES	204
5.2.1	<i>Conséquences touchant les instances décisionnelles du réseau.....</i>	204
5.2.2	<i>Conséquences touchant les organisations du réseau de services</i>	204
5.2.3	<i>Conséquences touchant les fournisseurs de technologies.....</i>	205
6	CONCLUSION.....	207
	ANNEXES	209
	<i>Annexe 1 : Scénarios d'utilisation des systèmes d'information</i>	211
	<i>Annexe 2 : Chaîne de résultats.....</i>	221
	<i>Annexe 3 : Échéancier de projet</i>	233
	<i>Annexe 4 : Fiches de projet.....</i>	237
	BIBLIOGRAPHIE	263
	LEXIQUE.....	271

LISTE DES DIAGRAMMES ET TABLEAUX

DIAGRAMMES

Diagramme 1 :	Exemple de l'accident.....	33
Diagramme 2 :	Exemple de la personne en perte d'autonomie	34
Diagramme 3 :	Modèle de gestion des ressources informationnelles.....	40
Diagramme 4 :	Portée des orientations technologiques.....	42
Diagramme 5 :	Vue d'ensemble des services communs.....	60
Diagramme 6 :	Vue des services communs d'intranet	61
Diagramme 7 :	Vue des services communs de sécurité intégrée	62
Diagramme 8 :	Vue des services communs de gestion des infrastructures partagées	64
Diagramme 9 :	Vue des services communs d'échanges évolués.....	66
Diagramme 10 :	Vue des services communs de contenus informationnels.....	68
Diagramme 11 :	Vue d'ensemble des infrastructures technologiques.....	71
Diagramme 12 :	Vue de second niveau des infrastructures technologiques.....	75
Diagramme 13 :	Contexte d'utilisation des dossiers électroniques de l'utilisateur.....	88
Diagramme 14 :	Vue des services communs d'accès aux données partageables des dossiers électroniques de l'utilisateur	99
Diagramme 15 :	Vue des infrastructures technologiques pour l'accès aux dossiers électroniques des usagers	101
Diagramme 16 :	Contexte d'utilisation des téléservices.....	104
Diagramme 17 :	Vue des services communs pour les téléservices.....	115
Diagramme 18 :	Vue des infrastructures technologiques pour les téléservices.....	116
Diagramme 19 :	Contexte d'utilisation des systèmes de type informationnel.....	119
Diagramme 20 :	Architecture générique du fonctionnement d'un entrepôt de données	126
Diagramme 21 :	Vue des services communs pour les systèmes de type informationnel.....	133
Diagramme 22 :	Vue des infrastructures technologiques pour les services du type informationnel	134
Diagramme 23 :	Contexte d'utilisation des systèmes de gestion des ressources.....	137
Diagramme 24 :	Vue des services communs pour les systèmes de gestion de ressources	143
Diagramme 25 :	Vue des infrastructures technologiques pour les services de gestion des ressources	145
Diagramme 26 :	Contexte d'utilisation des fonctions de sécurité logique	147
Diagramme 27 :	Fonctions de sécurité	157
Diagramme 28 :	Vue des services communs de sécurité.....	166
Diagramme 29 :	Vue des infrastructures technologiques de sécurité	168
Diagramme 30 :	Architecture actuelle pour les domaines clinique et médico-administratif	170

Diagramme 31 :	Architecture actuelle pour le domaine de la télésanté	171
Diagramme 32 :	Vue des services communs pour les télécommunications	178
Diagramme 33 :	Vue des infrastructures technologiques pour les télécommunications	182
Diagramme 34 :	Modèle de gestion des orientations technologiques.....	187
Diagramme 35 :	Chaîne sommaire des résultats.....	191
Diagramme 36 :	Contributions des orientations technologiques	202
Diagramme A1.1 :	Exemple de l'accident	215
Diagramme A1.2 :	Exemple de la personne en perte d'autonomie	219
	Formalisme de représentation	223
Diagramme A2.1 :	Vue d'ensemble de premier niveau de la mise en œuvre des orientations technologiques.....	224
Diagramme A2.2 :	Vue d'ensemble de second niveau de la mise en œuvre des orientations technologiques.....	225
Diagramme A2.3 :	Vue 1 de la mise en œuvre des orientations technologiques.....	226
Diagramme A2.4 :	Vue 2 de la mise en œuvre des orientations technologiques.....	227
Diagramme A2.5 :	Vue 3 de la mise en œuvre des orientations technologiques.....	228
Diagramme A2.6 :	Vue 4 de la mise en œuvre des orientations technologiques.....	229
Diagramme A2.7 :	Vue 5 de la mise en œuvre des orientations technologiques.....	230
Diagramme A2.8 :	Vue 6 de la mise en œuvre des orientations technologiques.....	231
Diagramme A2.9 :	Vue 7 de la mise en œuvre des orientations technologiques.....	232
Diagramme A3.1 :	Échéancier du projet	235

TABLEAUX

Tableau 1 :	Attributs d'un DSE.....	89
Tableau 2 :	Applications de téléservices en activité et leur technologie	106
Tableau 3 :	Applications de téléservices en développement et leurs technologies.....	107
Tableau 4 :	Enjeux propres aux projets de téléservices	108
Tableau 5 :	Répartition des demandes faites au Service de l'infocentre par client	121
Tableau 6 :	Typologie des données des régions régionales	123
Tableau 7 :	Standards particuliers à la vidéoconférence.....	177
Tableau 8 :	Échéancier des initiatives et projets technologiques.....	199

INTRODUCTION

Les premières orientations technologiques du réseau sociosanitaire ont été proposées principalement durant l'année 1992. Dans la foulée de la réforme associée à la Loi sur les services de santé et les services sociaux adoptée en 1991, ces orientations proposaient des principes et des balises en vue de guider la mise en place de mécanismes de partage et d'échange d'information essentiels à la concrétisation des objectifs stratégiques du réseau. À la suite d'une vaste consultation menée en 1993 et après avoir procédé aux ajustements pertinents, le Ministère publiait les orientations en 1994, convaincu de l'importance de faire connaître sa stratégie d'ensemble pour les technologies de l'information.

En même temps, et jusqu'au début de l'année 1996, les orientations technologiques ont été approfondies et complétées par un cadre de mise en œuvre, et elles ont fait l'objet d'une actualisation majeure qui a notamment permis d'ajouter des orientations en matière de télécommunications. Une nouvelle publication s'ensuivit à la fin de l'année 1996.

Le plan stratégique des ressources informationnelles de 1998-2001, dans son analyse du contexte technologique, souligne que ces orientations ont été le déclencheur d'une réflexion sur le rôle des ressources informationnelles dans une perspective d'ensemble. Les orientations ont en effet suscité de nombreuses discussions et permis de fixer des assises pour la réalisation de projets structurants dont les fruits sont aujourd'hui appréciés dans l'ensemble du secteur sociosanitaire. Soulignons, parmi ceux-ci, la mise en place des technocentres provincial et régionaux qui assurent l'accès à une expertise de qualité ainsi qu'à des infrastructures communes de traitement et de communications.

De plus, les orientations en télécommunications ont tracé la voie à la mise en place du Réseau de télécommunications sociosanitaire^{MO} (RTSS)¹, qui est sans doute l'un des plus importants projets structurants en technologie de l'information menés par le réseau sociosanitaire. Le RTSS offre désormais les possibilités de communications et d'échanges de données nécessaires pour soutenir la coopération et la collaboration dans le contexte d'un réseau intégré de services.

Bien que les objectifs associés aux orientations technologiques demeurent pertinents, les orientations elles-mêmes nécessitaient une mise à jour en raison de l'évolution rapide des besoins et des technologies. Une démarche d'actualisation a donc été entreprise depuis l'automne 2000.

1. La dénomination Réseau de télécommunications sociosanitaire, le sigle RTSS et le logo  sont des marques officielles.

Cette démarche s'arrime aux orientations définies dans la planification stratégique ministérielle 2001-2004 et aux orientations présentées dans le plan d'action en matière de ressources informationnelles qui y fait suite. Elle vise à fournir un cadre de référence pour la mise en place de services électroniques et d'infrastructures technologiques permettant un accès intégré et sécurisé à l'information. Ce cadre de référence exprime une vision d'entreprise du réseau sociosanitaire. Il servira à la planification et à la réalisation des différents projets en technologie de l'information.

Le présent document rend compte de la démarche d'actualisation des orientations technologiques du réseau sociosanitaire. La première partie décrit le contexte technologique actuel du réseau et le cadre de référence qui sous-tend la démarche. La deuxième partie présente les orientations générales et le modèle technologique global. La troisième partie aborde les orientations retenues dans six domaines particuliers de services électroniques. La quatrième partie traite de la mise en œuvre des orientations technologiques. Enfin, une cinquième et dernière partie met en lumière la contribution des orientations à l'évolution technologique du secteur de la santé et des services sociaux, et elle souligne les principales répercussions de ces orientations pour les acteurs visés.

Les orientations technologiques actualisées du réseau misent à la fois sur les acquis et sur les avancées technologiques les plus porteuses d'avenir. Elles présentent une vision d'évolution comportant bien sûr des défis de taille mais aussi des promesses enthousiasmantes de résultats quant au devenir technologique du réseau en ce début de millénaire.

1 LE CONTEXTE TECHNOLOGIQUE DU RÉSEAU SOCIO SANITAIRE

Plusieurs facteurs influencent l'évolution technologique du réseau socio sanitaire. Ces facteurs sont liés à la situation actuelle des technologies, aux tendances de l'industrie des technologies de l'information et aux stratégies d'ensemble qui sont adoptées pour le réseau. Afin de bien situer ces facteurs, la présente partie rappelle :

- le chemin parcouru par le réseau sur le plan technologique durant les dernières années ;
- les tendances les plus marquantes qui caractérisent actuellement l'industrie des technologies de l'information ;
- les orientations stratégiques privilégiées par le Ministère et les orientations du cadre de gestion global des actifs informationnels.

Ces éléments de contexte sont complétés par une description de la portée des présentes orientations technologiques.

1.1 Les progrès du réseau sur le plan technologique

Les progrès technologiques du réseau depuis les dernières années sont remarquables. Ces progrès résultent tant de l'adoption d'orientations stratégiques et technologiques appropriées que des efforts humains et financiers importants qui ont été investis pour les concrétiser. Un rappel des orientations et des grandes réalisations permet d'apprécier l'évolution du réseau sur le plan technologique.

1.1.1 *Rappel des orientations antérieures*

Après avoir diffusé une première version des orientations technologiques du réseau en 1994, le Ministère en publie une version actualisée en 1996. Ces orientations, qui instituent une nouvelle pratique dans la gestion des technologies du réseau, contribuent à faire connaître la vision globale d'évolution du réseau sur le plan technologique. Les points saillants de ces orientations sont les suivants :

- la mise en évidence de l'importance du partage des informations sur les usagers, afin d'assurer une prestation de services plus efficace et efficiente, notamment dans le contexte du virage ambulatoire ;

- le développement d'infrastructures donnant accès à des applications communes et à des services de communications tel que le courrier électronique et Internet ;
- la définition et l'application d'une politique globale de sécurité s'articulant au cadre légal et réglementaire en vigueur ;
- le déploiement d'un réseau de télécommunications reliant l'ensemble des organisations du réseau sociosanitaire ;
- l'implantation d'un technocentre provincial et de technocentres régionaux pour la gestion des infrastructures partagées et des services communs ;
- l'élargissement de la portée des systèmes d'information et la mise à profit du réseau de télécommunications ;
- l'alignement sur des architectures de systèmes ouverts et des normes reconnues par l'industrie.

Ces orientations marquent un point tournant de l'évolution technologique du réseau sociosanitaire. Elles ont été la bougie d'allumage pour la mise en place du RTSS.

Le plan stratégique 1998-2001 sur les ressources informationnelles du secteur de la santé et des services sociaux québécois constitue un autre pas important. Abordant les ressources informationnelles et non pas seulement les technologies, ce plan stratégique appuie, à l'aide d'exemples puisés à même des situations réelles du réseau, les principes directeurs suivants :

- faire des investissements qui accordent la priorité aux systèmes à valeur ajoutée ;
- évoluer vers un réseau intégré de systèmes soutenant le continuum des soins et services aux usagers avec une information de qualité ;
- assurer le respect de la vie privée des usagers, de leur consentement et de la confidentialité de l'information ;
- mettre en commun les infrastructures, les applications et les expertises ;
- implanter une approche de gestion de l'information commune à l'ensemble du secteur sociosanitaire.

Le plan stratégique 1998-2001 et les orientations technologiques qui l'ont précédé ont tracé la voie à des réalisations majeures qui ont fortement contribué à soutenir la transformation du réseau vers un réseau intégré de services.

Plus récemment, à l'occasion d'un colloque tenu en juin 2000, le Ministère précisait certains éléments de stratégie concernant les ressources informationnelles du réseau, dont les suivants :

- accorder la priorité aux besoins d'ordre clinique et au soutien des intervenants ;
- assurer la gestion adéquate du consentement de l'utilisateur quant au partage d'information ;
- inclure les intervenants privés de première ligne dans le réseau intégré de services (cliniques privées, pharmacies, organismes communautaires) ;
- renforcer l'encadrement de gestion des actifs communs et faire en sorte :
 - de réaliser une architecture globale de l'information,
 - de concevoir une politique de sécurité,
 - d'améliorer le contexte de gestion des projets,
 - d'élaborer de nouvelles orientations en matière de systèmes informationnels,
 - de mettre à jour les orientations technologiques du réseau,
 - de mettre en place un mécanisme de certification des applications avant leur intégration au RTSS, cela afin d'en garantir la sécurité et la performance.

Ces éléments ont été intégrés dans les récents travaux d'orientations stratégiques et technologiques. Par ailleurs, certains d'entre eux se sont déjà concrétisés, dont le mécanisme de certification des applications.

1.1.2 Progrès accomplis

Les orientations stratégiques et technologiques adoptées depuis 1996 ont suscité la mobilisation nécessaire à leur mise en oeuvre. Les efforts humains et financiers investis ont donc permis des réalisations significatives et bénéfiques pour le réseau socio-sanitaire. Quelques-unes de ces réalisations sont évoquées ci-après.

Le RTSS, un réseau privé unique de télécommunications, relie maintenant tous les établissements et compte au-delà de 1 400 sites répartis sur l'ensemble du territoire québécois. Grâce à ce réseau, plus de 45 000 utilisateurs ont accès à des services communs. Les télétravailleurs et les partenaires externes peuvent aussi accéder à certains services du RTSS, comme le courrier électronique, en passant par Internet à travers une zone de sécurisation (DMZ). De plus, des échanges

électroniques avec d'autres réseaux gouvernementaux, tels que ceux de la Commission de la santé et de la sécurité du travail (CSST) et du Réseau d'informations scientifiques du Québec (RISQ) sont supportés par des passerelles.

À l'heure actuelle, les utilisateurs du RTSS engendrent un volume moyen de trois millions d'accès à Internet par jour. Ces mêmes utilisateurs font quotidiennement appel à des services électroniques comme le courrier Notes, l'agenda et de nombreux forums. Par l'entremise du seul courrier électronique Notes, plus de 25 000 messages interrégionaux sont transmis chaque jour, sans compter les 1 000 à 5 000 messages qui sont envoyés à l'intérieur de chaque région.

Plusieurs systèmes d'information du réseau permettent de soutenir les services aux usagers et l'échange d'information entre les établissements, par exemple dans le cadre du Programme de dépistage du cancer du sein, pour le suivi à domicile de personnes préalablement hospitalisées (Lien CH-CLSC) ou pour les services à certaines clientèles ambulatoires (SI-PRSA).

D'autres applications ont permis l'informatisation des établissements, particulièrement dans le secteur social. C'est le cas notamment du Système Intégration CLSC (I-CLSC), du Système d'information pour les centres d'hébergement et de soins de longue durée (SICHELD) et du Système d'information sur les ressources de type familial (SIRTF).

Le développement de la télésanté se fait également peu à peu. Celle-ci répond à des besoins d'échanges spécialisés en cardiologie, en orthophonie, en psychiatrie, en radiologie, en orthopédie, en dermatologie, en pathologie, en oncologie et en formation médicale continue. Les réseaux de télésanté (Réseau québécois de télésanté pour enfants ou RQTE, Réseau mère-enfant ou RME et Réseau interrégional de télémedecine du Québec) implantés à même le RTSS s'entrecroisent et relient plus d'une quarantaine d'établissements.

De nombreux autres projets sont en cours ou ont été planifiés dans le domaine de la télésanté. À titre d'exemple, les Îles-de-la-Madeleine ont implanté un réseau pour les médecins de l'hôpital de l'Archipel qui consultent des collègues de différents établissements.

Ces progrès technologiques n'auraient pas été possibles sans une évolution sur le plan organisationnel. Ainsi, afin de soutenir le fonctionnement de ces infrastructures communes du réseau socio sanitaire, un technocentre national et dix-huit technocentres régionaux ont été mis en place. Le Ministère a aussi créé le Bureau d'accueil des applications, qui gère un processus de certification garantissant la sécurité et la performance des applications sur le RTSS. Il fait appel aux services d'un organisme indépendant, le Centre de recherche informatique de Montréal (CRIM), pour réaliser la certification.

Des mécanismes de gestion d'ensemble ont aussi été instaurés. Le Comité de concertation sur les ressources informationnelles du réseau (CCRI) est le lieu de concertation et d'échange sur les stratégies en ce qui concerne la gestion de l'information et les technologies de l'information. La Table ministérielle de télésanté soutient les projets en proposant un cadre de référence qui précise les critères permettant d'établir les priorités entre les projets. Le Comité national sur la protection des renseignements personnels et la sécurité (CNPRPS) a quant à lui fixé le cadre global de gestion de la sécurité des actifs informationnels du réseau de la santé et des services sociaux. Un document précise quelles mesures doivent considérer les établissements pour assurer la sécurité de leurs actifs informationnels. D'autres groupes plus spécialisés, comme la Table ministérielle pour le dossier patient partageable, complètent le cadre organisationnel actuel.

1.2 L'évolution de l'industrie des technologies de l'information et des communications

Les progrès du réseau en matière de technologies de l'information et de communications sont remarquables. Il reste cependant beaucoup à accomplir encore puisque, d'une part, les processus de services et de gestion des organisations sont en perpétuel changement et que, d'autre part, la constante évolution des technologies ouvre la voie à de nouvelles possibilités de rendre les organisations plus performantes.

La présente section traite des grandes tendances de l'évolution technologique susceptibles d'être d'intérêt pour le réseau. Les changements aux processus de services et de gestion seront quant à eux abordés à la section 1.3 qui décrit de nouvelles perspectives d'avenir pour le réseau.

L'industrie des technologies de l'information est un secteur d'activité en pleine effervescence. La vitesse à laquelle les innovations se multiplient et influencent les façons de faire est phénoménale. Un des défis, en ce qui concerne les orientations, consiste à différencier les modes passagers des véritables percées technologiques ayant un réel intérêt. Ce sont les tendances marquées correspondant à ces percées qui doivent surtout retenir l'attention.

Plusieurs avancées des technologies de l'information sont associées à des domaines comme la sécurité, les outils d'exploitation de données, les systèmes de gestion de ressources, les outils de gestion d'infrastructures et les télécommunications. Ces tendances technologiques sont effectivement d'intérêt pour le réseau et sont considérées dans le cadre des orientations spécifiques qui font l'objet du troisième chapitre du présent document.

De façon plus générale toutefois, deux grandes tendances technologiques se démarquent. La première est l'omniprésence des technologies de type Internet depuis la montée en popularité des services Web ; elle touche à peu près tous les

secteurs d'activité et toutes les industries. La seconde tendance d'intérêt, qui concerne plus particulièrement le secteur socio-sanitaire, consiste en la reconnaissance à l'échelle mondiale du concept de dossier électronique de l'utilisateur basé sur la normalisation de l'information.

Technologies de type Internet

Tout en ayant connu une croissance fulgurante ces dernières années, Internet demeure en pleine expansion. La facilité d'accès, le coût abordable de connexion ainsi que la diversité des informations et des services qu'on y trouve constituent des attraits irrésistibles pour le consommateur.

De leur côté, les entreprises y voient la possibilité de satisfaire un vaste public dans des délais très courts, ce qui permet de multiplier les occasions d'affaires en ligne. Même les gouvernements des différents pays emboîtent le pas pour offrir leurs services directement aux citoyens et aux entreprises. À cet égard, le gouvernement du Québec a pris les devants en réalisant récemment une architecture d'entreprise gouvernementale axée sur la prestation électronique de services aux citoyens et aux entreprises.

La percée d'Internet a stimulé l'industrie des technologies de l'information et des communications d'une façon exceptionnelle. Depuis les cinq dernières années, les grands fournisseurs de logiciels et d'équipements ont investi massivement dans le développement de nouvelles gammes de produits compatibles avec les standards d'Internet. Les concepteurs d'applications ont également innové et multiplié les portails de services en ligne à un rythme surprenant. Plusieurs nouveaux concepts ont vu le jour, dont :

- l'intranet, un réseau basé sur les standards d'Internet, qui soutient les services électroniques internes d'une organisation ou d'une communauté d'organisations se constituant en entreprise étendue ;
- l'extranet, un réseau basé sur les standards d'Internet, qui soutient une relation privilégiée d'affaires entre des organisations distinctes ;
- la gestion de la relation client (connue en anglais sous le sigle CRM, qui signifie *Customer Relationship Management*), initialement conçue pour permettre à une organisation de fidéliser ses clients en personnalisant le plus possible l'interaction électronique.

Les développements technologiques amenés par la vague Internet ont rendu plus facile que jamais auparavant l'intégration du multimédia aux applications, de sorte que les images, les sons et les documents vidéo prolifèrent sur le Web.

L'explosion des échanges d'information provoquée par le Web a aussi eu des répercussions considérables sur les télécommunications. La demande de bande

passante s'accroît constamment, et l'avènement de l'utilisation plus courante de la vidéoconférence sur le Web contribuera probablement à l'accroître encore davantage.

D'un point de vue technique, cette évolution a aussi modifié profondément la façon de concevoir et de réaliser les systèmes d'information et les architectures technologiques. Les nouveaux systèmes font maintenant appel à des architectures à multiples niveaux². Le logiciel client est le plus souvent un fureteur qui participe activement à l'application. Il recourt à un serveur d'application qui agit comme intermédiaire pour retrouver l'information là où elle est, c'est-à-dire sur un ou plusieurs autres serveurs. Cela est rendu possible grâce à la normalisation des langages de codification et des protocoles de communications apparus avec Internet. Une panoplie d'outils de développement sont offerts sur le marché pour permettre la réalisation d'applications Web.

Ces technologies présentent des avantages fonctionnels, techniques et économiques indéniables par rapport aux technologies plus traditionnelles. L'interface est généralement simple à utiliser ; elle permet à l'utilisateur d'avoir accès à l'ensemble des services électroniques et des applications à partir d'un même outil, le fureteur. Ce dernier peut fonctionner avec des postes de travail de différentes technologies qui ne nécessitent généralement pas une grande puissance.

Les normes ouvertes associées aux technologies Web sont supportées par la majorité des fournisseurs de technologies, de sorte que l'intégration des applications s'en trouve facilitée. L'éventail d'applications et d'outils disponibles sur plate-forme Web est extrêmement vaste. En fait, compte tenu du potentiel économique que représente maintenant Internet, les fournisseurs de technologies n'ont pratiquement plus le choix ; leurs produits doivent fonctionner en mode Web sinon ils sont écartés du marché.

Ces tendances touchent déjà plusieurs systèmes utilisés par les organisations du réseau. Il est prévisible que les fournisseurs offriront de plus en plus de logiciels et de services fonctionnant en mode Web. Le mouvement vers des technologies de type Internet est donc résolument amorcé. Un des défis majeurs du réseau sociosanitaire pour les prochaines années consistera donc à structurer adéquatement son intranet ainsi que les échanges électroniques avec ses partenaires, aussi bien à travers des extranets que dans Internet.

2. Dans la littérature spécialisée, l'expression multi-tiers est utilisée pour décrire ce type d'architecture, qui comprend des processus distribués sur plusieurs plates-formes technologiques.

Dossier électronique de l'utilisateur

Selon un document du Bureau de la santé et l'Inforoute de Santé Canada³, le Canada, ainsi que certains autres pays comme les États-Unis et le Royaume-Uni reconnaissent que les systèmes de dossiers de santé électroniques constituent un besoin. Ce même document définit le dossier de santé électronique comme un « dossier de santé d'une personne qui est accessible en direct à partir de nombreux systèmes distincts et interopérables au sein d'un réseau électronique⁴ ». Par ailleurs, le document souligne que toute implantation d'un système de dossiers de santé électroniques constitue une entreprise à long terme, complexe et coûteuse.

De fait, la réalisation de ce type de système a donné lieu à de nombreuses initiatives dans différents pays. La tendance semble inéluctable ; les investissements se chiffrent en centaines de millions de dollars et, tôt ou tard, des produits issus de ces initiatives envahiront le marché.

La mise en œuvre de ces systèmes fondés sur une automatisation avancée exige la normalisation de plusieurs informations administratives et cliniques. HL7, un organisme basé aux États-Unis et ayant des membres issus de nombreux pays, apparaît comme le leader mondial en matière de normalisation de ces informations. Ses normes sont déjà largement utilisées. Les nouvelles versions des normes proposées par HL7 sont prometteuses, car elles tirent profit des enseignements des versions antérieures et s'appuient sur XML, un langage de structuration de l'information normalisé sous l'autorité de l'Internet Society.

Il est aussi reconnu que la mise en œuvre des systèmes de dossiers de santé électroniques demande des identificateurs uniques pour l'utilisateur, l'établissement et le professionnel⁵. Par exemple, l'identificateur de l'utilisateur est essentiel pour permettre de reconstituer un dossier électronique à partir de segments d'information dispersés dans différents systèmes.

La possibilité d'utiliser ces identificateurs pour créer et exploiter des banques d'information consolidées sur la santé des personnes soulève des espoirs mais aussi des défis majeurs en matière de protection des renseignements personnels. En effet, ces informations sont souvent très sensibles et il est impératif non seulement que des mécanismes appropriés de sécurisation leur soient appliqués, mais aussi que le cadre juridique régissant leur utilisation soit défini de manière à assurer une protection adéquate pour chaque personne.

Dans la détermination des orientations technologiques du réseau, l'évolution vers des dossiers de santé électroniques, la normalisation de l'information et des mécanismes d'échanges d'information ainsi que la sécurisation des informations

3. Bureau de la santé et l'Inforoute, *Vers les dossiers de santé électroniques*, Ottawa, Santé Canada, Bureau de la santé et l'Inforoute, janvier 2001, p. 60.

4. *Ibid*, p. 12.

5. *Ibid*

sont des tendances inéluctables. Le défi consiste à mettre en place au plus bas coût des infrastructures technologiques capables de soutenir adéquatement les modes de partage de l'information qui peuvent être adoptés, compte tenu des défis politiques, sociaux, économiques, juridiques et éthiques soulevés par le dossier de santé électronique.

1.3 De nouvelles perspectives d'avenir pour le réseau

Comme dans tous les secteurs d'activité, les organisations du réseau sociosanitaire sont constamment appelées à changer pour se moderniser et s'adapter aux nouvelles lois, aux contraintes économiques, aux nouvelles pratiques professionnelles et de gestion, aux innovations technologiques (génie biomédical, nouveaux médicaments, technologies de l'information, etc.) ainsi qu'à des phénomènes démographiques et sociaux comme ceux qu'entraîne le vieillissement de la population.

Au Québec, les changements à l'organisation des services de santé et des services sociaux sont orientés par les stratégies gouvernementales et ministérielles. Comme ces stratégies déterminent les priorités d'investissement, les actions à entreprendre et les résultats visés, elles permettent de prévoir les changements susceptibles d'affecter les processus de services et de gestion, et ainsi d'aligner les stratégies et les orientations plus particulières aux ressources informationnelles sur les mêmes objectifs.

C'est dans cette optique que la présente section évoque les stratégies gouvernementales : celles qui portent sur les ressources informationnelles, et celles qui concernent plus particulièrement le secteur sociosanitaire.

1.1.1 Contexte gouvernemental québécois

Certaines politiques et directives du gouvernement peuvent avoir des effets sur les actions du réseau sociosanitaire en matière de technologies de l'information, telles que la Politique de l'utilisation du français dans les technologies de l'information et la Directive concernant la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale.

Par ailleurs, les plus récentes stratégies gouvernementales qui se rapportent aux technologies de l'information et des communications découlent de la Loi sur l'administration publique, adoptée au printemps 2000, et de la Politique québécoise de l'autoroute de l'information. En résumé, ces stratégies précisent que l'utilisation des technologies de l'information doit viser à :

- contribuer à accroître la qualité des services aux citoyens en facilitant l'accès à ces services et en simplifiant leur utilisation ;

- soutenir l'optimisation de la gestion des ressources et l'amélioration de la performance des processus de prestation des services ;
- maximiser les retombées des investissements sur les plans social, culturel, éducatif et économique.

Prenant appui sur ces stratégies, le Secrétariat du Conseil du trésor a défini une architecture d'entreprise gouvernementale (AEG), qui décrit :

- un modèle de prestation électronique de services visant à offrir des services gouvernementaux en ligne aux citoyens et aux entreprises ;
- un modèle d'infrastructures technologiques pour la prestation électronique de services, qui privilégie notamment l'utilisation des technologies du type Internet ;
- une architecture globale de sécurité de l'information numérique (AGSIN) où la protection des renseignements personnels est une préoccupation fondamentale.

Les orientations stratégiques et technologiques du réseau souscrivent aux stratégies gouvernementales ainsi qu'à l'architecture d'entreprise tout en poursuivant des objectifs adaptés aux besoins du réseau sociosanitaire et en rapport avec les stratégies plus particulières au secteur de la santé et des services sociaux. À cet égard, le plan stratégique ministériel 2001-2004 a été déposé à l'Assemblée nationale du Québec le 4 avril 2001. Le Ministère a également défini un plan d'action en matière de ressources informationnelles.

1.1.2 Plan stratégique ministériel 2001-2004⁶

Les orientations définies dans le plan stratégique sont nettement axées sur l'amélioration des services et l'optimisation de la gestion. Elles préconisent notamment :

- de convenir des objectifs prioritaires de santé et de bien-être auxquels tous les acteurs sont conviés à participer ;
- d'améliorer l'accès aux services et d'assurer une organisation optimale des ressources ;
- de doter le réseau de la santé et des services sociaux de ressources humaines qualifiées, de moyens informationnels adéquats et de méthodes de budgétisation appropriées ;

6. Selon le document intitulé *Plan stratégique 2001-2004 du ministère de la Santé et des Services sociaux*, publié par le Ministère en avril 2001.

- de stabiliser le financement des services de santé et des services sociaux ainsi que la croissance des dépenses ;
- de clarifier les responsabilités des différents acteurs et d'accroître leur imputabilité.

Conformément à ces orientations, le plan stratégique ministériel énonce un ensemble d'objectifs quant à de nouveaux modes de prestation des services à la population et à de nouveaux modes de gestion, dont les principaux éléments se résument comme suit :

- mettre en place des groupes de médecine de famille ;
- former des réseaux intégrés de services pour les usagers en perte d'autonomie ;
- mettre en place des chaînes complètes d'interventions pour les services préhospitaliers d'urgence ;
- renforcer la coordination des services pour les usagers ayant des problèmes complexes ;
- mettre en place une offre de services de base complète dans les CLSC ;
- accentuer les activités de promotion, de prévention et de protection avec intégration aux pratiques et au continuum de soins et de services ;
- recourir à des engagements de performance soutenus par l'allocation des ressources et la budgétisation ;
- axer la reddition de comptes sur l'évaluation des résultats et l'atteinte des objectifs ;
- maximiser la performance dans l'utilisation et le fonctionnement des services d'urgence ;
- affecter aux secteurs définis comme précaires un nombre suffisant de ressources humaines qualifiées ;
- optimiser le processus et les mécanismes d'inscription, de suivi et d'utilisation des médicaments.

Plusieurs de ces objectifs sont intimement associés à l'accessibilité de moyens informationnels adéquats dans les processus de services et de gestion. À cet égard, rappelons un énoncé explicite du rapport de la Commission Clair :

[...] les technologies de l'information et des télécommunications se développent à un rythme accéléré et transforment en profondeur le fonctionnement des organisations. Ces technologies permettent aux professionnels d'échanger, en temps réel et à distance, de l'information clinique et d'avoir accès à des connaissances nouvelles. Elles offrent la possibilité d'améliorer l'évaluation des services en mettant en relation des données cliniques, financières et opérationnelles⁷.

Le rapport met également en lumière que l'échange d'information sécurisée favorise l'intégration des services et préserve le respect de la confidentialité ainsi que l'autonomie des prestataires de soins⁸, et conclut qu'il « *n'y aura pas de réelle intégration des services sans systèmes fiables et partageables d'information clinique et de gestion⁹* ».

Le Ministère considère également comme indissociables les orientations stratégiques ministérielles et les stratégies de gestion des ressources informationnelles. Il a d'ailleurs défini un plan d'action en matière de ressources informationnelles qui précise ses orientations stratégiques. À l'instar de la Commission Clair, ce plan d'action souligne que le partage de l'information de nature clinique est le défi le plus important dans le contexte actuel.

S'inscrivant en continuité avec le plan stratégique ministériel, les stratégies en matière de ressources informationnelles doivent mettre l'accent sur :

- le soutien au renouvellement de l'organisation des services ;
- l'amélioration de la performance du réseau ;
- la prise en charge des événements récurrents.

Au regard du renouvellement de l'organisation des services, les ressources informationnelles doivent apporter un soutien à la consolidation de la première ligne en tant qu'assise du système de services de santé et de services sociaux. Dans le contexte d'un continuum de services et d'une collaboration étroite entre les différents intervenants, les ressources informationnelles doivent aussi contribuer à la relation de confiance entre l'utilisateur et ces intervenants. En fait, l'utilisateur doit savoir que l'information qui le concerne est protégée adéquatement et que le professionnel avec qui il est en relation possède, lorsque cela est pertinent, une connaissance d'ensemble de sa situation personnelle.

7. Commission d'étude sur les services de santé et les services sociaux, *Les solutions émergentes : Rapport et recommandations*, (S.I.), Commission d'étude sur les services de santé et les services sociaux, 2000, p. 17.

8. *Ibid*, p. 4.

9. *Ibid*, p. 106.

L'amélioration de la performance du réseau vise quant à elle l'obtention des meilleurs résultats compte tenu des ressources existantes. L'information est vue comme un élément essentiel à cette optimisation. Elle est aussi partie intégrante de la gestion axée sur les résultats, le processus de reddition de compte et le renouvellement du mode de budgétisation.

Quant à la prise en charge des événements récurrents, elle vise à réaliser un suivi continu des situations à risques afin de pouvoir agir rapidement en cas de nécessité. Par exemple, un suivi continu de l'achalandage des urgences ou de la répartition des ressources en région est essentiel afin de connaître le plus rapidement possible les situations à risques et prendre les mesures qui s'imposent.

Le renouvellement de l'organisation des services, l'amélioration de la performance du réseau et la prise en charge des événements récurrents nécessitent un ensemble de systèmes d'information. À titre d'exemples, voici quelques scénarios qui mettent en évidence les besoins d'échanges d'information entre les différents systèmes.

Un accident de la route est une première situation qui permet d'illustrer la complicité requise entre les établissements et entre les professionnels afin d'assurer la continuité et la complémentarité des interventions ainsi que leurs liens avec les aspects administratifs. Le scénario d'accident, illustré par le diagramme 1, montre quelques-unes des organisations concernées par le réseau intégré destiné à soutenir le continuum de services à l'utilisateur. Il met également en lumière les systèmes d'information et les besoins relatifs aux échanges d'informations entre ces systèmes, notamment à cause du fait que les informations utiles à la prestation des services sont distribuées dans différents systèmes qui doivent être reliés entre eux. Le scénario fait également ressortir que les systèmes utilisés dans les opérations sont indissociables des systèmes d'information sur les ressources et les services qui, eux, soutiennent les activités administratives et de recherche. Une description détaillée du scénario est présentée à l'annexe 1.

Ce scénario d'accident de la route peut avoir de nombreuses variantes mettant en cause d'autres organisations, d'autres intervenants et d'autres types d'événement comme un accident cardiovasculaire, un enfant victime de sévices corporels, un accident de travail ou la chute d'une personne âgée.

Par ailleurs, de multiples situations requièrent une continuité et une complémentarité des interventions de la part des organisations et des professionnels du secteur socio-sanitaire. Le diagramme 2 illustre le cas d'une personne en perte d'autonomie. Ce scénario est lui aussi décrit en détail à l'annexe 1. Tout comme celui de l'accident, il fait ressortir l'importance du partage de l'information de nature clinique afin d'assurer des services de qualité aux usagers du système socio-sanitaire.

Diagramme 1 : Exemple de l'accident

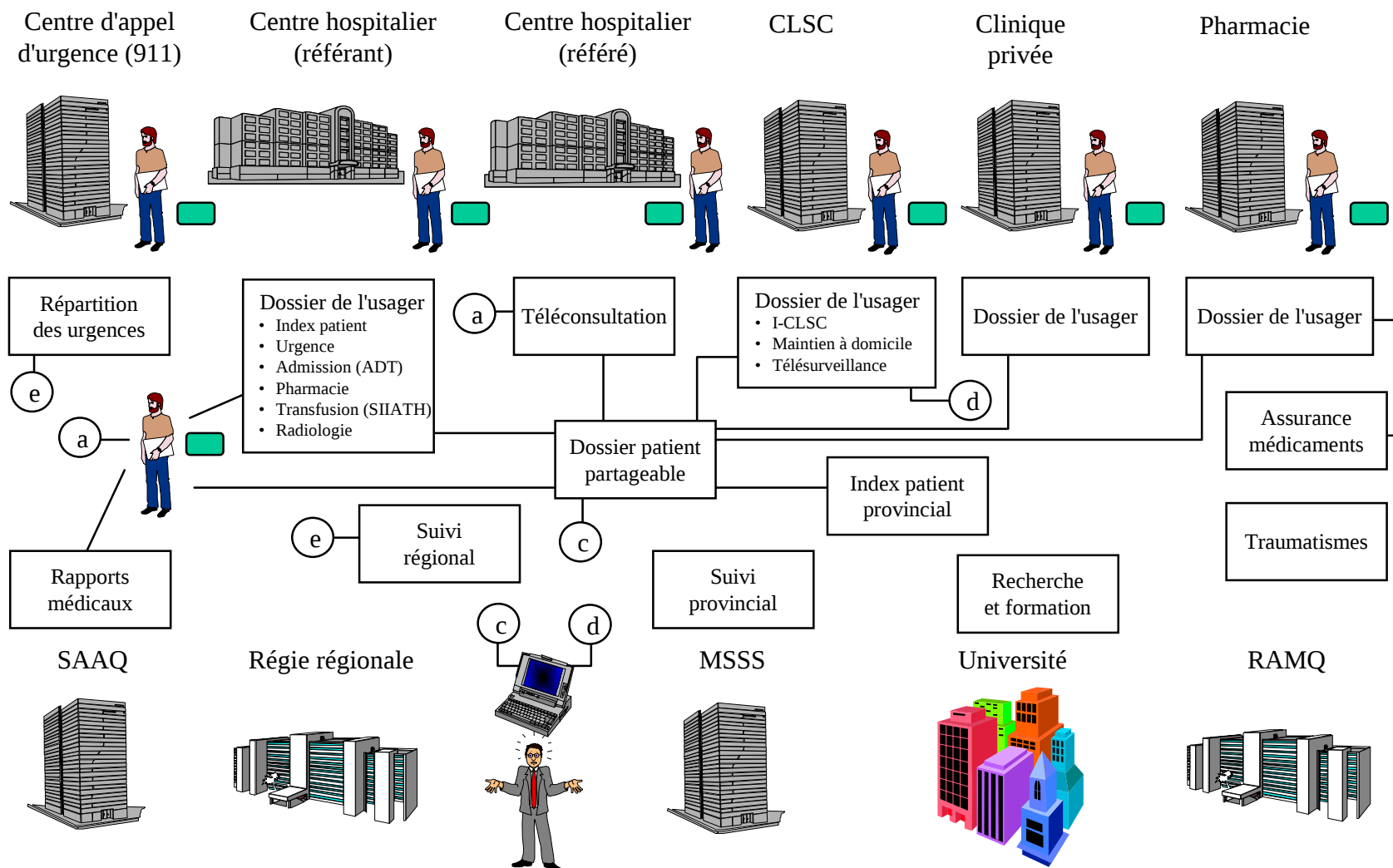
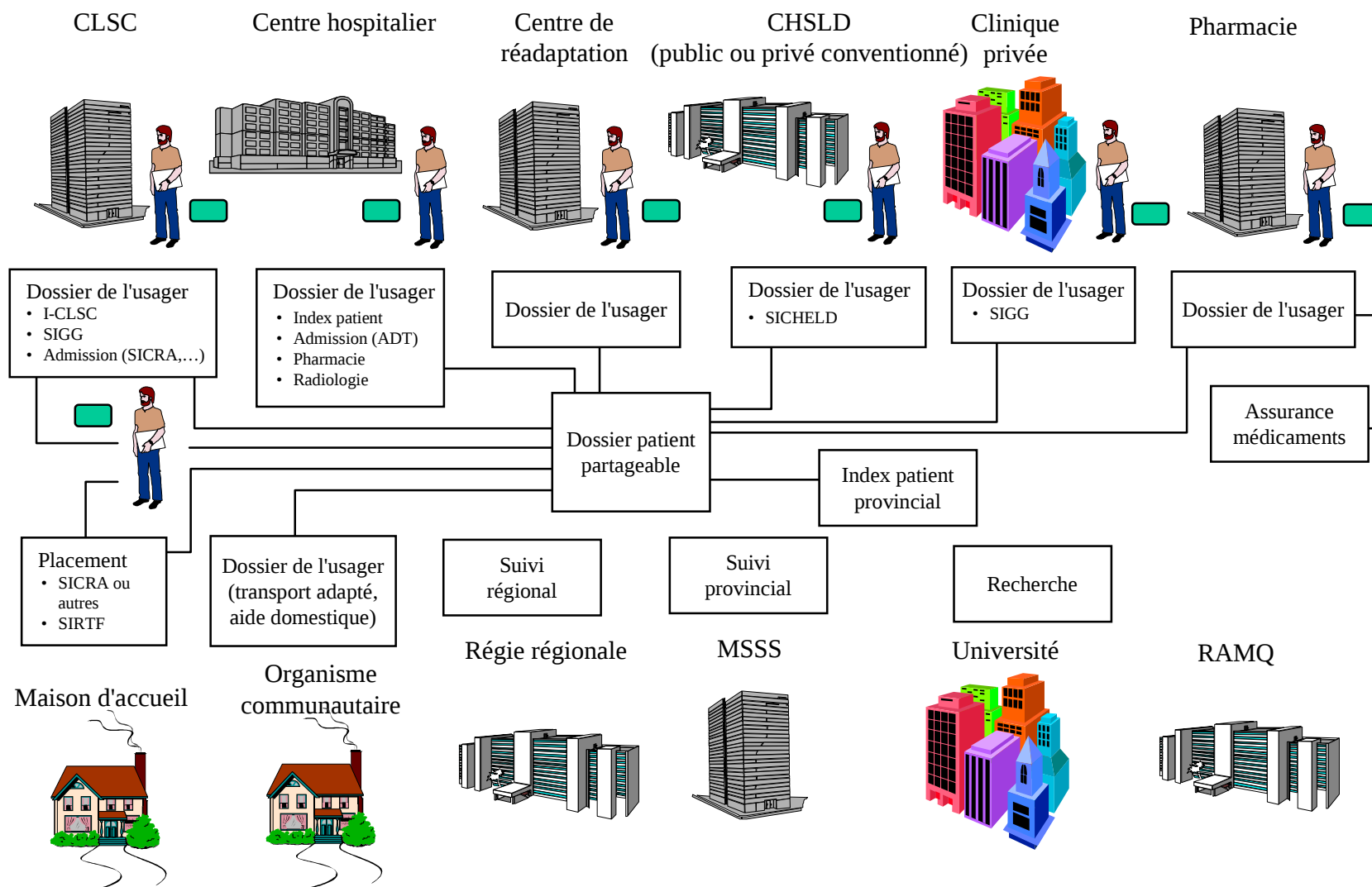


Diagramme 2 : Exemple de la personne en perte d'autonomie



Ces scénarios démontrent de façon concrète que des systèmes fiables et partageables d'information relative aux soins et à la gestion sont effectivement essentiels à une réelle intégration des services. Une multitude d'autres scénarios du même type peuvent appuyer cette conclusion. Le tableau ci-après donne un aperçu de plusieurs situations qui s'y prêteraient aisément.

Exemples de scénarios cliniques ou de santé publique	Exemples de scénarios de gestion de ressources
Services préhospitaliers Traitement du cancer Santé mentale Programmes de dépistage Info-Santé Vaccination (ex. : méningite) Déficience intellectuelle Jeunes en difficulté d'adaptation Toxicomanie Programmes de recherche	Allocation budgétaire Répartition des effectifs médicaux Formation du personnel Équipements biomédicaux Approvisionnements (nourriture, médicaments, buanderie, etc.) Administration (comptabilité, paie du personnel, etc.)

1.1.3 *Plan d'action en matière de ressources informationnelles*¹⁰

Tout en démontrant la nécessité de systèmes fiables pour partager l'information, le plan stratégique ministériel laisse entrevoir l'ampleur des besoins en informatisation du réseau. Les ressources financières et humaines actuelles obligent à procéder par priorités. À cet égard, le plan d'action en matière de ressources informationnelles :

- détermine les priorités retenues aux fins de la planification des projets de systèmes d'information ;
- définit les concepts généraux d'infrastructures nécessaires au soutien des projets de systèmes d'information en fonction des priorités retenues.

Compte tenu des orientations stratégiques pour 2001-2004, les priorités retenues en matière de ressources informationnelles pour la même période sont les suivantes.

Première priorité : Arrimer les développements de systèmes dans une vision d'ensemble.

La première priorité implique la réalisation de l'architecture de l'information et des systèmes d'information du réseau sociosanitaire. Cette architecture donnera au Ministère et au réseau une vision intégrée et partagée des besoins et des

10. *Le Plan stratégique des ressources informationnelles 2001-2004*, document présenté au colloque sur les ressources informationnelles, François Turenne, MSSS, 12 juin 2001, 17 p.

mesures nécessaires pour soutenir les priorités énoncées dans le plan stratégique ministériel. De cette architecture découleront les cadres de gestion et les cadres normatifs requis en matière d'échange d'informations, de données minimales, de sécurité, de protection des renseignements personnels et de gestion du consentement. Ces cadres normatifs et ces cadres de gestion sont nécessaires à l'encadrement des projets de systèmes d'information du réseau.

Cette priorité implique également l'implantation d'une infrastructure nationale d'exploitation de données au moyen de la mise en réseau des infocentres. Une telle infrastructure a pour but de soutenir l'accessibilité et la qualité des données. Ainsi, la mise en réseau des infocentres permettra d'utiliser les contenus informationnels et l'expertise du réseau sociosanitaire pour offrir les services d'exploitation en fonction des besoins des différentes organisations.

Deuxième priorité : Mettre en place l'infrastructure nationale d'accès et d'échange d'information entre les intervenants.

La deuxième priorité prend appui sur le Réseau de télécommunications sociosanitaire, le RTSS, qui permet de relier tous les établissements publics de santé et de services sociaux. Cette infrastructure, robuste et sécuritaire, constitue le noyau autour duquel pourront s'élargir les échanges avec, notamment, les partenaires participant à la prestation de services du réseau sociosanitaire.

Ainsi, la première action, sous ce volet, consiste à ouvrir le RTSS en établissant des liens de communication avec les groupes de médecine de famille. Différentes mesures de sécurité sont déjà prévues pour assurer le branchement des premiers groupes.

La deuxième infrastructure visée est le portail santé québécois. Le portail est la porte d'accès principale à l'ensemble des informations et des services électroniques dont ont besoin les différents acteurs du réseau dans l'exercice de leurs fonctions. Cette porte sera éventuellement ouverte aux usagers du réseau et à la population du Québec en général afin de favoriser l'accessibilité des services du réseau. Le portail permet d'unir les organisations du réseau de la santé et des services sociaux au sein d'une même grande entreprise virtuelle et de soutenir leurs relations avec leurs partenaires externes. Ce type d'infrastructure permet notamment de gérer les besoins en information de chaque personne travaillant dans cette entreprise en fonction de son rôle et de ses droits d'accès aux applications et aux services électroniques.

Sur le plan fonctionnel, l'accès à l'information et l'échange d'information nécessitent également des infrastructures, telles que l'identificateur unique et le dossier patient partageable, et des mécanismes qui permettent les échanges, tels que l'outil requête-résultat générique. Le développement de ces infrastructures doit être arrimé au projet Carte Accès Santé Québec de la Régie de l'assurance maladie du Québec. En effet, ce projet, adopté par le gouvernement en avril

2001, vise à offrir au réseau sociosanitaire les services d'application pour la gestion de l'index patient national et du dossier carte santé ainsi que pour la gestion du consentement en fonction des règles de sécurité et de protection des renseignements personnels. Des travaux sont prévus afin que les arrimages s'effectuent notamment sur la base des orientations technologiques du réseau.

À la deuxième priorité est également associé le plan de mise en œuvre des orientations technologiques du réseau. Ce dernier prévoit la mise en place de services électroniques communs qui permettent de gérer de manière intégrée les services intranet, la sécurité, les échanges entre les applications et l'exploitation des infrastructures technologiques. Ces services seront obligatoires et toutes les nouvelles applications auront à s'y conformer.

En outre, des actions plus particulières viseront la mise en place des mécanismes de gestion des infrastructures et des mesures de relève destinées à garantir l'accessibilité et la performance de ces infrastructures communes.

Troisième priorité : Améliorer progressivement l'équipement requis pour la télésanté.

Les besoins en télésanté sont nombreux et touchent plusieurs spécialités. Aussi, les actions sous ce volet consistent principalement à améliorer les liens de communication des établissements demandeurs afin de les relier à haute vitesse aux divers centres de référence du Québec.

En corollaire, les équipements qui supportent dans chaque domaine la télésanté spécialisée devront être déployés. Les besoins à cet égard sont analysés cas par cas par la table ministérielle de télésanté.

Quatrième priorité : Mettre en place les applications nationales prioritaires.

La quatrième priorité vise la réalisation des systèmes d'information retenus dans le plan stratégique ministériel 2001-2004 afin de soutenir la gestion de problèmes importants et récurrents dans le réseau sociosanitaire. Les besoins concernent la gestion des activités transfusionnelles et d'hémovigilance (SIIATH), la gestion de l'accès aux services (SGAS), la gestion des départements d'urgence (SIGDU) ainsi que l'établissement de prix de revient et de coût par service rendu.

Cinquième priorité : Terminer le déploiement des systèmes d'information du secteur social.

Plusieurs systèmes du secteur social arrivent à la fin de leur réalisation ou en sont à la phase de déploiement dans le réseau. Aussi, les efforts qui sont consentis dans le plan d'action visent à finaliser ces projets, et ce, dans les meilleures conditions possibles pour les usagers du réseau et les utilisateurs de ces systèmes.

Dans le secteur jeunesse, les applications visées sont le Projet intégration jeunesse (PIJ), le Système de soutien à la pratique jeunesse (SSPJ) ainsi que le Système d'information sur les ressources intermédiaires et les ressources de type familial (SIRTF). Dans le domaine des soins de longue durée, le déploiement du Système d'information pour les centres d'hébergement et de soins de longue durée (SICHELD) doit être finalisé dans les quelques établissements restants ; de plus, des travaux complémentaires sont prévus pour la mise à jour des protocoles de soins. Enfin, des modules complémentaires au système Intégration CLSC (I-CLSC) devront être développés afin de soutenir les activités de maintien à domicile des CLSC et l'intégration au SICHELD.

Le plan d'action ministériel des ressources informationnelles annonce des concepts et des initiatives qui convergent avec les tendances constatées à l'échelle mondiale tout en répondant aux besoins plus immédiats du système québécois de services de santé et de services sociaux.

En matière technologique, et pour peu que le Québec évolue de façon comparable aux autres pays, les voies qui apparaissent les plus prometteuses sont :

- la mise en place de services électroniques communs en vue de soutenir le continuum des soins et services aux usagers ;
- la prévision d'une capacité de soutien des conventions d'échange de contenus informationnels afin de permettre le partage d'information ;
- la mise en place d'infrastructures constituant une assise qui garantisse la sécurité et la protection des renseignements personnels ;
- l'utilisation des technologies favorisant des échanges électroniques évolués et l'ouverture entre les applications ;
- un virage vers des technologies du type Internet.

1.4 Un modèle de gestion des ressources informationnelles renouvelé

La situation technologique du réseau, l'évolution du marché des technologies de l'information et les orientations stratégiques du réseau sont des éléments déterminants dans la définition des orientations technologiques. Le cadre de gestion est également un élément d'une grande importance dans le succès de la mise en œuvre d'une architecture des ressources informationnelles, y compris les orientations technologiques.

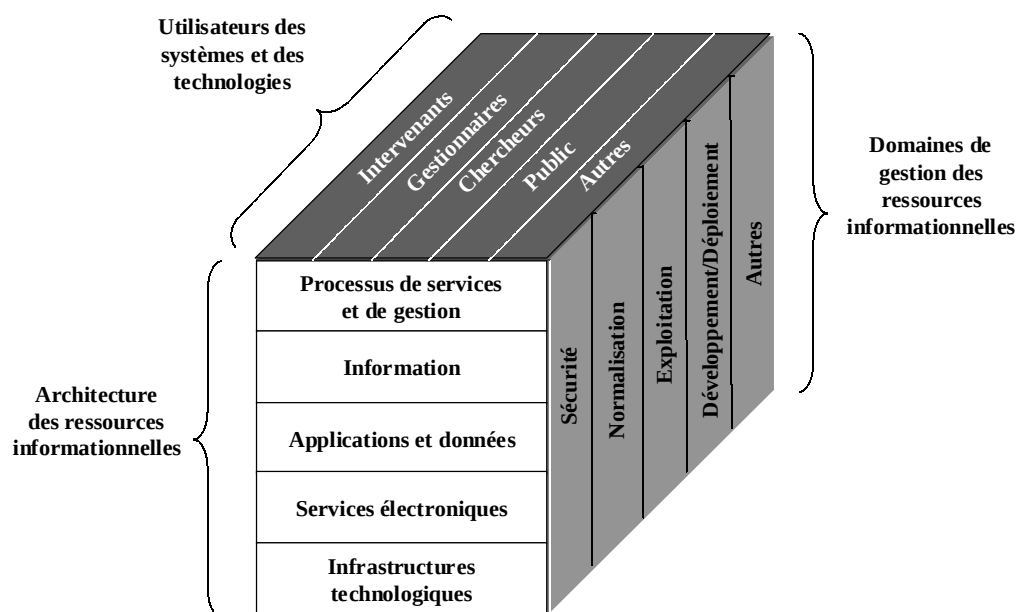
Or, la modernisation du modèle de gestion des ressources informationnelles est requise, particulièrement au regard des actifs informationnels communs du réseau. Les principes directeurs qui sous-tendent ce modèle de gestion sont les suivants :

- *la reconnaissance de la nécessité de s'appuyer sur une vision commune des besoins et des mesures* susceptibles d'améliorer la qualité des informations, de permettre l'interopérabilité des systèmes et de favoriser la réutilisation des composantes. Cette vision doit faire en sorte de susciter une collaboration concrète afin de relever les défis collectifs, en particulier en ce qui a trait au partage d'informations cliniques ;
- *l'adoption d'un cadre de référence qui permette la normalisation des systèmes d'information et des infrastructures technologiques*, et ce, en rendant facilement accessibles les informations les plus à jour en matière de ressources informationnelles ;
- *la mise en place des mécanismes requis pour soutenir l'utilisation de ce cadre de référence*, et ce, dans un esprit de coopération mutuelle.

Le nouveau modèle de gestion s'appuie sur les axes suivants :

- l'architecture des ressources informationnelles ;
- les besoins des différents groupes d'utilisateurs des systèmes et des technologies ;
- les domaines de gestion des ressources informationnelles.

Le diagramme 3 illustre le modèle de gestion intégrant ces trois axes.

Diagramme 3 : Modèle de gestion des ressources informationnelles

L'architecture des ressources informationnelles comprend toutes les couches d'objets à gérer pour concevoir, réaliser et mettre en œuvre les systèmes d'information, soit :

- les processus de services aux usagers du réseau ainsi que les processus de gestion de ces services et des ressources ;
- l'information ou les extrants des systèmes d'information servant aux utilisateurs dans les processus de services et de gestion ;
- les applications et les données ou, en d'autres termes, les programmes informatiques qui traitent les données pour produire l'information ;
- les services électroniques, c'est-à-dire l'ensemble des fonctions nécessaires aux utilisateurs et aux applications pour obtenir et traiter l'information ainsi que pour communiquer ;
- les infrastructures technologiques qui comprennent les équipements, les logiciels et les services de télécommunications sur lesquels s'appuient les applications et les services électroniques pour permettre les communications et livrer l'information.

L'axe des groupes d'utilisateurs représente les clientèles cibles des systèmes d'information du réseau : les intervenants, les gestionnaires, les chercheurs, le public et les autres. Bien que sommaire dans le diagramme, cet axe rappelle que

les systèmes d'information ne sont pas une fin en soi et qu'ils doivent répondre aux besoins des utilisateurs.

Enfin, l'axe des domaines de gestion des ressources informationnelles met en évidence les diverses dimensions que doit considérer la gestion des ressources informationnelles, soit : la sécurité, la normalisation, l'exploitation, le développement et le déploiement, notamment. Cette liste n'est pas complète¹¹ ; elle mentionne cependant les domaines de gestion qui sont directement concernés par les orientations technologiques.

Compte tenu de ces trois axes, le nouveau modèle de gestion des ressources informationnelles permet :

- de positionner les projets nationaux et les initiatives des organisations dans le modèle en fonction de leur nature et de définir ainsi leur contribution à l'atteinte des objectifs stratégiques du réseau en matière de ressources informationnelles¹² ;
- d'appuyer les rôles et les responsabilités des différents acteurs engagés dans le développement et l'évolution des ressources informationnelles du réseau ;
- de prévoir les mécanismes de soutien à l'architecture des ressources informationnelles, à la coordination des projets et à chacun des domaines de gestion prévus au modèle.

En ce qui concerne ce dernier point, précisons qu'un mécanisme de gestion des orientations technologiques est défini dans la planification de mise en œuvre au chapitre 4 du présent document.

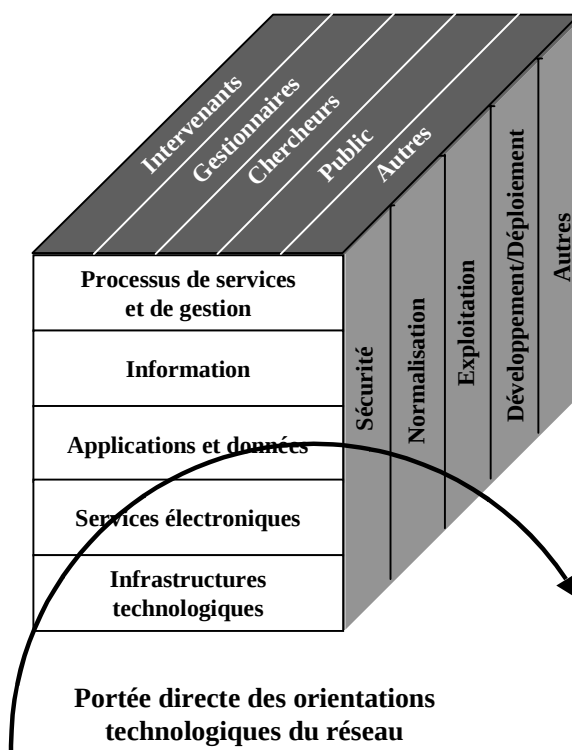
1.5 La portée des orientations technologiques

Selon le modèle de gestion des ressources informationnelles présenté précédemment, la portée des orientations technologiques du réseau consiste à définir, dans une perspective générale, les couches architecturales ayant trait aux services électroniques et aux infrastructures technologiques, en appui aux autres couches d'architecture.

Le diagramme 4 reprend le modèle de gestion des ressources informationnelles pour illustrer les couches d'architecture sur lesquelles portent plus directement les orientations technologiques.

11. Outre ceux qui ont déjà été mentionnés, les domaines couverts par le cadre de gestion sont : la protection des renseignements personnels, le financement, le partenariat, la gestion de la propriété des actifs, la commercialisation, la certification des applications et la planification d'ensemble.

12. Ce modèle peut être utilisé pour positionner autant des projets d'encadrement (tels que la planification stratégique des ressources informationnelles ou l'architecture globale de l'information) que des projets de réalisation technique (par exemple, un système d'information particulier ou la mise en place d'une infrastructure technologique).

Diagramme 4 : Portée des orientations technologiques

Comme l'illustre le diagramme, les orientations technologiques portent avant tout sur les services électroniques et les infrastructures technologiques. Elles influencent certains aspects de la couche des applications et des données à cause de la vision technologique sur laquelle ces dernières devront s'appuyer. En effet, les orientations technologiques prévoient la mise en place de services électroniques communs et d'infrastructures technologiques partagées ; les applications devront nécessairement être conçues de façon à favoriser l'utilisation de ces services et infrastructures afin que soient assurées l'intégration de l'information et l'interopérabilité des applications.

Par rapport à l'axe des clientèles, les orientations technologiques ont été définies en fonction des besoins de certaines clientèles sur la base de domaines d'applications particuliers. C'est ainsi que des orientations ont été définies pour les domaines d'application suivants :

- les services électroniques aux intervenants relativement aux dossiers des usagers ;
- les téléservices ;
- les services électroniques d'information sur les ressources et les services (ou services informationnels) ;

- les services électroniques de gestion des ressources ;
- les services électroniques de sécurité intégrée ;
- les services en matière de télécommunications.

Par ailleurs, la version actuelle des orientations technologiques tient compte des besoins de l'ensemble des acteurs du système de santé et des services sociaux (ce qui inclut les partenaires privés), mais exclut les besoins du public, c'est-à-dire les usagers du réseau et la population québécoise en général. L'approche et les sujets ont été déterminés en fonction des priorités pour le réseau, des ressources existantes et des délais impartis au projet d'actualisation des orientations technologiques.

Plusieurs autres sujets technologiques d'intérêt, tels que la gestion des connaissances, les choix d'outils de développement de systèmes et les télécommunications sans fil n'ont pas été retenus non plus. Ils seront éventuellement couverts dans des travaux ultérieurs.

Enfin, les orientations technologiques influencent les décisions qui peuvent être prises à l'égard des rôles et des responsabilités qui incombent aux différents acteurs dans chacun des domaines de gestion précisés par le modèle. C'est ainsi que, dans le domaine de la normalisation, le document sur les orientations technologiques décrit un processus en matière d'application et d'évolution des orientations technologiques. La mise en place de ce processus nécessitera une définition du cadre de gestion propre à ces activités. De même, les énoncés d'orientations concernant les services électroniques communs et les infrastructures technologiques partagées impliqueront une révision des cadres de gestion propres à la sécurité, au développement et à la gestion des infrastructures communes du réseau.

C'est donc dans une perspective générale que la présente version des orientations technologiques aborde les sujets suivants :

- la description du contexte technologique du réseau, qui a été présentée dans le présent chapitre ;
- des orientations générales comprenant de grands principes de gestion des systèmes et des technologies ainsi que la description du modèle technologique à mettre en œuvre ;
- des orientations spécifiques sur des domaines d'application particuliers ;
- un plan de mise en œuvre destiné à concrétiser les orientations technologiques.

2 LES ORIENTATIONS TECHNOLOGIQUES GÉNÉRALES

Fortement axées sur les télécommunications, le partage d'infrastructures et la normalisation des technologies, les orientations technologiques antérieures ont fourni un cadre de référence qui a guidé l'évolution du réseau vers la mise en place de plusieurs des infrastructures actuelles, dont le RTSS, les services Lotus Notes, certains systèmes d'information en réseau ainsi que les technocentres national et régionaux. En se dotant de telles infrastructures, le réseau a franchi une étape importante vers le fonctionnement selon le mode d'entreprise étendue.

Pendant que les nouvelles orientations stratégiques du réseau et la redéfinition du cadre de gestion des ressources informationnelles tracent la voie à une organisation des services plus efficace, l'effervescence de l'industrie des technologies de l'information fait également apparaître des perspectives pouvant contribuer favorablement à la performance et à la qualité des services de santé et des services sociaux offerts à la population québécoise.

L'actualisation des orientations technologiques du réseau s'inscrit nettement dans la foulée des stratégies du réseau, des actions qui en découlent et de l'utilisation des nouvelles technologies. Elle se veut aussi un prolongement du mouvement déjà engagé en faveur d'une entreprise réseau étendue qui reliera l'ensemble des organisations concernées par la livraison des services aux usagers, qu'elles soient publiques ou privées.

Les présentes orientations technologiques définissent donc un cadre de référence qui inclut à la fois les services électroniques et les infrastructures technologiques du réseau. Ce cadre constitue un des éléments clés de l'architecture d'ensemble qui vise :

- à soutenir la réalisation des orientations stratégiques du réseau en matière de services aux usagers et de ressources informationnelles ;
- à mettre en place les services électroniques communs et les infrastructures technologiques partagées nécessaires aux organisations du réseau pour leurs échanges d'informations entre elles et avec leurs partenaires ;
- à améliorer les pratiques de gestion des technologies de l'information et des communications et à faire évoluer ces technologies en tenant compte des tendances marquées de l'industrie.

Compte tenu de ces objectifs, les orientations technologiques générales présentent :

- des *principes directeurs* qui constituent des points de repère destinés à guider l'évolution des technologies au sein du réseau ;
- un *modèle technologique de référence* qui décrit le cadre technique général retenu pour orienter l'évolution technologique du réseau.

2.1 Les principes directeurs de gestion des technologies de l'information

Les principes directeurs énoncent des lignes de conduite générale concernant la gestion et l'évolution des technologies de l'information. Ces principes couvrent trois niveaux de considération, soit les ressources informationnelles, les systèmes d'information et les technologies.

Principes relatifs à l'évolution des ressources informationnelles

Les principes qui suivent se rapportent plus particulièrement à la gestion d'ensemble des ressources informationnelles.

Principe 1 : Guider l'évolution technologique selon les stratégies gouvernementales adoptées pour le secteur de la santé et des services sociaux.

La Loi sur l'administration publique, la Politique d'utilisation du français dans les technologies de l'information, la Politique québécoise de l'autoroute de l'information et les résultats de travaux y afférents (comme l'architecture d'entreprise gouvernementale¹³ et l'architecture globale de sécurité de l'information numérique¹⁴) sont indicatifs des stratégies gouvernementales en matière de technologies de l'information et des communications.

Le plan stratégique ministériel, déposé à l'Assemblée nationale du Québec, et le plan d'action en matière de ressources informationnelles, défini par le Ministère, énoncent les stratégies propres au secteur socio-sanitaire.

De plus, les orientations technologiques du réseau souscrivent aux stratégies gouvernementales tout en poursuivant des objectifs adaptés aux besoins du réseau et reliés aux stratégies plus particulières au secteur de la santé et des services sociaux. Elles présentent les moyens techniques retenus pour concrétiser ces stratégies.

13. Le projet AEG est réalisé par le Secrétariat du Conseil du trésor.

14. Le projet AGSIN est réalisé par le Secrétariat du Conseil du trésor.

Principe 2 : Faire évoluer les orientations en assurant une veille stratégique et technologique continue afin de tenir compte des nouvelles réalités du réseau et de l'industrie des technologies de l'information.

Les stratégies de transformation organisationnelle évoluent constamment afin de répondre à des pressions de nature sociale, politique, économique, technologique ou autre. De leur côté, les technologies de l'information et des communications progressent rapidement et créent de nouvelles opportunités dans tous les secteurs d'activités.

L'étendue du domaine que doivent couvrir les orientations technologiques, les ressources existantes et les délais de réalisation limitent la portée des orientations. Cela fait en sorte que les orientations présentent une vision valable d'évolution au moment de leur définition et traitent des sujets jugés les plus importants. Certains sujets technologiques ne sont donc pas couverts dans la présente version des orientations.

En conséquence, une veille stratégique et technologique continue est nécessaire pour s'assurer que les orientations technologiques demeurent en rapport avec les stratégies de services du réseau. Cette veille vise à compléter et à améliorer les orientations en tenant compte des progrès de l'industrie des technologies de l'information ainsi que de l'évolution des stratégies gouvernementales et ministérielles.

Principes relatifs aux systèmes d'information

Les principes qui suivent se rapportent plus particulièrement à la conception des systèmes d'information.

Principe 3 : Intégrer les moyens technologiques aux méthodes de travail de façon à maximiser les bénéfices de l'informatisation.

L'amélioration de la performance des processus de travail par l'utilisation de systèmes et de technologies est tributaire de l'intégration de ces systèmes et technologies aux méthodes de travail des utilisateurs. Aux fins de cette intégration, les systèmes et les technologies doivent généralement offrir aux utilisateurs les caractéristiques suivantes :

- un accès facile aux informations et une convivialité adéquate ;
- un soutien interactif à la réalisation des opérations ;
- une assistance qui permette à l'utilisateur d'être le plus autonome possible dans son travail ;

- un niveau de service adapté aux besoins des utilisateurs et aux tâches à accomplir.

Les utilisateurs des systèmes et des technologies doivent également recevoir une formation suffisante et pouvoir obtenir un soutien adéquat lorsqu'ils en ont besoin.

Principe 4 : Respecter le cadre légal et réglementaire en matière de sécurité des systèmes et de protection des renseignements personnels.

La présence d'informations nominatives dans les systèmes du réseau, telles que les données personnelles sur les usagers, impose le respect des lois et des règles qui régissent l'utilisation de ces informations.

Selon le cadre légal présentement en vigueur au Québec, les données nominatives sur les usagers sont sous la responsabilité directe des établissements. Elles peuvent être déposées à la RAMQ lorsque les établissements lui confient explicitement un mandat à cet égard. Les données nominatives peuvent être partagées à l'intérieur d'un même établissement et elles peuvent être échangées entre des établissements, si l'utilisateur y consent et si elles sont nécessaires pour lui rendre les services que son état requiert. Enfin, le ministre peut également obtenir des données nominatives. Des changements légaux sont nécessaires pour permettre d'autres possibilités de gestion ou d'échange de données nominatives sur les usagers.

Les systèmes et les technologies qui utilisent les données nominatives sur les usagers doivent donc comporter les mécanismes qui assurent une protection adéquate des renseignements personnels. Ces mécanismes comprennent notamment la gestion du consentement à l'utilisation des données personnelles des usagers du réseau ainsi que la gestion de l'accès à l'information et de la confidentialité des informations, ce qui inclut la journalisation des accès.

Par ailleurs, la protection des renseignements personnels s'applique aussi aux données nominatives sur le personnel du réseau, qui sont protégées par les lois concernant l'accès à l'information. Ces données doivent donc elles aussi faire l'objet d'une attention particulière.

Principe 5 : Concevoir les systèmes d'information de manière à permettre le partage des informations et à favoriser la mise en commun des ressources.

Dans le but de faciliter les échanges électroniques d'information et de capitaliser sur les actifs informationnels communs du réseau, il faut, au moment de la conception des systèmes :

- prévoir et soutenir les échanges d'information avec les autres systèmes en respectant les conventions adoptées selon l'architecture globale de l'information, les cadres normatifs et les orientations technologiques du réseau ;
- utiliser les services électroniques communs du réseau;
- privilégier l'utilisation d'infrastructures technologiques partagées et l'interopérabilité avec les infrastructures et les systèmes existants.

Principe 6 : Soutenir la normalisation des données ainsi que la saisie unique et un niveau de qualité élevé.

La normalisation des données est indispensable à la connectivité sans faille entre les systèmes. Elle permet d'améliorer l'accessibilité, la qualité des données (fiabilité, validité, comparabilité) et l'information diffusée. Pour ces mêmes raisons, la discipline d'échange des données doit elle aussi être normalisée.

À ces fins, une approche globale de normalisation doit être définie dans le cadre d'une gestion d'ensemble, et ce, d'une manière qui tienne compte des progrès de la normalisation sur le plan international (classifications, architecture de documents d'ordre clinique, etc.).

Les efforts pour la normalisation des données et la discipline d'échange doivent faire en sorte que les données soient saisies une seule fois pour être utilisées de façon intègre dans chaque système où elles figurent. Ils doivent aussi faire en sorte que les données soient validées préférentiellement dès leur saisie afin d'en assurer la qualité.

Principes relatifs aux technologies

Les principes qui suivent se rapportent plus particulièrement à la gestion des orientations technologiques ainsi qu'à la définition des architectures technologiques et des choix techniques.

Principe 7 : Maximiser l'utilisation des ressources en contrôlant l'évolution des technologies selon une perspective globale.

Une perspective globale doit être adoptée afin d'assurer un meilleur contrôle de l'évolution des technologies dans le réseau socio sanitaire puisque ce dernier est vu sous l'angle d'une entreprise étendue. Les orientations stratégiques et technologiques du réseau contribuent à définir la perspective globale. Celle-ci permet de positionner les systèmes de portée commune et les infrastructures qui contribuent à l'entreprise réseau.

La perspective globale doit faire en sorte de retenir les meilleures orientations afin d'obtenir la meilleure qualité et la meilleure performance des échanges d'information entre les différentes organisations du secteur socio-sanitaire. Elle doit aussi guider les développements de systèmes d'information pour les aspects visant leur interopérabilité.

L'évolution des technologies dans une perspective globale favorise notamment :

- l'intégration des informations, des systèmes et des infrastructures technologiques ;
- la normalisation des mécanismes d'échange d'informations ;
- l'utilisation optimale des systèmes et des infrastructures existantes ;
- le regroupement des acquisitions afin de bénéficier des meilleurs rapports qualité-prix ;
- le partage d'expertises et de connaissances sur le plan technologique.

Un mécanisme de révision des architectures et un processus de certification des applications concourent à l'application de ce principe.

Principe 8 : Rationaliser les environnements technologiques en limitant la diversité et en assurant l'intégration à la mosaïque technologique globale du réseau socio-sanitaire.

Compte tenu de l'évolution des technologies et de leurs caractéristiques fonctionnelles, une certaine diversité technologique est pratiquement inévitable. Une trop grande diversité entraîne cependant des coûts additionnels de gestion, de développement, de soutien et d'exploitation. Le réseau socio-sanitaire doit donc chercher à limiter la diversité tout en demeurant ouvert à l'évolution.

Les orientations technologiques mettent l'accent sur l'interopérabilité des systèmes ainsi que sur l'utilisation de services communs fonctionnant sur des infrastructures partagées. À cette fin, elles définissent un modèle de référence et des règles d'architecture, y compris des normes techniques qui doivent être respectées. Ce modèle et ces règles se prolongent dans les conditions d'intégration au RTSS de manière à s'assurer que l'encadrement technologique adopté par le réseau est effectivement appliqué.

Le respect de ce principe conduit à une meilleure intégration des systèmes et des technologies. Il en facilite l'évolution et le soutien tout en permettant de réduire les coûts globaux d'acquisition, d'entretien et d'exploitation.

Principe 9 : Garantir la performance des systèmes, la sécurité des actifs informationnels et la continuité opérationnelle adéquate des systèmes.

L'importance de pouvoir accéder aux informations au moment opportun et dans des délais acceptables demande que les systèmes soient performants, intègres et disponibles. L'intégrité et la performance transactionnelle de bout en bout doivent également être garanties, particulièrement pour certaines applications critiques. Les systèmes et les technologies doivent donc être gérés de manière à ce que :

- les capacités techniques soient suffisantes ;
- les mécanismes adéquats de contrôle soient intégrés aux infrastructures ;
- les applications et les données soient adéquatement protégées tout au long de leur cycle de vie (création, mise à jour, stockage, consultation, archivage, disposition) ;
- les mécanismes d'urgence et de relève requis permettent d'assurer une disponibilité suffisante ;
- des outils adéquats supportant cette gestion d'infrastructure soient déployés.

Le respect de ce principe implique éventuellement une classification des applications en fonction de leur portée sur les services du réseau. En effet, contrôler la seule performance du RTSS ne suffit pas ; il faut aussi contrôler celle des applications et mettre en place le support organisationnel (ressources humaines) adéquat pour gérer les problèmes qui surviennent.

Principe 10 : Privilégier l'utilisation de technologies conformes aux normes de l'industrie afin de favoriser l'interopérabilité des systèmes.

Dans l'industrie des technologies de l'information et des communications, la normalisation se développe selon différentes modalités, ce qui donne lieu à toute une gamme de normes. À un pôle, une norme est dite propriétaire quand elle émane d'un fournisseur. À l'autre pôle, la norme est dite ouverte, notamment parce que l'organisation qui la définit est réputée indépendante des fournisseurs (ISO, IEEE, ANSI, Internet Society, HL7). Entre les deux pôles, il existe une variété de normes, plus ou moins ouvertes, définies par des organisations représentant tantôt des fournisseurs, tantôt des utilisateurs.

De façon générale, le respect des normes les plus ouvertes favorise davantage la portabilité des applications, les interconnexions et l'interopérabilité des systèmes. Par ailleurs, une norme à déploiement international, qu'elle soit ouverte ou propriétaire, peut avoir des effets similaires à une norme ouverte.

Les technologies respectant des normes ouvertes ou des normes à grand déploiement doivent donc être privilégiées. Ce principe est également applicable au regard des communications entre les applications et entre les composantes d'application.

2.2 Le modèle technologique de référence

Le *modèle technologique de référence* présente le cadre technique général retenu pour orienter l'évolution technologique du réseau. Avec les principes directeurs de gestion des technologies, ce modèle constitue le fondement des orientations technologiques du réseau.

Le modèle de référence prend appui sur un ensemble de prémisses issues du contexte technologique du réseau et il comprend les éléments suivants :

- un ensemble d'énoncés généraux de direction ;
- des perspectives conceptuelles d'évolution technologique ;
- des règles d'architecture technologique.

La présente section traite des prémisses et des éléments du modèle technologique de référence.

2.2.1 Prémisses du modèle technologique de référence

Le contexte technologique du réseau permet de faire plusieurs constats, dont les suivants :

- les stratégies ministérielles traduisent la volonté du milieu socio-sanitaire de poursuivre sa progression vers une mise en commun des informations afin de soutenir le continuum des soins et services, la performance du réseau et la qualité des services ;
- les systèmes d'information du réseau seront conçus de plus en plus dans la double optique de la coopération entre les organisations et la mise à profit des infrastructures d'échange et de partage d'informations ;
- la protection des renseignements personnels, qui est un enjeu de société particulièrement sensible en matière de services de santé et de services sociaux, doit être gérée adéquatement ;
- les ressources financières, humaines et technologiques du réseau sont limitées et sont réparties dans un grand nombre d'organisations ;

- la diversité technologique est inéluctable compte tenu d'un marché en évolution rapide, de la présence de plusieurs générations de systèmes et du recours à de multiples fournisseurs misant sur des produits différents.

Ces constats sont représentatifs des grands défis que doit relever le réseau sociosanitaire en matière de ressources informationnelles. Les orientations technologiques représentent une part importante de la solution. En effet, les éléments d'architecture technologique définis par les orientations sont cruciaux à l'interopérabilité des systèmes et aux échanges électroniques d'informations.

Plusieurs orientations et éléments d'architecture technologique peuvent être déterminés avant que des architectures globales d'information ou de systèmes aient été formellement définies. L'adoption de telles orientations permet de mettre en place plus rapidement des composantes structurantes essentielles à l'évolution technologique. Ces orientations servent aussi de levier au regard des autres architectures.

Cependant, les orientations technologiques ne peuvent garantir à elles seules le succès de l'intégration de l'information nécessaire au soutien de la mission des organisations. Les différentes architectures (information, systèmes et technologies, par exemple) devront donc être arrimées à une architecture d'ensemble, conçue sur le modèle d'une entreprise étendue, afin de gérer adéquatement toutes les dimensions des ressources informationnelles du réseau¹⁵.

À cet égard, rappelons que les couches de l'architecture des ressources informationnelles s'influencent mutuellement. En effet, du point de vue des processus d'affaires et de gestion, l'information, les applications et les technologies permettent de transformer en profondeur le fonctionnement des organisations. Par ailleurs, du point de vue technologique, les services électroniques et les infrastructures sont des moyens de concrétiser les orientations stratégiques ainsi que les architectures d'information, d'application et de données.

Compte tenu du contexte, de la nécessité des orientations technologiques, des expériences antérieures du réseau en cette matière ainsi que des pratiques observables dans d'autres milieux pour des situations comparables¹⁶, la démarche retenue :

- présente une position ferme quant à l'évolution prévue et souhaitée pour le réseau sociosanitaire québécois en matière de technologies de l'information et des communications ;
- détermine les éléments d'architecture technologique les plus cruciaux pour encadrer la conception des systèmes d'information, de façon à soutenir :

15. Cette façon de faire est recommandée dans des articles de GartnerGroup et fait partie d'approches reconnues, dont celle de MetaGroup.

16. Par exemple, l'architecture d'entreprise gouvernementale réalisée par le Secrétariat du Conseil du trésor.

- la simplicité d'utilisation des systèmes et des technologies,
- la communication et le partage des informations,
- la protection des renseignements personnels et la sécurité des actifs informationnels,
- les meilleures pratiques de gestion des technologies ;
- suppose une approche de gestion à la fois rigoureuse, en ce qui concerne les éléments d'architecture retenus, et souple, de façon à suivre l'évolution rapide du marché des technologies ;
- retient les concepts les plus prometteurs devant s'appliquer progressivement aux systèmes d'information et aux technologies, ce qui implique une phase de transition au cours de laquelle des solutions intermédiaires seront adoptées.

Ces prémisses sont donc évocatrices des considérations importantes qui ont prévalu dans la définition des orientations technologiques du réseau.

2.2.2 Énoncés généraux de direction

Première composante du modèle technologique de référence, les énoncés généraux de direction précisent la vision d'évolution technologique au moyen d'une terminologie non technique. Ces énoncés sont importants, car les perspectives conceptuelles et les règles d'architecture décrites par la suite traduisent la vision en termes techniques et sont, par conséquent, moins facilement accessibles aux non-spécialistes.

Énoncé 1 : Moderniser l'environnement de travail du personnel du réseau en misant sur les nouvelles technologies de l'information et en assurant une utilisation optimale des technologies en place.

Conséquemment à ce premier énoncé de direction, les solutions technologiques doivent faire en sorte :

- d'élargir l'accessibilité et l'éventail des services offerts aux utilisateurs des systèmes d'information et des technologies afin de répondre à leurs besoins en information (dossier électronique de l'utilisateur, information sur les services et les ressources, connaissances, etc.) ;
- d'offrir à l'utilisateur une interface intégrée d'accès sécurisé et adaptatif (paramétrable) pour l'ensemble des services électroniques (applications, information et intranet, par exemple) ;

- de prévoir des mécanismes permettant une harmonisation des systèmes patrimoniaux¹⁷ avec les nouveaux systèmes.

Énoncé 2 : Accentuer le mouvement de mise en commun d'informations, d'applications et d'infrastructures engendré par la formation de regroupements d'utilisateurs et de communautés de pratique.

Conséquemment à ce second énoncé de direction, les solutions technologiques doivent faire en sorte :

- de soutenir les échanges évolués entre les utilisateurs et entre les organisations en assurant une gestion adéquate de la transaction et des contenus informationnels ;
- de faciliter l'harmonisation des processus de prestation des services entre eux et avec les processus de gestion des services et des ressources ;
- de permettre la mise en place, la gestion et l'utilisation de banques d'information de référence définissant l'information commune et ses structures de contenu ;
- d'offrir aux intervenants travaillant en première ligne (groupes de médecine de famille, médecins en cabinets et pharmaciens, entre autres) des services d'accès et d'échange au regard des informations requises pour assurer le continuum des soins et services ;
- de réduire les coûts liés au développement, au déploiement et à l'entretien des systèmes ainsi que les coûts de gestion des infrastructures et d'exploitation.

Énoncé 3 : S'assurer de mettre en place l'ensemble des mécanismes nécessaires à la sécurité et à la protection des renseignements personnels.

Conséquemment à ce troisième énoncé de direction, les solutions technologiques doivent faire en sorte :

- de soutenir la gestion appropriée du consentement de l'utilisateur à l'utilisation des informations personnelles qui le concernent ;
- d'appuyer la gestion de la sécurité sur des mécanismes communs, notamment en matière d'identification, d'authentification, d'habilitation, de signature, de chiffrement et de journalisation ;

17. Aussi connus sous l'appellation anglaise de *Legacy systems*.

- de doter le réseau des outils appropriés pour la gestion des infrastructures dans le but d'assurer la continuité des activités, de coordonner efficacement la sécurité, de garantir des niveaux suffisamment performants de services et de réduire les coûts d'exploitation.

Énoncé 4 : Favoriser l'emploi, par les utilisateurs, des outils (ou mécanismes d'assistance) les plus adéquats afin de leur faciliter l'accès aux informations.

Conséquemment à ce quatrième énoncé de direction, les solutions technologiques doivent faire en sorte :

- de poursuivre la mise en place de services électroniques communs, en particulier ceux du type Web ;
- d'outiller les utilisateurs de façon à leur permettre l'accès à l'ensemble des services par un portail intranet d'entreprise ;
- de soutenir différents mécanismes d'accès à l'information (poste de travail fixe et portable, assistant personnel – PDA – et téléphone cellulaire, entre autres) ;
- de permettre l'utilisation des nouvelles technologies sans fil et de reconnaissance vocale¹⁸.

Énoncé 5 : Privilégier l'utilisation de technologies évoluées, soutenues par des fournisseurs reconnus, et compatibles avec les principales normes de l'industrie des technologies de l'information.

Conséquemment à ce cinquième énoncé de direction, les solutions technologiques doivent :

- permettre de tenir compte de l'évolution technologique mondiale, en particulier en ce qui a trait aux technologies du type Internet et aux nouveaux standards de l'industrie des technologies de l'information ;
- faire en sorte que les technologies supportent des normes récentes et reconnues ;
- privilégier de façon générale l'utilisation des standards les plus ouverts pour les communications et les échanges électroniques.

Énoncé 6 : Voir au respect et à l'évolution du cadre de référence technologique, notamment en ce qui a trait à l'utilisation de services électroniques communs par les applications.

18. Ces technologies ne sont toutefois pas traitées dans la présente version des orientations technologiques.

Conséquemment à ce sixième énoncé de direction, les solutions technologiques doivent faire en sorte :

- de soutenir la conception, la réalisation et le déploiement de systèmes d'information utilisant des services électroniques communs, de manière à réduire les coûts afférents aux technologies et à la gestion des systèmes ;
- de faciliter le recours aux services électroniques communs ainsi qu'à des conventions définies portant sur les contenus et les échanges d'informations ;
- de favoriser le partage d'infrastructures permettant de bénéficier d'économies d'échelle et de réduire les coûts de gestion ;
- de prévoir un arrimage aux processus de gestion nécessaires à l'application du cadre de référence technologique.

2.2.3 Perspectives conceptuelles

Les perspectives conceptuelles présentent les concepts et les modèles retenus pour la mise en place d'infrastructures technologiques et de services électroniques communs, alignés sur les principes directeurs et les énoncés de direction des orientations technologiques. Ces concepts et ces modèles visent :

- à permettre d'instaurer une approche de gestion des technologies qui soit souple et adaptée le mieux possible aux besoins d'une entreprise réseau étendue, c'est-à-dire un ensemble d'organisations relativement autonomes devant agir en coopération pour réaliser leur mission ;
- à intégrer les technologies qui correspondent aux tendances les plus fortes de l'industrie selon les firmes spécialisées du domaine¹⁹ et aux choix retenus pour le réseau selon un ensemble représentatif de gestionnaires, d'utilisateurs et d'informaticiens du réseau²⁰.

Les perspectives conceptuelles sont exprimées sous forme de vues qui illustrent le devenir prévu et souhaité des composantes technologiques d'accès, de sécurisation, d'échange, de partage et de gestion des systèmes d'information. Ces vues sont abordées sous deux angles :

- celui des services électroniques communs ;
- celui des infrastructures technologiques.

Sous chaque angle, sont présentés un modèle d'ensemble et des modèles décrivant un niveau de détail additionnel.

19. En particulier GartnerGroup, comme le démontre la bibliographie.

20. Cet ensemble renvoie aux participants à la consultation menée auprès de nombreux représentants du réseau en avril 2001.

Vues des services électroniques communs

Les services électroniques, tels qu'ils ont été définis dans la section 1.4 portant sur le modèle de gestion des ressources informationnelles, constituent une couche architecturale qui se situe entre la couche des applications et données et la couche des infrastructures technologiques. Certains de ces services s'adressent directement aux utilisateurs, comme le courrier électronique. D'autres services sont invisibles aux utilisateurs, car ils sont utilisés par les applications elles-mêmes, par exemple pour obtenir ou transmettre des données. Ces derniers services sont souvent assurés par des programmes informatiques appelés intergiciels (mieux connus sous l'appellation anglaise *middleware*).

Des services électroniques sont utilisés par toutes les applications. Dans le but d'harmoniser les échanges d'information et la gestion des technologies, les présentes orientations préconisent la mise en place et l'utilisation commune de certains d'entre eux. C'est ce qu'on entend par l'expression *services électroniques communs* (ou, en abrégé, *services communs*).

Cette orientation est cruciale. En effet, elle permet d'ouvrir les systèmes aux échanges et au partage sécurisés de l'information. D'un point de vue technologique, un système ouvert est celui qui utilise les standards de l'industrie. Dans le contexte du réseau, un système ouvert sera celui qui utilise les *services communs* en plus d'utiliser les standards de l'industrie. Un système ouvert du réseau permettra de communiquer avec plusieurs autres systèmes sans qu'il soit nécessaire de le modifier.

Un système ouvert ne vise pas à ce que toutes les communications utilisent le même protocole d'échange, mais plutôt à ce que chaque système ayant un potentiel d'échange d'information dispose des ouvertures nécessaires pour lui permettre d'échanger avec les autres systèmes. Cette orientation ne remet donc pas en cause les architectures actuelles des systèmes et elle n'impose pas non plus une architecture interne particulière pour les nouveaux systèmes. Elle préconise avant tout l'ajout des fonctions nécessaires aux systèmes visés pour permettre des échanges selon les protocoles normalisés par les *services communs*.

Cette approche s'inspire d'Internet et de son modèle de gestion très décentralisé. Celui-ci fonctionne sur la base d'une organisation, l'Internet Society, qui édicte des normes (HTML, HTTP, POP, MIME et TCP/IP) et certaines règles minimales (par exemple, pour la gestion des noms de domaine). Ces normes et ces règles permettent à la communauté mondiale de concevoir et d'utiliser toutes les applications utiles à la communication et à la coopération, et ce, dans un univers technologique tout à fait hétérogène.

Poussée plus avant, cette analogie avec Internet amène à constater que la stratégie de mise en œuvre sous-jacente aux orientations technologiques du réseau devra consister, entre autres, à prescrire des conventions et des protocoles normalisés

pour les échanges d'information, car c'est sur cette base que les systèmes pourront se transmettre l'information partageable.

L'évolution dans ce sens nécessite un certain niveau d'encadrement et de normalisation par une structure de gestion concertée :

- des orientations doivent être adoptées et respectées quant à la nature des *services communs* du réseau ;
- des architectures propres à ces mêmes *services communs* doivent être définies, notamment en ce qui a trait aux protocoles d'application et aux conventions d'échange d'informations.

Les vues des *services communs* qui sont exposées ici constituent des orientations initiales quant à la nature des *services communs* du réseau. Des travaux ultérieurs, indispensables à la poursuite de cette approche, sont inclus dans la planification de mise en œuvre présentée au quatrième chapitre du présent document.

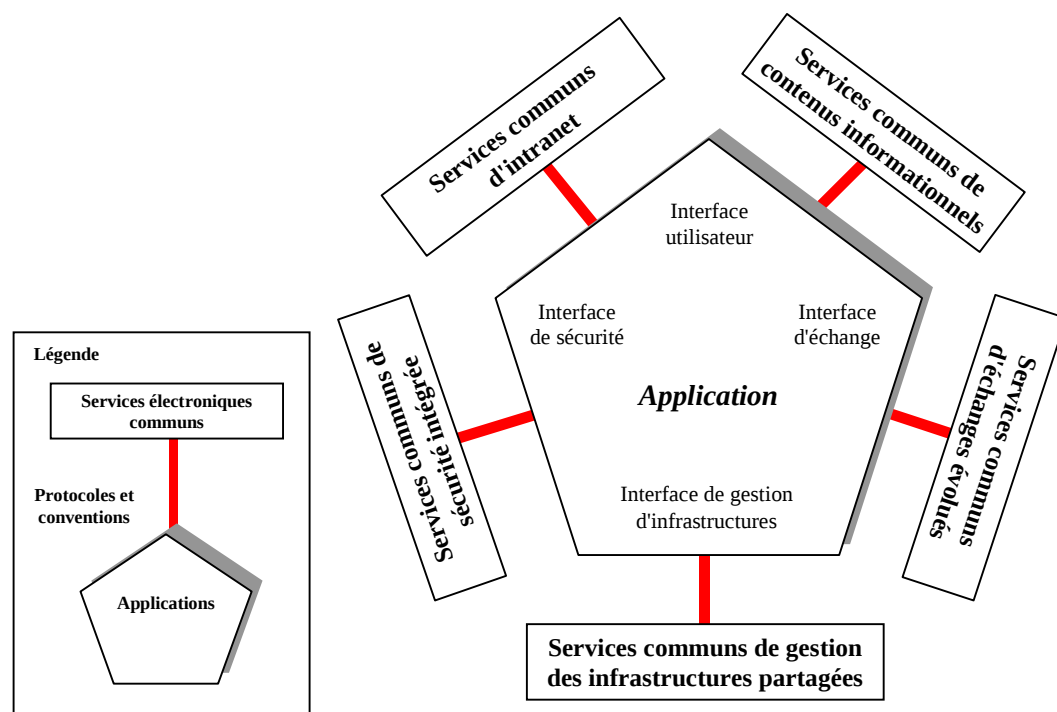
Vue d'ensemble des services communs

Le diagramme 5 illustre l'ensemble des *services communs*. Il représente le concept d'une application qui a sa propre architecture interne (les éléments apparaissant à l'intérieur du pentagone) et qui est reliée au monde externe (les autres applications), par l'intermédiaire d'interfaces, à des *services communs*. Les différentes catégories (ou classes) de *services communs* sont :

- les *services communs* d'intranet ;
- les *services communs* de sécurité intégrée ;
- les *services communs* de gestion des infrastructures partagées ;
- les *services communs* d'échanges évolués ;
- les *services communs* de contenus informationnels.

Comme l'illustre le diagramme, l'application utilise les *services communs* par l'intermédiaire de conventions et de protocoles (représentés par les lignes reliant le pentagone de l'application aux rectangles des classes de *services communs*).

Diagramme 5 : Vue d'ensemble des services communs



Services communs d'intranet

Ces services offrent une interface d'accès du type Web permettant d'utiliser un navigateur pour accéder à des fonctions d'échange et de partage d'informations (courrier électronique, agenda, nouvelles, groupes de discussion, entre autres) ainsi qu'aux applications. Les *services communs* d'intranet comprennent le *portail intranet d'entreprise* et un ensemble de *services de base de l'intranet*²¹.

Le *portail intranet d'entreprise* fournit un cadre paramétrable de présentation pour les services électroniques directement accessibles à l'utilisateur et pour les applications. Il utilise une interface à multiples fenêtres dynamiques²². Cette interface permet à l'utilisateur de demander une mise en contexte pour voir sur son écran des affichages synchronisés de plusieurs applications. Comme le portail est paramétrable, il est possible d'en faire des instanciations²³ distinctes et personnalisées.

21. Comme les services au public ne sont pas couverts par les présentes orientations, il n'y a pas, pour l'instant, de composante portail public. C'est pourquoi seuls les services intranet sont abordés dans la présente section.

22. Il ne s'agit pas de « cadre » HTML mais plutôt de plusieurs fenêtres d'application actives simultanément.

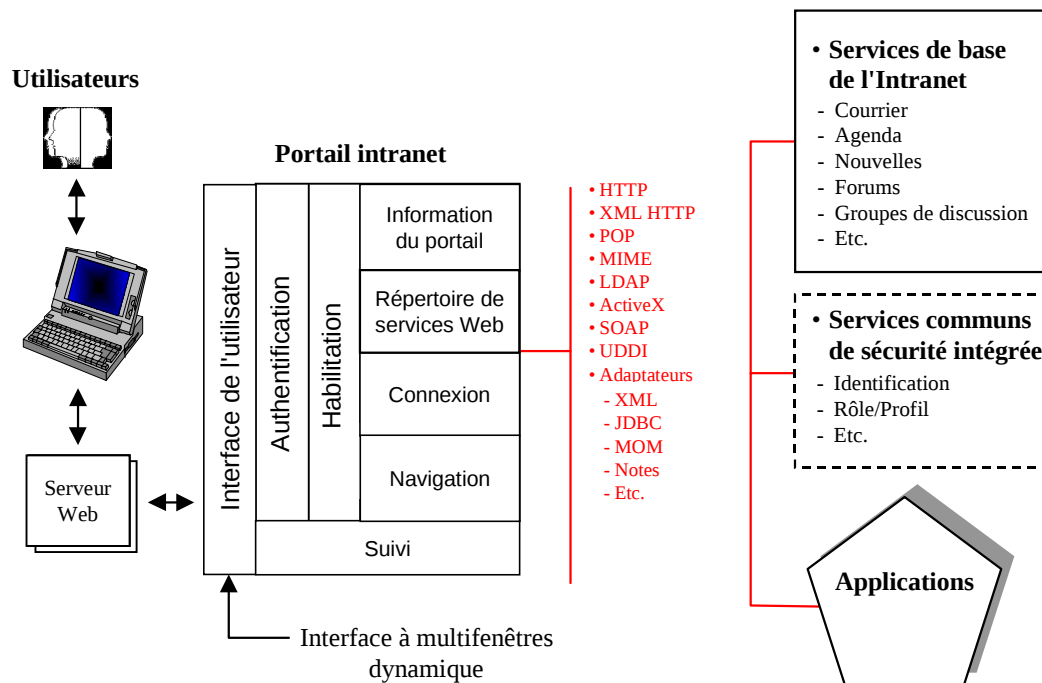
23. L'instanciation est une copie exécutable dans un environnement distinct, qui reproduit les caractéristiques de l'original mais qui peut également posséder ses caractéristiques propres, comme certains aspects visuels (format de présentation, logo, etc.).

L'étiquette « entreprise » associée au portail intranet signifie qu'il donne accès, moyennant les autorisations requises, à l'ensemble des services offerts par le RTSS.

Les *services de base de l'intranet*, quant à eux, sont des services électroniques directement accessibles par l'utilisateur à l'aide d'un fureteur ou pouvant interagir avec des applications au moyen d'interfaces standard. Ces services sont propres aux utilisateurs du réseau (et à leurs partenaires lorsqu'ils y sont autorisés). Le courrier électronique et l'agenda sont des exemples de ce type de services.

Le portail intranet d'entreprise et les services de base de l'intranet sont illustrés par le diagramme 6.

Diagramme 6 : Vue des services communs d'intranet



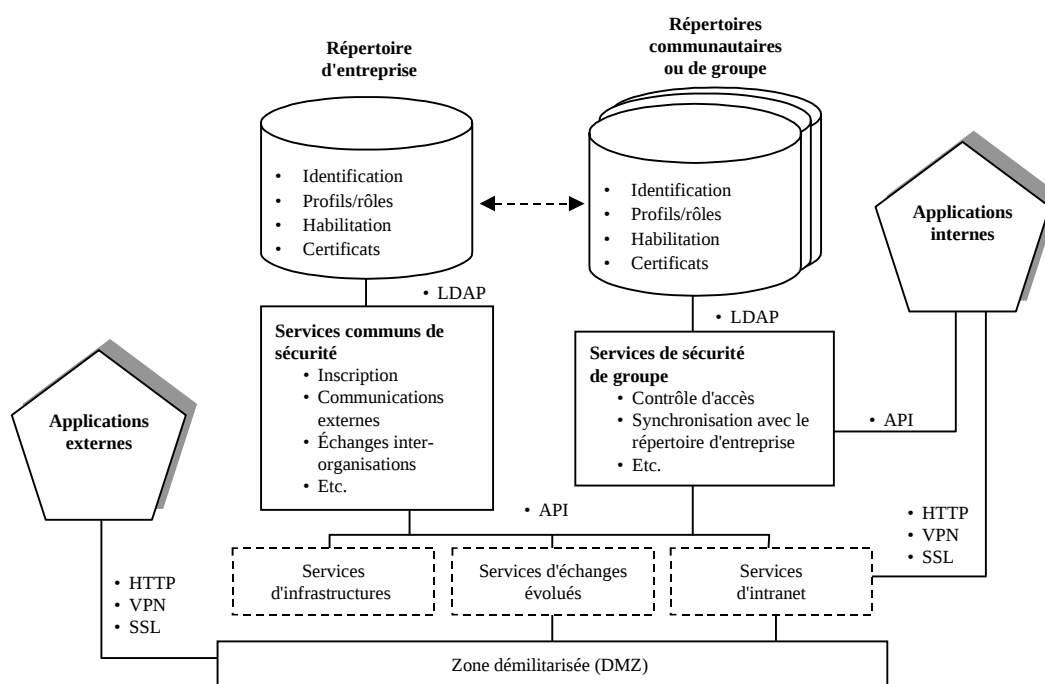
L'utilisateur accède au portail à l'aide d'un poste de travail (ou d'un autre mécanisme d'accès). Ce portail comprend plusieurs composantes, dont l'interface visuelle de l'utilisateur, l'authentification, l'habilitation (vérification des privilèges d'accès), les informations propres du portail (fonctions d'aide, par exemple), le répertoire des services Web, la navigation, le suivi (activités de la session de travail) et la connexion à d'autres services ou applications. Cette dernière composante supporte des protocoles standard majeurs (HTTP, POP, SOAP et XML, entre autres) soit directement, soit au moyen d'adaptateurs. Elle permet l'utilisation des services de base de l'intranet.

Le diagramme 6 montre également que les services de sécurité intégrés sont intimement liés au portail. Au début d'une session de travail, le portail communique avec les services de sécurité pour authentifier l'utilisateur, lui associer un rôle et lui donner les droits d'accès qui vont avec ce rôle et son identité.

Services communs de sécurité intégrée

Les services communs de sécurité intégrée comprennent un ensemble d'outils de gestion de la sécurité et un ensemble de services électroniques capables d'interagir avec les applications pour, par exemple, identifier et authentifier un utilisateur ou une application, vérifier un privilège d'accès et obtenir une clé de cryptage. Le diagramme 7 montre une vue des composantes des *services communs* de sécurité intégrée²⁴.

Diagramme 7 : Vue des services communs de sécurité intégrée



La structure de répertoire est la base des services de sécurité. Deux niveaux de répertoires sont représentés :

24. Certaines composantes n'apparaissent pas dans le diagramme, notamment les outils de gestion utilisés par les responsables de la sécurité et les dépôts associés à la journalisation. Les outils de gestion sont plutôt présentés dans la vue des *services communs* de gestion des infrastructures partagées.

- le répertoire d'entreprise, qui est un dépôt de données où sont notamment consignées des informations de sécurité concernant l'ensemble des utilisateurs pouvant accéder au RTSS ;
- les répertoires de groupe, qui sont des dépôts de données où sont notamment consignées des informations de sécurité concernant des utilisateurs regroupés sous une même autorité de sécurité selon le cadre de gestion de la sécurité.

Certaines informations sont reproduites automatiquement par ces répertoires de façon à simplifier l'administration de la sécurité, aussi bien pour les responsables du RTSS que pour les responsables de groupes.

À chaque répertoire sont associés des *services communs* de sécurité pouvant être utilisés par l'intermédiaire d'API²⁵. Ces services utilisent le protocole standard LDAP pour accéder aux répertoires.

Le diagramme montre également que les services de sécurité sont accessibles à partir de services d'infrastructures (par exemple, le système d'exploitation d'un serveur), de services d'échanges évolués (par exemple, un système de messagerie entre applications) et de services d'intranet (par exemple, le portail intranet d'entreprise et les autres services de base décrits dans la vue des services intranet).

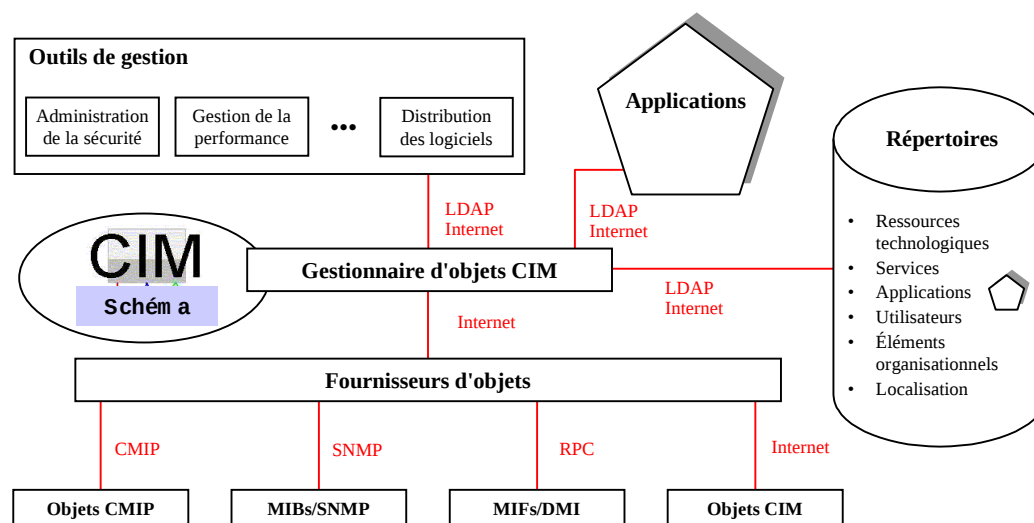
En ce qui a trait aux applications, elles utilisent les *services communs* de sécurité à l'aide d'API lorsqu'elles sont internes et peuvent aussi utiliser des protocoles standard en passant par la DMZ. Par contre, les applications externes au RTSS doivent nécessairement passer par la DMZ en utilisant des protocoles standard pour bénéficier des services de sécurité.

Services communs de gestion des infrastructures partagées

Ces services comprennent un ensemble d'outils de gestion des infrastructures et un ensemble de services électroniques généralement intégrés aux infrastructures afin d'alimenter les outils de gestion. De nombreux outils peuvent être utilisés tels que ceux qui servent à l'inventaire des équipements et des logiciels, ceux qui servent à donner l'alerte en cas de mal fonctionnement d'un serveur ou d'une pièce d'équipement du réseau, ceux qui servent à l'administration de la sécurité, ceux qui servent à la mesure de la performance et ceux qui sont utilisés pour la distribution de versions de logiciels. Le diagramme 8 montre une vue des composantes des *services communs* de gestion des infrastructures partagées.

25. Le sigle API signifie *Application Programming Interface*. Il s'agit d'une façon d'appeler les services par programmation informatique.

Diagramme 8 :
Vue des services communs de gestion des infrastructures partagées



Le diagramme précédent est inspiré des travaux réalisés par le DMTF²⁶ (Distributed Management Task Force) qui regroupe les principaux fournisseurs de logiciels et d'équipements²⁷. Ce diagramme représente une orientation commune des fournisseurs et non un état de fait. Il n'y a donc pas présentement sur le marché d'outils intégrés de gestion couvrant l'ensemble des concepts apparaissant dans le diagramme. Toutefois, les outils risquent fort d'être de plus en plus conformes à ce modèle.

Les données de base sont stockées dans un ou plusieurs répertoires²⁸. Chacun contient les données d'inventaire des équipements et des logiciels, l'identification des services, des applications et des utilisateurs, des données du type organisationnel (servant par exemple à implanter une gestion par rôle) et des données de localisation des ressources. Le répertoire sert à gérer les infrastructures et également à gérer la sécurité. Il est accessible grâce au protocole LDAP.

Le standard CIM (Common Information Model) constitue le langage commun permettant une intégration dynamique des informations de gestion des infrastructures. Il est défini en XML.

Les outils de gestion et autres applications utilisent des objets CIM pour obtenir les données du répertoire. Ces objets standard permettent d'obtenir toutes les données du répertoire par l'entremise du protocole LDAP (et un protocole

26. Voir le site Internet du DMTF pour plus de détails sur ces travaux.

27. Comme Microsoft, IBM, HP, Compaq, Cisco et plusieurs autres. Notons cependant qu'Oracle n'en fait pas partie.

28. D'entreprise, communautaires ou de groupe.

d'Internet comme TCP/IP), quel que soit le service électronique qui les y a stockées et quel que soit son protocole de gestion (CMIP, SNMP, RPC, objet CIM).

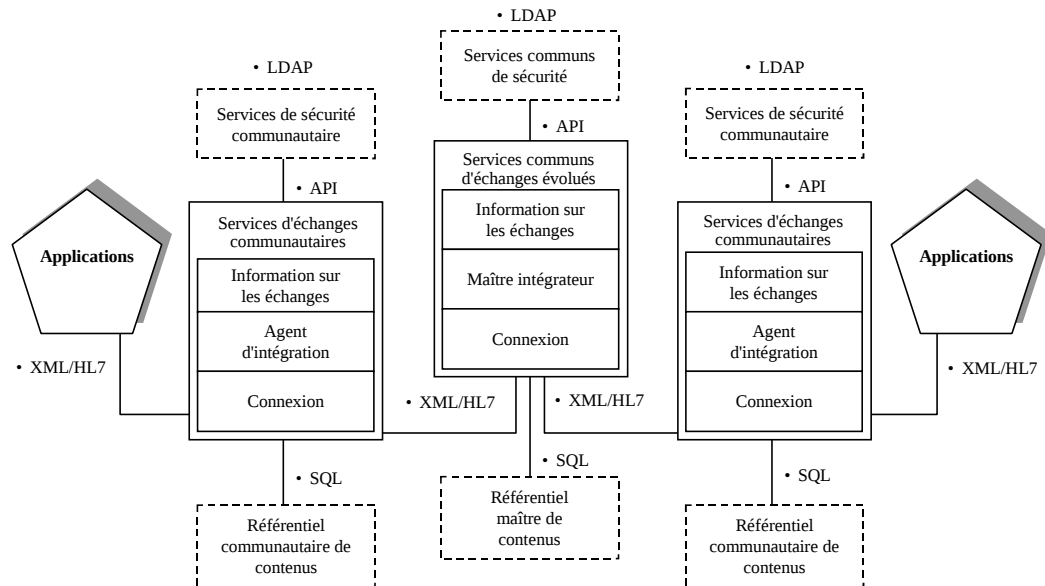
Les outils de gestion des infrastructures fonctionneront de plus en plus en mode Web et en utilisant le CIM. Le DMTF appelle DEN (Directory Enabled Architecture) l'ensemble de cette approche qui se concrétisera au cours des prochaines années. Ce mouvement est déjà amorcé chez plusieurs fournisseurs.

En ce qui a trait aux services électroniques intégrés aux équipements et aux logiciels, ils doivent supporter le protocole de gestion SNMP ou encore des objets CIM, le premier étant le protocole le plus largement utilisé et le second étant en devenir. Un alignement sur ces standards permet d'évoluer dans la direction appropriée compte tenu de l'avenir prévisible des outils de gestion d'infrastructures et du réseau de télécommunications.

Il est également d'intérêt de mentionner que le DMTF a opté pour les normes ITIL en ce qui a trait aux processus de gestion des infrastructures. Les outils seront donc conçus de plus en plus pour soutenir ce modèle de gestion. Aussi, le réseau socio sanitaire devrait-il tendre à aligner ses processus de gestion sur ce standard.

Services communs d'échanges évolués

Dans la présente version des orientations technologiques, seule la messagerie d'application est retenue dans les *services communs* d'échanges évolués. La messagerie d'application s'appuie généralement sur des intergiciels appelés MOM (ou Message Oriented Middleware). Les intergiciels de messagerie d'application comprennent des outils d'administration et des services électroniques de messagerie entre applications utilisables par des API. Le diagramme 9 montre une vue des composantes des *services communs* d'échanges évolués.

Diagramme 9 : Vue des services communs d'échanges évolués

Le diagramme met en présence deux applications qui communiquent entre elles par l'intermédiaire de services d'échanges communautaires et de messages normalisés XML ou HL7. Ces services comprennent:

- un agent d'intégration, qui gère les échanges de messages ;
- des informations sur les échanges, qui sont principalement des files de messages ;
- une composante de connexion permettant de communiquer avec les services communs d'échanges évolués.

Ces composantes soutiennent les échanges à l'intérieur d'une même communauté. Elles sont sous la responsabilité d'une organisation qui peut choisir son propre intergiciel de messagerie en autant que celui-ci puisse communiquer avec les *services communs* d'échanges évolués.

L'agent d'intégration joue plusieurs rôles. Il est une plaque tournante pour les échanges à l'intérieur de la communauté. Il utilise les services communs de sécurité pour gérer la sécurité des échanges entre les applications et, à l'aide d'un référentiel communautaire de contenus, il peut effectuer les conversions nécessaires entre les applications de la communauté.

Pour les échanges entre deux communautés, ou avec une application de groupe, l'agent d'intégration communique avec les *services communs* d'échanges évolués. Ceux-ci comprennent :

- un maître intégrateur, qui gère les échanges de messages entre les agents d'intégration ;
- des informations sur les messages en transit entre les agents d'intégration ;
- une composante de connexion capable de communiquer avec l'ensemble des agents d'intégration.

Le maître intégrateur joue lui aussi plusieurs rôles. Il sert de passerelle entre les différentes technologies de messagerie sur lesquelles sont implantés les agents d'intégration. Il utilise les services communs de sécurité pour gérer la sécurité des échanges entre les applications de différentes communautés et, à l'aide d'un référentiel maître de contenus, il peut aussi effectuer les conversions nécessaires entre ces mêmes applications. Cela permet une communication entre des applications qui utilisent chacune sa propre version de données de référence.

Un message XML ou HL7 émis par une application est reçu par l'agent d'intégration des services d'échanges communautaires. Si le message s'adresse à une entité en dehors de sa communauté, il le transmet au maître intégrateur pour acheminement. Ce dernier relaie le message aux services d'échanges communautaires du destinataire en réalisant les conversions nécessaires (entre intergiels de messagerie et entre données de référence). Enfin, les services d'échanges communautaires du destinataire livrent le message à l'application réceptrice.

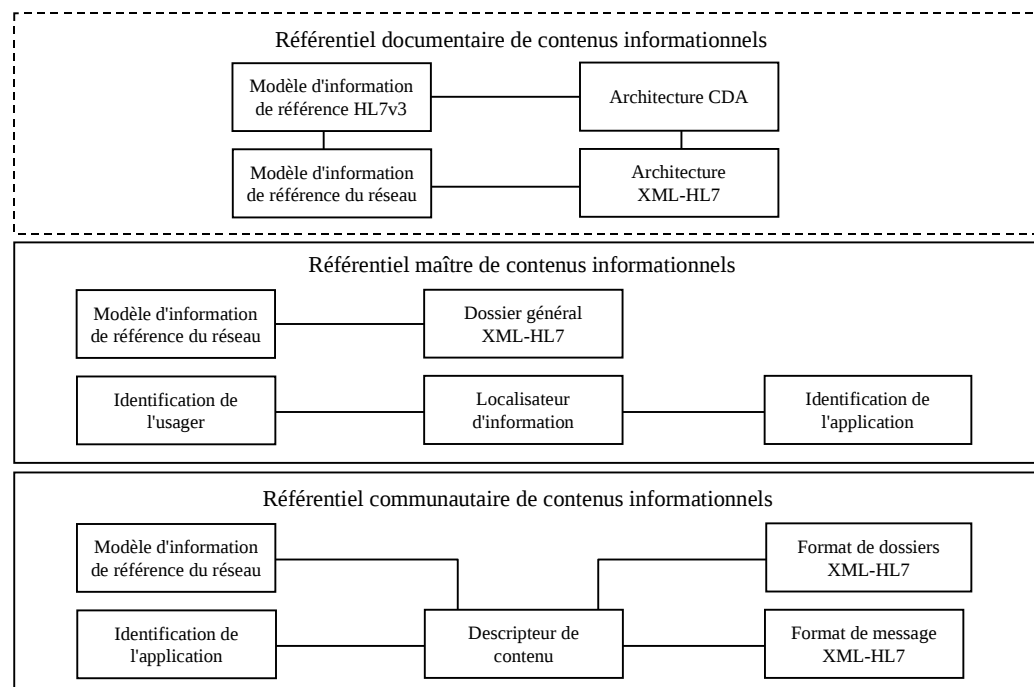
Il est à remarquer que les services d'échanges vérifient l'identification des applications qui communiquent. Ils peuvent ainsi s'assurer que la communication entre elles est autorisée. Les services d'échanges peuvent également crypter les communications à l'aide de clés provenant du répertoire d'entreprise. En fait, ils ont accès aux différents services de sécurité offerts par la structure de répertoire décrite dans la vue des *services communs* de sécurité intégrée.

Services communs de contenus informationnels

Dans la présente version des orientations technologiques, les *services communs* de contenus informationnels comportent :

- une structure de référentiel documentaire ;
- une structure de référentiel maître ;
- une structure de référentiel communautaire.

Le diagramme 10 montre une vue de ces composantes.

Diagramme 10 : Vue des services communs de contenus informationnels

La structure de référentiel documentaire est un ensemble de métadonnées informationnelles qui décrit les types de données suivants :

- les standards qui sont utilisés comme base de référence pour la définition des modèles d'information propres au réseau sociosanitaire québécois. Ces standards peuvent comprendre le modèle d'information de référence HL7 et l'architecture CDA ;
- les modèles d'information propres au réseau sociosanitaire québécois et les composantes d'architecture d'information XML et HL7 utilisées dans les échanges évolués.

Ce référentiel contient la documentation de modèles, de structures d'information et de données, et il n'est pas utilisé directement dans les applications, hormis celles qui traitent cette documentation.

La structure de référentiel maître de contenus informationnels comprend deux ensembles de données :

- le modèle d'information de référence du réseau, qui contient notamment les versions des données de référence normalisées distribuées aux applications du réseau et les informations de gestion de distribution. Ce modèle est lié au dossier général XML-HL7, qui représente le gabarit d'un dossier électronique réseau d'utilisateur ;

- la structure de localisation des segments de dossier d'un usager, ce qui comprend l'identification de l'utilisateur, le localisateur d'information (autrement dit l'adresse du segment de dossier) et l'identification de l'application capable de retrouver le segment de dossier. D'autres données peuvent s'ajouter, au besoin.

Le référentiel maître est utilisé d'une part pour la distribution de données de référence et, d'autre part, pour la localisation d'un dossier électronique réseau d'utilisateur. Ces notions sont davantage définies dans les orientations spécifiques (voir les sections 3.1 et 3.3 du chapitre 3).

Quant à la structure de référentiel communautaire, elle comporte :

- un modèle d'information de référence propre à une communauté, qui inclut notamment une version des données de référence telles que le découpage territorial et les classifications (CIM 10 et centre d'activités, par exemple) ;
- des gabarits de dossier XML-HL7 et des gabarits de message XML-HL7 ;
- l'identification des applications utilisées dans la communauté qui sont capables de soutenir des échanges évolués ;
- une description codifiée des éléments de données accessibles pour chaque application.

Le référentiel communautaire est utilisé par un système automatisé qui coordonne les communications entre les applications à l'intérieur d'une communauté ainsi que le trafic provenant et sortant de la communauté. Ce système est implanté sous la forme des *services communs* d'échanges évolués décrits précédemment. D'ailleurs, le diagramme illustrant ces *services communs* d'échanges évolués fait explicitement référence au référentiel maître de contenus et aux référentiels communautaires.

Vues des infrastructures technologiques

Les vues d'infrastructures technologiques sont des représentations plus physiques des composantes technologiques que les vues des *services communs*. Toutefois, la complexité des infrastructures d'une entreprise étendue aussi vaste que celle du réseau socio sanitaire rend incontournable un certain niveau d'abstraction.

Les vues technologiques comportent deux niveaux de détail. Le premier niveau présente une vue d'ensemble des infrastructures technologiques, qui montre les grands ensembles de composantes. Le second niveau permet de distinguer les principales composantes technologiques faisant partie des grands ensembles.

Vue d'ensemble des infrastructures technologiques

La vue d'ensemble permet de situer les principaux regroupements technologiques qui participent aux infrastructures du réseau. Ces regroupements sont :

- les réseaux de télécommunications ;
- les environnements ;
- les entités externes.

Les réseaux de télécommunications sont des regroupements technologiques qui comprennent des infrastructures permettant de connecter les environnements entre eux et avec les entités externes. Les réseaux de télécommunications comprennent :

- le RTSS ;
- Internet ;
- les réseaux gouvernementaux tels que le RICIB et bientôt le RETEM, le RISQ et le réseau de la CSST ;
- des réseaux privés de partenaires.

Un environnement est un ensemble de composantes technologiques qui soutient les systèmes d'un regroupement organisationnel. Un tel regroupement peut comprendre une ou plusieurs organisations et permet de soutenir un réseau intégré de services d'un type donné. Un centre hospitalier universitaire ou le Réseau mère-enfant sont des exemples de regroupements organisationnels qui correspondent chacun à un environnement.

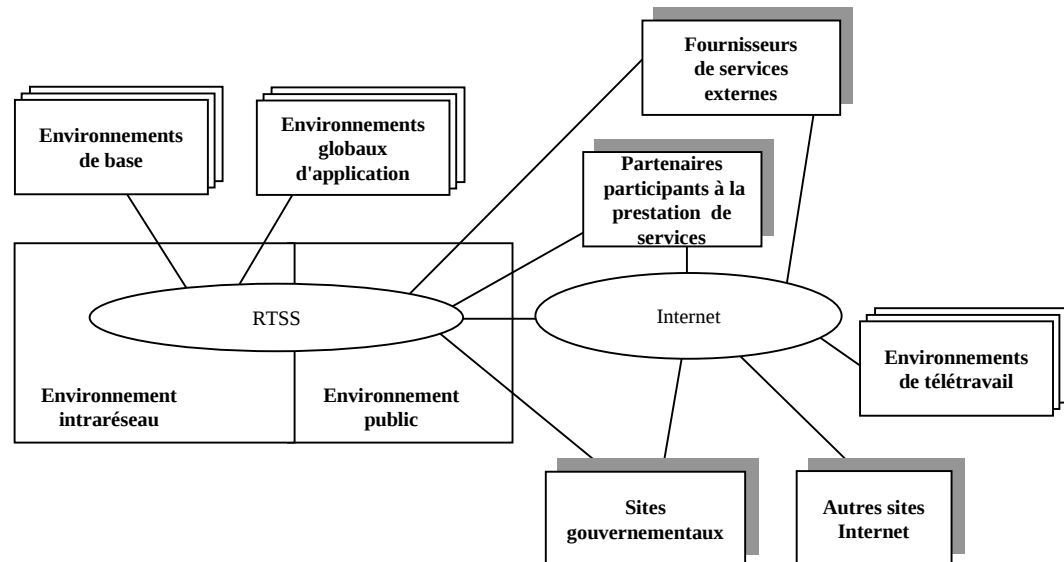
Une entité externe représente un regroupement technologique qui participe au secteur sociosanitaire sans en faire partie. Les entités externes comprennent :

- les infrastructures des partenaires participant à la prestation de services, telles que celles des cliniques privées, des pharmacies, des laboratoires, des écoles et des corps policiers ;
- les infrastructures des sites gouvernementaux, comme celui de la CSST, qui échangent régulièrement des informations avec les organisations du réseau sociosanitaire ;

- les infrastructures des fournisseurs de services externes, tels que les partenaires d'approvisionnement en médicaments et fournitures ainsi que les fournisseurs de services d'applications à distance (par exemple, en mode ASP²⁹) ;
- les infrastructures de sites Internet qui sont accessibles au personnel du réseau.

Le diagramme 11 illustre la vue d'ensemble des principaux réseaux de télécommunications, des environnements et des entités externes. Le diagramme représente les réseaux par des ovales et les environnements par des rectangles. La superposition de plusieurs rectangles signifie qu'il y a plusieurs environnements. Quant aux entités externes, elles sont représentées par des rectangles ombragés.

Diagramme 11 : Vue d'ensemble des infrastructures technologiques



En plus des regroupements d'infrastructures déjà mentionnés, le diagramme illustre différents types d'environnement qui se définissent comme suit.

- Environnements de base :
Infrastructures communautaires comportant des applications de nature clinique et administrative utilisées à l'échelle d'une ou de plusieurs organisations.
- Environnements globaux d'application :

29. Le sigle ASP signifie *Application Service Provider*. Il s'agit d'un mode d'exploitation de systèmes qui consiste à installer un ou des progiciels sur les infrastructures d'un fournisseur (nécessairement hors RTSS) qui vend ces mêmes services à plusieurs organisations afin de rentabiliser ses activités.

Infrastructures de portée multicommunautaire qui comporte des applications de nature clinique ou administrative et qui fonctionnent en liaison avec les environnements de base à l'aide des services de l'environnement intraréseau.

- Environnement intraréseau :

Infrastructures partagées, d'usage généralisé, qui soutiennent l'intégration des applications des environnements de base et globaux.

- Environnement public :

Infrastructures partagées, d'usage généralisé, qui soutiennent des échanges soit par Internet, soit par passerelles à d'autres réseaux.

- Environnement de télétravail :

Infrastructures de soutien aux membres du personnel, qui accèdent aux applications du réseau en dehors de leur lieu habituel de travail, c'est-à-dire à partir de leur propre domicile, du domicile de l'utilisateur ou d'un autre endroit.

Ces concepts étant définis, une vue de second niveau des infrastructures technologiques permet de distinguer les principales composantes de chaque regroupement et d'établir les liens avec les vues des *services électroniques communs*.

Vue de second niveau des infrastructures technologiques

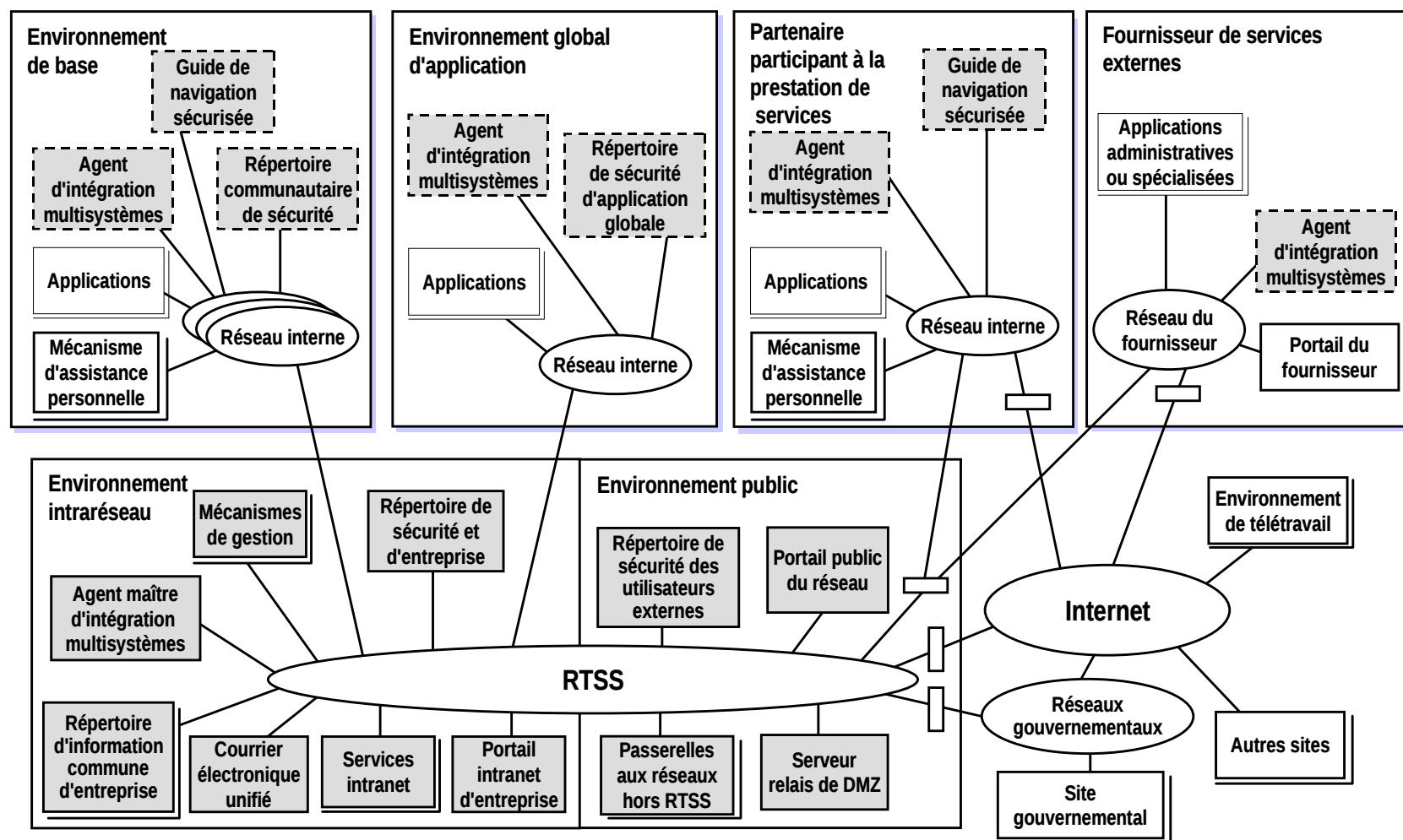
La vue de second niveau montre les regroupements de composantes technologiques pour les principaux environnements en fonction de leur usage. Elle illustre également certains groupes de composantes technologiques des infrastructures des entités externes qui transigent avec le personnel du réseau.

Le diagramme 12 illustre les regroupements technologiques et leurs principales composantes. Le symbolisme de représentation est le suivant :

- un rectangle est une application ou un service électronique. Le rectangle avec un double trait indique l'existence possible de plusieurs applications ou services. Un trait pointillé indique une existence optionnelle alors qu'un trait plein indique que l'environnement comporte généralement au moins une occurrence ;
- un rectangle avec un fond gris correspond à une composante implantant un *service électronique commun* ;

- un ovale représente un réseau de télécommunications. La superposition de plusieurs ovales correspond à plusieurs réseaux de télécommunications ;
- un trait entre deux rectangles représente un lien de télécommunication ;
- un petit rectangle blanc sur un lien de télécommunication représente un mécanisme de sécurisation pouvant comprendre, par exemple, un coupe-feu et un aiguilleur.

Diagramme 12 : Vue de second niveau des infrastructures technologiques



Environnement de base

Les composantes technologiques illustrées dans le diagramme 12 se définissent comme suit.

- Applications :

Ce sont les applications de nature clinique ou administrative qui sont utilisées par les membres de la communauté et qui ont la capacité d'émettre une requête standard ou d'y répondre en communiquant avec l'agent d'intégration.

- Mécanisme d'assistance personnelle :

Cette composante désigne les moyens d'accès aux applications et aux services électroniques, comme, un poste de travail fixe ou portable, un assistant personnel numérique (PDA) ou un appareil sans fil. Ces moyens incluent également les logiciels d'accès, dont un fureteur, une application cliente et un client Notes.

- Guide de navigation sécurisée :

Cette composante des *services communs* est une instanciation personnalisée du portail intranet d'entreprise. Le guide de navigation sécurisé permet :

- un accès sécurisé aux applications et aux services des différents environnements ;
- l'accès à Internet et à d'autres réseaux par l'entremise des passerelles du RTSS ;
- le multifenêtrage dynamique avec gestion de contexte ;
- une personnalisation par rôle, profil et communauté ;
- une gestion de la sécurité sur la base d'un répertoire, effectuée d'une façon qui respecte la politique et les normes de sécurité du réseau ;
- l'utilisation d'une infrastructure partagée de serveurs localisée dans un établissement pour les données personnelles sur les usagers (afin de respecter les contraintes légales).

- Répertoire communautaire de sécurité :

Cette composante des *services communs* est un répertoire de sécurité de groupe qui permet une gestion décentralisée de la sécurité et qui est basée sur la gestion par rôle.

- Agent d'intégration multisystèmes :

Cette composante des *services communs* est une instanciation d'une messagerie entre applications permettant des échanges évolués entre les applications des différents environnements.

- Réseau interne :

Il s'agit d'infrastructures de télécommunication internes des organisations qui sont connectées au RTSS.

Environnement global d'application

Les composantes de l'environnement global d'application sont similaires à celles de l'environnement de base. Cependant, l'application de nature clinique ou administrative est utilisée par les membres de multiples communautés à travers leurs applications locales. Le répertoire de sécurité d'application globale et l'agent d'intégration multisystèmes doivent donc pouvoir fonctionner dans un contexte de multiples communautés.

Environnement intraréseau

L'environnement intraréseau comporte plusieurs composantes technologiques qui lui sont propres et qui se définissent comme suit.

- Répertoire d'information commune d'entreprise :

Cette composante des *services communs* est un répertoire contenant les informations nécessaires à la coordination entre les systèmes. Ce répertoire correspond au concept de référentiel maître défini dans la vue des *services communs* de contenus informationnels.

- Répertoire de sécurité et d'entreprise :

Cette composante des *services communs* est le répertoire d'entreprise pour la gestion du réseau informatique et de la sécurité. Ce répertoire contient les données nécessaires à la gestion de la sécurité pour l'ensemble des utilisateurs situés à l'intérieur du RTSS. Cette composante correspond au concept de répertoire défini dans la vue des *services communs* de sécurité intégrée.

- Agent maître d'intégration multisystèmes :

Cette composante des *services communs* est l'instanciation maîtresse de l'agent d'intégration fournissant des services d'échanges évolués entre les applications des différents environnements du réseau et des infrastructures des partenaires. Elle permet de gérer des transactions d'une recherche basée sur

les localisateurs d'information. Sa messagerie évoluée d'application fournit des services de conversion technologique (MOM-MOM). Elle correspond au concept de maître intégrateur défini dans la vue des *services communs* d'échanges évolués.

- Portail intranet d'entreprise :

Cette composante des *services communs* permet de constituer les guides de navigation sécurisée des environnements de base, qui en sont autant d'instanciations. Elle permet également d'offrir un guide de navigation aux utilisateurs qui n'ont pas d'attache à une communauté. Le portail intranet d'entreprise soutient le concept de portail de la vue des *services communs* d'intranet.

- Services intranet :

Cette composante des *services communs* regroupe des services du type Web accessibles à l'ensemble des utilisateurs du réseau, comme des nouvelles et des forums. Cette composante correspond aux services intranet de base définis dans la vue des *services communs* d'intranet, à l'exception du courrier électronique unifié qui fait l'objet d'une composante technologique particulière.

- Courrier électronique unifié :

Cette composante des *services communs* correspond aux services de courrier électronique accessibles à l'ensemble des utilisateurs du réseau. Cette composante est déjà en place, soit le système de courrier électronique Lotus Notes.

- Mécanismes de gestion :

Cette composante des *services communs* regroupe les outils communs de gestion des infrastructures et de l'exploitation. Cette composante correspond aux outils de gestion tels qu'ils sont définis dans la vue des *services communs* de gestion des infrastructures partagées.

Environnement public

L'environnement public comporte également des composantes qui lui sont propres et qui se définissent comme suit.

- Portail public du réseau :

Cette composante tient compte des services offerts par l'intermédiaire de sites Web ou d'autres moyens électroniques à différentes clientèles, comme les

usagers du réseau, les partenaires, les sites gouvernementaux, les fournisseurs et les internautes en général. Le portail public est également accessible au personnel du réseau.

Bien qu'elle soit définie dans les infrastructures, cette composante n'a pas fait l'objet d'une analyse dans le cadre de la présente version des orientations technologiques. Le portail public sera analysé dans d'autres travaux.

- Répertoire de sécurité des utilisateurs externes :

Cette composante des *services communs* est le répertoire de gestion de la sécurité pour les utilisateurs hors RTSS. Ce répertoire contient les données nécessaires à la gestion de la sécurité pour l'ensemble des utilisateurs situés à l'extérieur du RTSS.

Le répertoire de sécurité des utilisateurs externes ainsi que le répertoire d'entreprise et de sécurité de l'environnement intraréseau correspondent au concept de répertoire d'entreprise défini dans la vue des *services communs* de sécurité intégrée.

- Passerelles aux réseaux hors RTSS :

Cette composante regroupe les passerelles d'interconnexion qui permettent des échanges électroniques sécurisés entre le RTSS et d'autres réseaux de télécommunications.

- Serveur relais de DMZ :

Cette composante de sécurité permet l'accès au RTSS à partir de l'extérieur. Elle ne contient pas de données et elle permet d'éviter les accès directs aux applications du RTSS. Cette composante, déjà en place, est appelée à évoluer, notamment pour s'intégrer à l'utilisation de la structure de répertoires de sécurité.

- Interconnexion du RTSS à d'autres réseaux :

La vue de second niveau des infrastructures technologiques (diagramme 12) montre que le RTSS permet les échanges avec des réseaux externes comme Internet et les réseaux gouvernementaux (RICIB, RETEM, RCEB, etc.). Le RTSS doit également permettre l'interconnexion des infrastructures des partenaires de services et des fournisseurs de services externes.

Toutes les interconnexions entre le RTSS et les infrastructures externes sont sécurisées par des interfaces constituées de passerelles, de coupe-feu et du serveur relais de la DMZ. Ces interfaces sont représentées sommairement

dans le diagramme par des petits rectangles sur les liens de télécommunication. Leur définition et leur formalisme de présentation seront précisées dans la section 3.5 portant sur les orientations spécifiques en matière de sécurité.

Infrastructure d'un partenaire participant à la prestation de services

Ce type d'infrastructure doit comporter des composantes similaires à celles de l'environnement de base. Ces composantes permettent l'utilisation des services de l'intranet sociosanitaire aux intervenants hors RTSS. L'interconnexion au RTSS nécessite cependant une entente contractuelle obligeant le respect des conditions imposées par le réseau. Le mécanisme d'interconnexion avec un partenaire se différencie de l'environnement de base par l'utilisation d'une passerelle pour avoir accès au RTSS et par le respect d'exigences précises en matière de sécurité, en particulier si le partenaire utilise Internet. De plus, il n'y a pas de répertoire communautaire de sécurité chez un partenaire. C'est la structure des répertoires de sécurité du réseau sociosanitaire qui permet de gérer la sécurité d'accès aux applications et aux services internes du RTSS pour tous les utilisateurs externes.

Infrastructure d'un fournisseur de services externes

L'infrastructure d'un fournisseur de services externes peut permettre l'utilisation d'applications de nature administrative ou spécialisée localisées à l'extérieur du RTSS, généralement en mode ASP. Le fournisseur peut avoir son propre portail de services Web.

L'interconnexion à l'infrastructure d'un fournisseur de services externes nécessite une entente contractuelle obligeant le respect des conditions imposées par le réseau bien que l'application du fournisseur ne puisse comporter de données nominatives sur les usagers. Comme pour le partenaire participant à la prestation de services, l'infrastructure du fournisseur de services externes se différencie de l'environnement de base, en ce qui concerne les mécanismes d'interconnexion, par l'utilisation d'une passerelle pour avoir accès au RTSS et par le respect d'exigences précises en matière de sécurité, en particulier si le fournisseur utilise Internet.

Un agent d'intégration multisystèmes doit également être utilisé par le fournisseur de services externes afin que les systèmes qui y sont localisés puissent participer aux échanges évolués. Cela permet notamment l'obtention, par des applications internes au RTSS, de données administratives ou provenant d'applications spécialisées localisées chez un fournisseur de services externes.

2.2.4 Règles d'architecture

Les règles d'architecture précisent les normes techniques retenues pour mettre en oeuvre le modèle technologique de référence du réseau. Elles définissent également les critères qui doivent être considérés au moment de la conception d'une architecture technologique de système.

Le succès de la mise en œuvre des orientations technologiques repose sur le respect des normes techniques. La certification des applications sera donc nécessaire.

Sans constituer des règles architecturales ou des normes techniques, un ensemble des meilleures pratiques pourrait cependant servir de guide aux organisations du réseau. Un guide des meilleures pratiques est de nature à favoriser l'amélioration de la gestion des technologies, par exemple sur les plans :

- du développement des systèmes ;
- de la réutilisation de composantes ;
- du partage d'expertises et de connaissances techniques ;
- du regroupement des acquisitions de technologies.

Des travaux complémentaires permettront éventuellement de constituer un tel guide.

La première version des règles architecturales, soit les normes techniques et les critères de conception d'architecture technologique, est présentée ci-après. Les travaux de mise en œuvre des orientations technologiques permettront de réaliser des versions ultérieures.

Normes techniques

Dans un premier temps, les normes techniques sont définies en fonction des principaux critères nécessaires à la mise en œuvre des perspectives conceptuelles exposées précédemment. Ces normes sont les suivantes.

Accès à l'interface personne-système

Une application doit être accessible sur un ordinateur personnel par un fureteur, à l'aide d'une version récente³⁰. Les versions des logiciels qui sont supportés seront précisées dans la documentation du portail intranet.

30. Les fonctionnalités des applications Web ne sont pas normalisées comme le faisait le guide de l'IPS réalisé après les orientations technologiques de 1996.

Systèmes d'exploitation

Les systèmes d'exploitation doivent supporter :

- le protocole LDAP pour l'accès au répertoire d'identification et de ressources ;
- les protocoles de communication de TCP/IP selon les normes d'Internet, y compris les protocoles d'application de cette architecture – dont SNMP et SMTP.

Sécurité

L'ensemble des mesures de sécurité adoptées par le réseau doit être respecté. Plus précisément :

- le protocole LDAP est retenu pour l'accès à tous les répertoires de sécurité et d'entreprise, alors que les protocoles SSL et IPSEC sont recommandés pour le chiffrement des messages ;
- un même système joue le rôle de répertoire d'entreprise et de sécurité pour les environnements intraréseau et public ;
- les systèmes de répertoire des environnements de base et global, appelés respectivement répertoire communautaire et répertoire de sécurité d'application globale, sont compatibles avec le répertoire d'entreprise et de sécurité ;
- les produits et les versions supportés pour ces répertoires seront précisés dans la documentation du répertoire d'entreprise et de sécurité.

Intergiciel (middleware) de messagerie entre applications

Un intergiciel unique de messagerie sera retenu pour la fonction d'agent maître d'intégration correspondant aux *services communs* d'échanges évolués. Il permettra les échanges avec les principaux intergiciels de même nature offerts sur le marché, de sorte que les organisations du réseau pourront choisir les agents d'intégration des environnements de base et global. À terme, tout système d'information devant échanger des informations avec un autre système devra utiliser un des logiciels de messagerie supportés pour le réseau sociosanitaire.

Les produits et les versions supportés pour les intergiciels de messagerie seront précisés dans la documentation de l'agent maître d'intégration.

Services intranet

Les applications doivent utiliser les infrastructures communes du réseau sociosanitaire, lesquelles offriront les services intranet courants (courrier électronique, moteur de recherche, agenda, forums, groupes de discussion,

nouvelles, etc.) accessibles par des interfaces standard. Pour le courrier électronique et les services y afférents, le choix du logiciel Lotus Notes est maintenu, en mode natif pour la transition et en mode Web, dès que possible.

Pour l'ensemble des services intranet, les produits et les versions supportés pour le réseau socio sanitaire seront précisés dans la documentation du portail Intranet.

Normes d'interface pour le portail intranet

L'utilisation des normes d'internet est généralement favorisée, dont les protocoles HTTP et HTTPS pour le transport d'information ainsi que les protocoles standards tels que POP et MIME.

Les normes UDDI et SOAP sont envisagées pour la constitution d'un répertoire de services Web.

Le portail comportera en outre les adaptateurs requis pour interfacer avec des SGBD et des serveurs sous différentes architectures (comme COM/DCOM, CORBA et JDBC).

D'autres normes seront précisées dans le cadre d'un projet de développement du portail intranet notamment au regard de la gestion des contenus (*contain management*) ainsi que du soutien de la voix et de l'image (par exemple, pour la dictée vocale et la vidéoconférence).

Les protocoles, les interfaces et les versions supportées pour le réseau socio sanitaire seront précisées dans la documentation du portail intranet.

Protocoles d'application

L'expression *protocoles d'application* renvoie aux protocoles utilisés pour structurer et transmettre les contenus informationnels échangés entre les applications.

Chaque application désignée devra comporter une composante permettant de communiquer avec d'autres systèmes en respectant les protocoles d'application normalisés pour le réseau.

Le langage XML est retenu pour la définition des contenus normalisés de données échangeable entre les applications. Plus précisément, l'architecture HL7 sert de modèle de référence. À terme, la version 3 et les versions ultérieures du protocole HL7 seront supportées par les applications désignées ; entre-temps, les versions antérieures peuvent être utilisées.

De même, l'architecture CDA (*Clinical Document Architecture*) définie en XML sera supportée par les applications désignées.

Les spécifications XML et les adaptations à l'architecture HL7 définies pour le réseau sociosanitaire québécois seront documentées.

Critères de conception d'une architecture technologique de système

De façon générale, les composantes des architectures technologiques de système doivent être choisies dans une perspective d'entreprise réseau étendue, en fonction des critères suivants :

- la croissance des capacités selon les volumes et la complexité d'exécution des transactions ;
- l'évolution sur le chapitre de l'ouverture des technologies, ce qui permettra de gérer les systèmes et ces infrastructures de façon souple et de limiter les répercussions des changements technologiques ;
- la stabilité recherchée sur les plans de la sécurité, du recouvrement des données et de la redondance ;
- la vitesse requise en ce qui a trait au temps-réponse et au délai de réalisation des transactions ;
- la dimension du partage entre les plates-formes technologiques et les bases de données ;
- la simplicité dans la gestion des systèmes et des infrastructures.

Ces critères doivent être considérés au moment de concevoir un système d'information.

3 LES ORIENTATIONS SPÉCIFIQUES

Les principes et le modèle technologique de référence présentés dans les orientations technologiques générales décrivent la vue d'ensemble de l'évolution technologique prévue pour le réseau. Dans le présent chapitre, certains sujets sont approfondis davantage. Ces sujets ont été retenus à cause de leur importance pour la réalisation des orientations stratégiques du réseau. Ce sont :

- les services électroniques aux intervenants relativement aux dossiers des usagers ;
- les téléservices ;
- les services électroniques d'information sur les ressources et les services ;
- les services électroniques de gestion des ressources ;
- la sécurité et les passerelles d'échanges électroniques ;
- les télécommunications.

Les sections qui suivent permettent de faire le point sur les principaux éléments se rapportant à chacun de ces sujets. Elles précisent aussi, pour chaque sujet, les principes directeurs et les perspectives conceptuelles complémentaires au modèle technologique de référence. Comme pour les orientations générales, les principes directeurs expriment la vision de l'évolution technologique alors que les perspectives conceptuelles traduisent cette vision dans un vocabulaire technique moins accessible au non-spécialiste.

3.1 Les orientations en matière de services électroniques aux intervenants relativement aux dossiers des usagers

L'évolution du concept de dossier électronique de l'utilisateur a été évoqué à la section 1.2. Les conclusions qui se dégagent des tendances actuelles en cette matière veulent que soient mises en place, au plus bas coût, des infrastructures technologiques capables de soutenir adéquatement les modes de partage de l'information qui peuvent être adoptés. La présente section précise le contexte relatif au traitement électronique des dossiers des usagers et les orientations retenues pour le réseau sociosanitaire québécois.

Avant même d'aborder les éléments du contexte, il importe de définir le concept de dossier électronique de l'utilisateur.

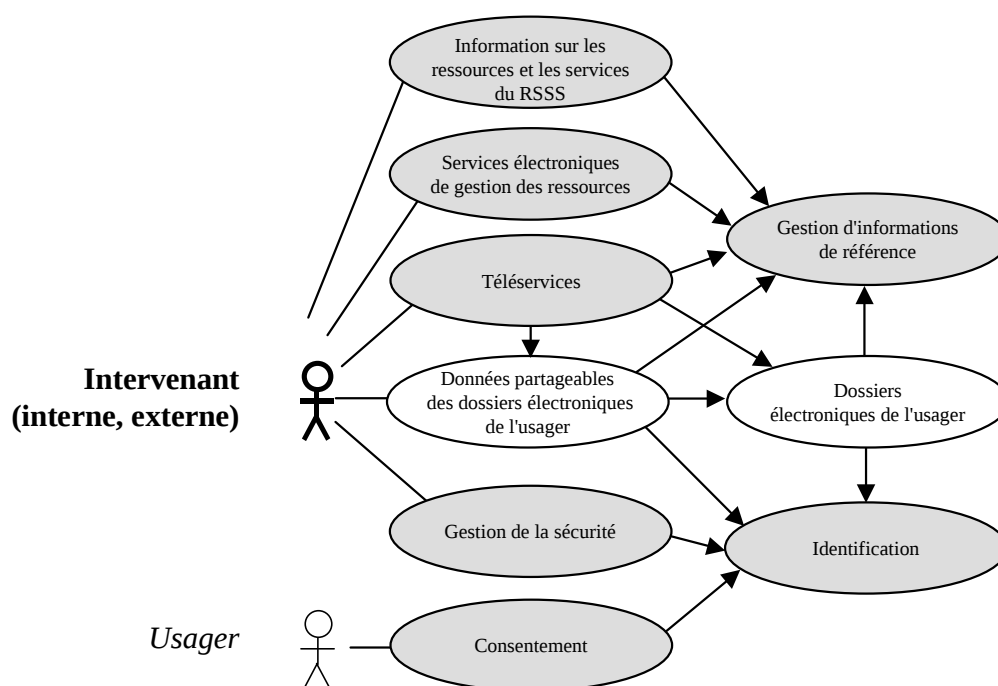
Le *dossier électronique de l'utilisateur* se définit comme un segment d'information sur la santé et le bien-être d'une personne, lequel dossier est accessible à partir d'un système au sein d'un réseau électronique.

Il peut exister plusieurs dossiers électroniques pour un usager, comme il peut exister plusieurs formes de dossiers. Ainsi, chaque établissement auquel l'utilisateur s'est présenté pour obtenir un service peut gérer un ou plusieurs dossiers électroniques le concernant. Ce dossier peut être constitué des informations générales sur la prestation de services reçus, ou il peut être spécialisé comme dans le cas de l'historique transfusionnel de l'utilisateur.

Dans le cadre d'une prestation de services, un intervenant devrait pouvoir obtenir les informations de santé pertinentes d'un usager grâce à un processus permettant de regrouper l'ensemble ou un sous-ensemble des segments d'information sur la santé et le bien-être de cette personne, qui sont disponibles à partir de systèmes distincts et interopérables au sein d'un réseau électronique et ce, avec son consentement.

Le diagramme 13 situe ces concepts dans une vue globale du contexte d'utilisation de différents systèmes d'information par un intervenant.

Diagramme 13 :
Contexte d'utilisation des dossiers électroniques de l'utilisateur



L'illustration suppose que, dans l'exercice de ses fonctions, un intervenant (interne ou externe au réseau sociosanitaire) utilise des informations regroupées des *dossiers électroniques de l'utilisateur*, disséminées dans différents systèmes et banques de données. Le diagramme suppose également que :

- l'intervenant utilise plusieurs systèmes reliés entre eux notamment par des informations de référence, par les dossiers électroniques de l'utilisateur ainsi que par l'identification de l'utilisateur ou de l'intervenant lui-même ;
- l'accès aux systèmes est sécurisé par des mécanismes appropriés de gestion de la sécurité ;
- l'utilisateur consent au partage de l'information de son dossier.

Tout en prenant en considération les relations entre les différents systèmes, les présentes orientations portent particulièrement sur les dossiers électroniques de l'utilisateur et l'accès aux données partageables qu'ils contiennent (représentés par deux ovales à fond blanc dans le diagramme). Les relations avec les autres systèmes (ovales à fond gris) sont couvertes dans les autres sections du présent chapitre³¹.

3.1.1 Éléments de contexte

Évolution du concept sur le plan international

En 1997, aux États-Unis, l'Institute of Medicine (IOM) publie un rapport proposant douze attributs comme points de repère à partir desquels les progrès relatifs aux dossiers de santé électroniques³² (DSE) peuvent être mesurés. Ces attributs, qui ont par ailleurs reçu l'appui du Computer-based Patient Record Institute, sont présentés dans le tableau qui suit.

Tableau 1 : Attributs d'un DSE

1	Le DSE contient une liste qui décrit clairement les problèmes de santé et l'état actuel du patient.
2	Le DSE favorise et soutient tant la mesure systématique que l'enregistrement de l'état de santé et du niveau fonctionnel du patient afin de permettre une évaluation plus précise et routinière des résultats des soins donnés au patient.

31. Les éléments concernant l'identification et la gestion du consentement sont traités dans la section sur la sécurité.

32. Selon le document *Vers les dossiers de santé électroniques*. Op. cit.

3	Le DSE précise la base logique de tous les diagnostics ou de toutes les conclusions, base qui devient un moyen d'appuyer la justification des décisions concernant la gestion des soins au patient.
4	Le DSE peut être relié à d'autres dossiers cliniques sur le patient, qui proviennent de divers lieux et qui couvrent diverses périodes, afin de constituer un dossier longitudinal des événements qui peuvent avoir eu une influence sur sa santé.
5	Le système DSE gère de façon complète la confidentialité des données sur le patient, particulièrement en veillant à ce que le DSE ne soit accessible qu'aux personnes autorisées.
6	Le DSE est accessible à tout moment pour une utilisation rapide par les personnes autorisées et concernées par les soins directs au patient.
7	Le système DSE permet la recherche sélective et le formatage de l'information par les utilisateurs.
8	Le système DSE peut être relié à des bases de données, tant locales qu'éloignées, documentaires et administratives ainsi qu'à des systèmes, de façon à ce que l'information contenue soit immédiatement disponible pour aider les praticiens à prendre leurs décisions.
9	Le DSE peut faciliter et, dans certains cas, orienter le processus de résolution de problèmes cliniques en fournissant aux praticiens des outils d'analyse des décisions, des aide-mémoire, des évaluations du risque des pronostics et d'autres aides.
10	Le DSE supporte la collecte structurée de données et enregistre l'information en utilisant un vocabulaire défini. Il accepte adéquatement l'entrée directe de données par les praticiens.
11	Le DSE peut aider les cliniciens en pratique individuelle et les établissements fournisseurs de soins de santé à gérer et à évaluer tant la qualité que le coût des soins.
12	Le DSE est suffisamment flexible et extensible pour combler non seulement les besoins d'information de base d'aujourd'hui, mais aussi les besoins futurs de chaque spécialité et sous-spécialité clinique.

Dans le même rapport, l'IOM constate qu'aux États-Unis, la mise en place de l'infrastructure technique avance plus rapidement que l'élaboration des politiques nécessaires à son déploiement. Il ressort également que l'obtention des consensus nécessaires avec les prestataires de services sur les questions telles que les protocoles et les définitions est de loin plus problématique que les aspects techniques.

Aussi, malgré de nombreuses initiatives d'envergure concernant les DSE dans plusieurs pays, il semble qu'aucune n'ait encore intégré à ce jour tous les attributs proposés par l'IOM.

Les normes HL7

Différentes études et expérimentations sur les dossiers de santé électroniques mettent en lumière le besoin d'un vocabulaire commun afin de permettre le traitement automatisé des données qui y sont contenues. Des efforts importants ont déjà été consacrés à la normalisation du vocabulaire, comme en font foi les systèmes de classification des maladies tels que CIM 10 et SNOMED ou encore le *Compendium des produits pharmaceutiques*.

Quoiqu'ils soient essentiels, les systèmes de classification et les compendiums sont nettement insuffisants pour permettre une automatisation des dossiers électroniques des usagers. La normalisation doit aller bien au-delà et définir tant les formats que les contenus de « documents électroniques », comme un rapport d'observations cliniques ou une ordonnance. C'est la voie qu'explorent depuis maintenant plus d'une dizaine d'années plusieurs organismes internationaux de normalisation. Parmi ceux-ci, HL7 est celui qui apparaît comme le plus avancé pour le secteur de la santé.

Accrédité par l'ANSI, HL7 est un organisme sans but lucratif à adhésion volontaire dont les membres comprennent des prestataires de services, des vendeurs de logiciels et de services informatiques, des consultants, des assureurs, des organismes gouvernementaux et d'autres adhérents intéressés au développement de standards cliniques et administratifs pour le domaine de la santé. En plus des États-Unis, de nombreux pays participent à l'initiative HL7, dont l'Australie, le Canada, la Chine, la Finlande, l'Allemagne, l'Inde, le Japon, la Corée, les Pays-Bas, la Nouvelle-Zélande, l'Afrique du Sud, la Suisse et le Royaume-Uni.

HL7 a défini plusieurs versions de standards d'échange pour les données cliniques et administratives dans le domaine de la santé. Depuis 1996, il s'affaire à développer de nouveaux standards basés sur XML. En 1999, il a retenu XML comme une solution de remplacement à HL7 V2.3.1, et il prévoit soumettre à l'ANSI l'encodage XML pour la version 2.4.

En septembre 2000, HL7 a également produit la première version d'une architecture XML pour l'échange de documents cliniques (soit le « Clinical Document Architecture »), l'organisme entend soumettre cette norme à l'ANSI pour approbation. HL7 a annoncé que la version 3 de sa norme d'échange de données cliniques et administratives, prévue pour décembre 2001, sera basée uniquement sur XML.

De plus, HL7 participe activement aux travaux concernant XML, qui se réalisent sous l'égide de W3C (organisation internationale responsable du développement de XML), ce qui renforce encore davantage la crédibilité de cette orientation.

Les tendances canadiennes

De nombreuses études sur les dossiers électroniques et sur l'utilisation d'infrastructure à clé publique (ICP) pour la sécurisation des dossiers de santé ont été publiées par Santé Canada. Elles présentent les concepts de dossiers électroniques et d'ICP, et décrivent de nombreux projets que réalisent différents pays sur ces sujets.

Le document de consultation intitulé *National Health Infostructure, Blueprint and Tactical Plan*, daté d'août-septembre 2000, est indicatif de certaines orientations du gouvernement canadien qui se traduisent par :

- la mise en place d'un portail santé pancanadien principalement destiné à diffuser des informations au public ;
- la mise en place d'un portail pour les prestataires de services (médecins, personnel infirmier, pharmaciens). Le concept proposé met l'accent sur l'établissement de liens avec des systèmes d'information régionaux, y compris la télésanté et l'aide à la décision ;
- une initiative portant sur le dossier de santé électronique basé sur dix à quinze projets majeurs, en vue notamment d'établir des standards canadiens relativement à l'échange de données, aux technologies et à la sécurité.

En ce qui concerne l'initiative portant sur le dossier de santé électronique, ce même document de l'infostructure canadienne de la santé prévoit l'adoption d'une approche nationale de protection des renseignements personnels de santé et l'harmonisation des lois provinciales. Il précise aussi qu'un standard national pour le dossier de santé électronique et un standard national sur la sécurité des dossiers de santé, ce qui inclut l'ICP, seront élaborés.

Faits saillants à l'échelle québécoise

Au Québec, plusieurs projets de systèmes visant à soutenir le continuum des soins et services ont été conçus depuis 1998. Certains ont été réalisés, d'autres sont présentement en cours. Chacun de ces projets implique de multiples organisations

et poursuit des objectifs s'appliquant à une situation ou à une population donnée. Ce sont, par exemple :

- le projet de dépistage du cancer du sein (système SI-PQDCS) ;
- le projet réalisé pour le Centre hospitalier ambulatorio de la région de Laval (site SI-PRSA) ;
- le projet de système intégré d'information sur les activités transfusionnelles et d'hémovigilance (système SIIATH) ;
- le projet de transfert de données entre centres hospitaliers et CLSC dans le cadre du programme de maintien à domicile (lien CH-CLSC) ;
- le projet de système d'information en géroto-gériatrie (système SIGG) ;
- le projet du Réseau mère-enfant.

D'autres études et projets ont aussi permis d'approfondir des concepts généraux pour l'intégration des systèmes du réseau socio sanitaire, y compris le concept de dossier électronique de l'utilisateur, dont :

- un rapport de réflexion sur l'architecture cible pour l'index patient provincial (IPP), le dossier patient partageable (DPP) et le système requêtes-résultats génériques (RRG), réalisé par Sogique et présenté en avril 1999 ;
- la proposition d'un projet de portail santé québécois, présentée par Sogique en janvier 2000 ;
- un rapport traitant de la gestion du consentement de l'utilisateur et de la sécurité, réalisé par Sogique dans le cadre du projet IPP-DPP-RRG et présenté en janvier 2000.

Les projets, études et réflexions des dernières années ont fait en sorte que le Ministère a annoncé sa volonté d'évoluer vers la concrétisation des concepts reliés au dossier électronique de l'utilisateur en les inscrivant au plan d'action en matière de ressources informationnelles.

Récemment, soit en avril 2001, le projet relatif à la carte accès santé de la Régie de l'assurance maladie du Québec a reçu l'aval du gouvernement pour la conception d'une carte à microprocesseur qui remplacerait l'actuelle carte d'assurance maladie et la constitution d'un dossier Carte Santé. Un projet de loi devra être déposé pour soutenir la réalisation de ce projet et permettre le débat public sur cette question de dossier électronique.

Tendances technologiques

En dehors des tendances déjà décrites à la section 1.2 et dans les paragraphes qui précèdent, les tendances technologiques les plus pertinentes relativement à la constitution de dossiers de santé électroniques des usagers ont trait :

- aux normes et aux mécanismes qui permettent de soutenir l'intégration des applications dans un contexte de distribution des dépôts d'information ;
- à la sécurité de l'information et à la protection des renseignements personnels (les tendances relatives à la sécurité sont précisées à la section 3.5 ; seules quelques éléments majeurs sont indiqués dans la présente section.

En matière de normes et de mécanismes d'intégration des systèmes, les nouvelles technologies tendent à privilégier une intégration dynamique des services électroniques, des applications et des informations. Ces tendances se manifestent notamment par :

- l'utilisation de technologies Web en mode multi-tiers ;
- l'intégration des services et applications dans un portail d'entreprise soit à l'horizontale (accès aux informations de l'entreprise et aux portails verticaux), soit à la verticale (accès à des applications ou à des fonctions particulières d'affaires) ;
- l'intégration des composantes d'une même application ou l'intégration entre applications par différentes techniques, comme :
 - des architectures orientées vers les services électroniques, telles que CORBAmed, HL7 et ASC X.12N,
 - des spécifications XML définies avec MOM (Message Oriented Middleware), IB (Information Broker) et engin d'interface, avec SOAP comme protocole d'échange entre services et avec COM/DCOM ou CORBA à plus bas niveau,
- l'intégration par gestion des flux (*workflow*) sur la base de protocoles comme WAPI, SWAP et jFlow, dans des produits futurs ou avec un produit homogène tel que Lotus Notes, tant que des standards d'échange ne seront pas couramment supportés.

Aucune de ces techniques ne permet à elle seule de réaliser l'intégration dynamique des services électroniques, des applications et des informations. Il faut donc en combiner plusieurs.

En matière de sécurité, les principales tendances laissent entrevoir que :

- les répertoires supportant le protocole LDAP constituent un élément clé d'infrastructure. Ils permettent de constituer l'infrastructure de base pour les outils d'ouverture de session et les outils d'habilitation. Ils sont nécessaires à une gestion des profils et sont aussi un élément essentiel à l'implantation d'une ICP ;
- les technologies d'ICP sont nouvelles. Elles peuvent offrir différents niveaux de sécurité (de faible à très élevé). Celles dont le niveau de sécurité est élevé ont été utilisées avec succès pour des groupes restreints d'utilisateurs car elles entraînent généralement des coûts importants, aussi bien sur le plan technique que sur le plan administratif.

Selon un article de GartnerGroup³³, les solutions intégrées et évoluées de gestion de la sécurité ne pourront être conçues avant une prochaine génération de produits de type « gestion de réseau et de système ». Les produits devront notamment intégrer un répertoire de ressources avec le répertoire de sécurité.

Principaux constats

La situation et la normalisation sur les plans international, canadien et québécois ainsi que les tendances technologiques permettent d'établir les constats qui suivent.

La mise en place d'un dossier de santé électronique de l'utilisateur correspondant aux critères de l'IOM est une orientation à très long terme vers laquelle, sans doute, tous les pays évolueront progressivement. Tout en avançant dans cette direction, le Québec doit adopter des orientations qui permettent un partage accru de l'information et comportent des avantages concrets à plus court terme.

Compte tenu de la situation au Canada, aux États-Unis, en Australie et dans plusieurs pays européens et asiatiques, le Québec aurait intérêt à mettre en place sa propre organisation vouée à la normalisation du dossier de santé électronique de l'utilisateur. Par ailleurs, les standards de HL7 sont parmi les plus avancés et les plus utilisés au monde, et ils peuvent être retenus comme base de normalisation.

En matière de systèmes d'information, et s'accordant en cela au rapport *Vers les dossiers de santé électroniques*³⁴, de Santé Canada, le DSE devrait comporter les éléments suivants :

33. Dang VAN MIEN, « The Information Security Market Space Invasion Has Begun », Gartner Advisory, Research Note Markets, 17 février 2000.

34. *Op. Cit.*

- **le code d'identification personnel**, soit un code universel qui identifie de façon unique chaque personne faisant partie du système de santé ;
- **le code d'identification de l'établissement**, soit un code universel qui identifie de façon unique chaque établissement ou centre qui fournit des services au sein du système de santé ;
- **le code d'identification du fournisseur**, soit un code universel qui identifie de façon unique chaque fournisseur de soins de santé au sein du système de santé ;
- **de l'information sur la santé**, soit les données sur la santé (par ex. : diagnostics, radiographies, ordonnances) présentées dans un format normalisé. Ces données sont le résultat des interactions entre les personnes et les fournisseurs de soins de santé ;
- **de l'information administrative**, soit les données normalisées qui soutiennent les fonctions administratives telles que la facturation.

Le DSE possède les avantages :

- de soutenir les soins au patient et d'en améliorer la qualité ;
- d'améliorer la productivité des professionnels de la santé et de réduire les frais d'administration associés à la prestation et au financement des soins de santé ;
- de soutenir la recherche clinique et la recherche sur les services de santé ;
- de faciliter les progrès futurs de la technologie, des politiques, de la gestion et des finances en matière de soins de santé ;
- de garantir à tout moment la confidentialité des renseignements personnels sur le patient.

Par ailleurs, l'application du concept de DSE au contexte québécois doit tenir compte du fait que le système couvre à la fois les services de santé et les services sociaux, de sorte qu'il sera nécessaire d'en élargir la portée.

De plus, les conceptions les plus récentes de systèmes d'information de portée commune du réseau québécois de la santé et des services sociaux ont adopté des architectures qui mettent l'accent sur :

- la constitution de dossiers partageables par les prestataires de services (ex. : SI-PRSA, Réseau mère-enfant) ;
- l'échange d'information entre de multiples organisations, par exemple le Système intégré d'information sur les activités transfusionnelles et d'hémovigilance (SIIATH), le lien CH-CLSC, la refonte du Système

d'information du Programme québécois de dépistage du cancer du sein (SI-PQDCS).

3.1.2 ***Principes directeurs concernant les services électroniques aux intervenants relativement aux dossiers des usagers***

Le fait de définir des orientations de fonctionnement pour les dossiers électroniques des usagers et l'accès aux données partageables qu'ils contiennent permet de préciser les orientations technologiques. Plusieurs scénarios possibles de fonctionnement ont déjà été envisagés dans des études et projets antérieurs. D'autres doivent être analysés. La définition des orientations technologiques suppose préalablement que :

- Les données des dossiers électroniques de l'utilisateur qui présentent un intérêt commun pour le partage et l'échange entre les intervenants sont identifiées, disponibles et normalisées ;
- Un identifiant unique de l'utilisateur est utilisé dans tous les systèmes d'information qui gèrent des informations de son dossier ;
- Les règles d'accès qui définissent les modalités de partage des données sur l'utilisateur sont connues et appliquées dans chaque contexte d'utilisation en fonction des besoins des intervenants faisant partie d'une communauté de pratique ;
- Les règles de gestion du consentement de l'utilisateur sont définies et appliquées dans tout contexte d'utilisation où cette gestion est obligatoire ;
- Les règles de sécurité concernant l'accès aux données cliniques de l'utilisateur sont définies et appliquées dans tous les environnements technologiques du réseau.

Sur la base de ces prémisses, les principes directeurs concernant l'accès aux données partageables en provenance des dossiers électroniques des usagers sont les suivants :

- des ***applications spécialisées*** soutiennent les activités de nature clinique ou administrative et interagissent avec leur environnement en utilisant les ***services communs***. Ces applications peuvent gérer ou accéder des segments d'information correspondant aux dossiers électroniques des usagers et ce, en fonction des règles particulières qui sont définies selon le contexte d'utilisation d'un regroupement d'utilisateurs ou d'une communauté de pratique donnée. Ces applications se retrouvent au sein des ***environnements de base ou globaux***, sauf pour les cas d'exception prévus dans les lois et autorisés par le gouvernement ;

- une **banque d'informations partagées** pour chaque environnement de base ou global contient un dépôt unique de données de repérage et de localisation des segments de dossier électronique des usagers à l'aide de l'identifiant unique afin de répondre aux besoins d'accès des différentes communautés de pratique ;
- un **répertoire d'information commune d'entreprise**, combiné avec un agent maître d'intégration multisystèmes (décrit dans les orientations technologiques générales), permet de repérer dynamiquement la localisation des données requises dans un processus d'échange d'un regroupement d'utilisateurs ou d'une communauté de pratique ;
- le **répertoire d'information commune d'entreprise** et les **banques d'information partagées** implantent des **services communs** qui soutiennent les conventions d'échanges d'information et de contenus informationnels retenues pour le réseau sociosanitaire québécois ;
- pour les besoins futurs d'échanges d'information, par exemple avec les partenaires participant à la prestation de services, le **répertoire d'information commune d'entreprise** pourra être utilisé en respectant les règles de sécurité et de protection des renseignements personnels adoptées par les autorités québécoises.

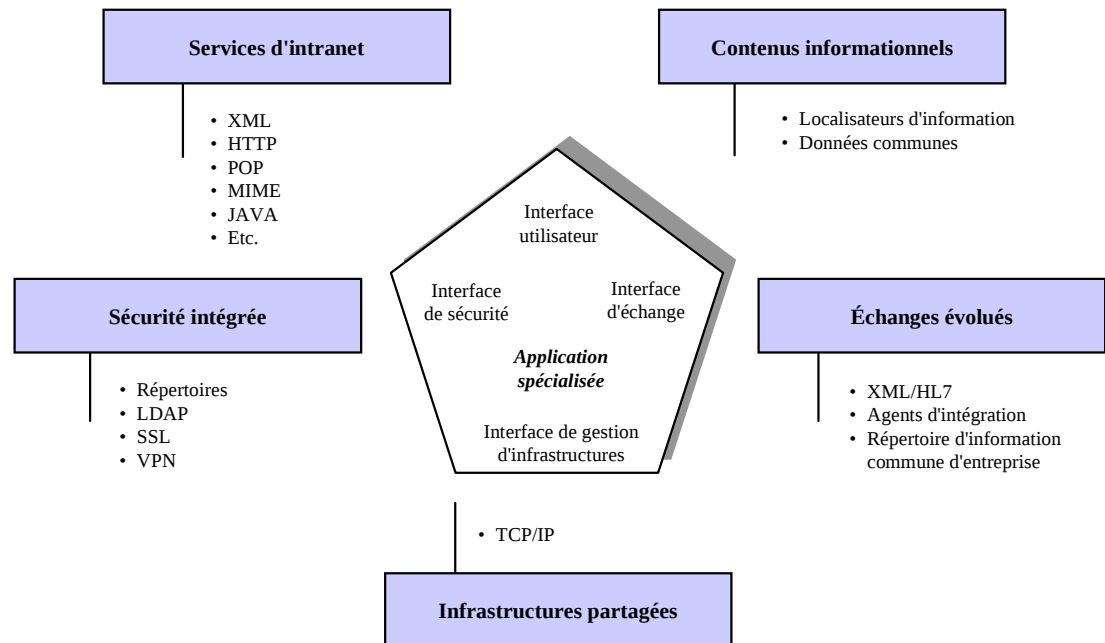
3.1.3 **Perspectives conceptuelles**

En complément aux perspectives conceptuelles du modèle technologique de référence présenté au chapitre 2, les concepts et les modèles apparaissant ci-après sont ceux qui ont été retenus pour les dossiers électroniques des usagers, en vue de la mise en place d'infrastructures technologiques et de services électroniques communs capables de les supporter. Une vue des services électroniques communs et une vue des infrastructures technologiques sont présentées ci-après.

Vue des services communs

Les concepts et les modèles de services communs définis dans le modèle technologique de référence présenté au chapitre 2 permettent entre autres de soutenir la mise en œuvre du système de repérage et de localisation des dossiers électroniques des usagers. Le diagramme 14 rappelle la vue d'ensemble des services communs et indique, pour chaque classe de services, les concepts et les types de standards associés à l'accès aux données partageables des dossiers électroniques des usagers.

Diagramme 14 : Vue des services communs d'accès aux données partageables des dossiers électroniques des usagers



Vue des infrastructures technologiques

La vue des infrastructures technologiques est illustrée par le diagramme 15. Elle est complémentaire à la vue de second niveau des infrastructures technologiques présentée dans le modèle technologique de référence du chapitre 2 et elle utilise le même symbolisme de représentation.

Conformément aux principes directeurs concernant l'accès aux données partageables des dossiers des usagers, la vue des infrastructures montre que les environnements de base et global d'application héritent chacun d'une nouvelle composante : une banque d'informations partagées. La notion d'application est également précisée et prend la désignation d'application spécialisée. Ces composantes technologiques se définissent comme suit.

- Banque d'informations partagées :

Cette composante consiste en un dépôt de données de repérage et de localisation des segments d'information des dossiers électroniques des usagers, géré dans l'environnement de base afin de répondre aux besoins d'un regroupement d'utilisateurs ou d'une communauté de pratique, ou géré dans

un environnement global d'application afin de répondre aux besoins d'un ensemble de regroupements ou de communautés de pratique. Ce type de dépôt est propre au réseau sociosanitaire et est sous la responsabilité d'une organisation autorisée à le gérer.

- Applications spécialisées :

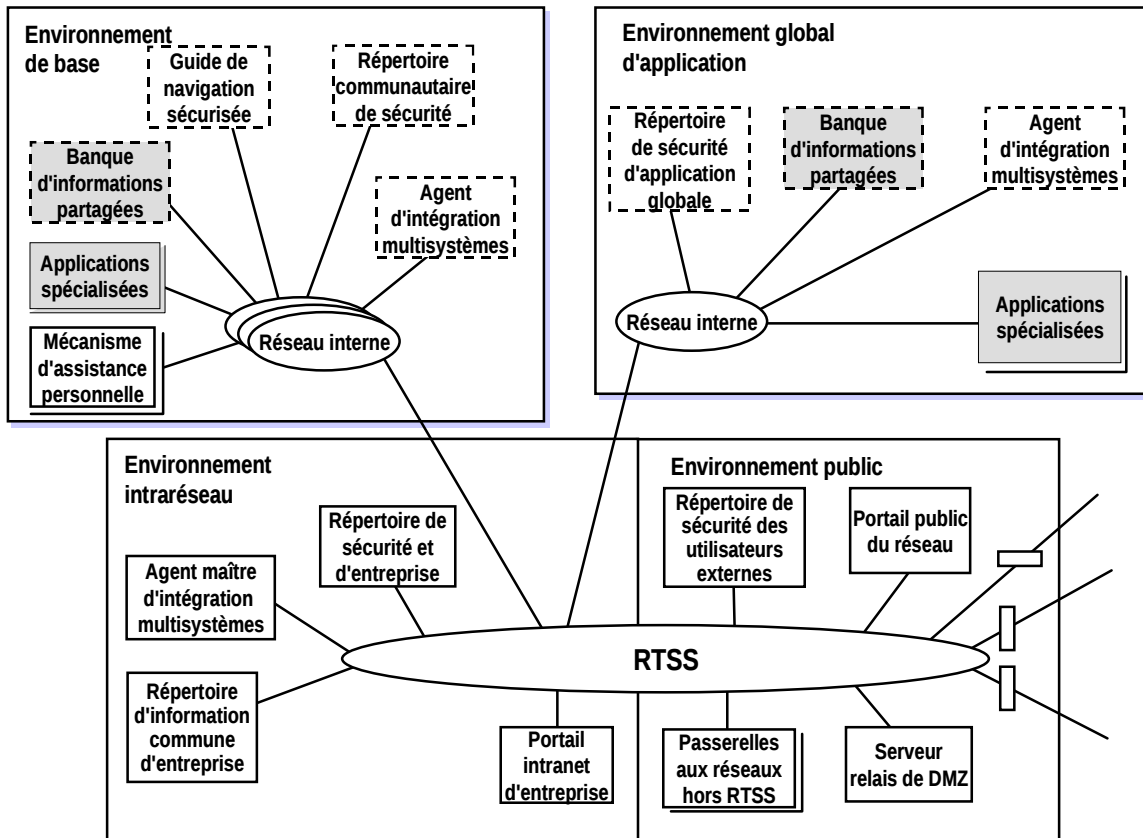
Les applications spécialisées soutiennent des activités de nature clinique ou administrative et elles interagissent avec leur environnement en utilisant les services communs. Ces applications gèrent des dossiers électroniques d'utilisateur et peuvent accéder à des informations en provenance de dossiers électroniques des usagers externes à son environnement.

Les données des applications spécialisées sont stockées physiquement dans un établissement, ou dans un autre lieu selon les cas d'exception prévus dans les lois et autorisés par le gouvernement.

Ces applications se caractérisent par le fait qu'elles sont capables de répondre à une requête standard en provenance de l'agent d'intégration. De plus, elles s'intègrent au portail d'entreprise instancié par le guide de navigation sécurisée.

Les contrôles d'accès aux applications sont gérés à l'aide du répertoire communautaire de sécurité ou du répertoire de sécurité de groupe selon l'environnement où l'application se trouve (soit l'environnement de base ou l'environnement global).

Diagramme 15 : Vue des infrastructures technologiques pour l'accès aux dossiers électroniques des usagers



3.2 Les orientations en matière de téléservices

En juin 2001, le Dr Claude Poirier, responsable de la Table ministérielle en télésanté, définissait le champ d'application de la télésanté comme suit :

« La télésanté désigne les soins et services de santé, les services sociaux, préventifs ou curatifs, rendus à distance par le biais d'une télécommunication, incluant les échanges audiovisuels, à des fins d'information, d'éducation et de recherche et le traitement de données cliniques et administratives [...] »³⁵

Le terme *téléservices* employé ici intègre le concept de télésanté en plus de toutes les autres applications d'échanges audiovisuels qui peuvent être utilisées dans un contexte autre que clinique, telles que des rencontres à caractère administratif ou des échanges entre experts dans un domaine particulier.

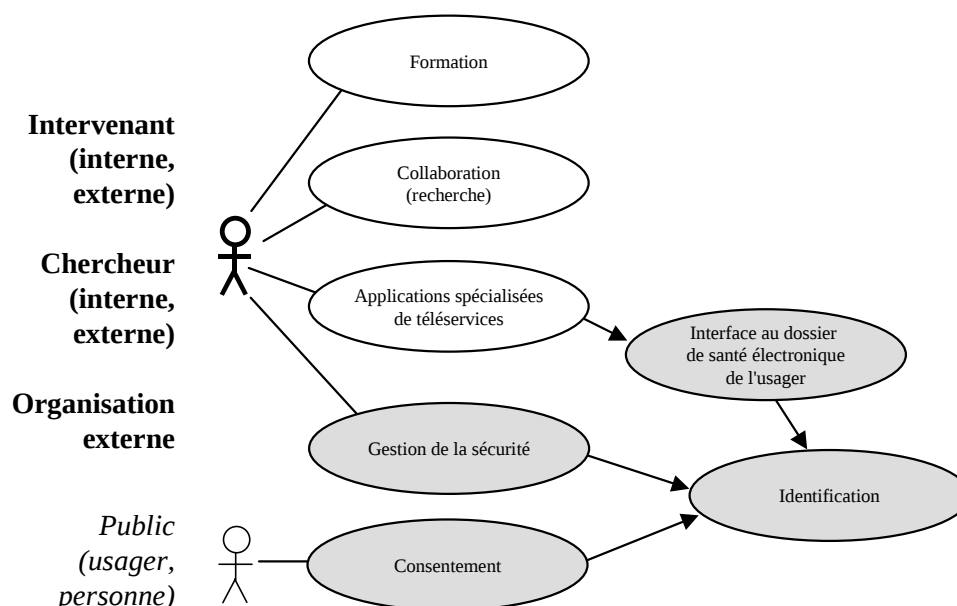
Les orientations de la présente section s'intéressent plus particulièrement aux téléservices à base de technologies d'imagerie animée ou fixe et à la vidéoconférence. Certains aspects des téléservices sont cependant couverts dans d'autres sections, plus précisément celles qui ont trait aux dossiers électroniques des usagers (section 3.1), à la sécurité et aux passerelles d'échanges électroniques (section 3.5), ainsi qu'aux télécommunications (section 3.6).

Le diagramme 16 situe le contexte d'utilisation des téléservices à l'intérieur de la portée des présentes orientations spécifiques. L'illustration suppose que, dans l'exercice de ses fonctions, un intervenant (interne ou externe au réseau sociosanitaire) utilise des applications spécialisées de téléservices ainsi que des applications de formation et de collaboration à distance.

Le diagramme suppose également que :

- les applications spécialisées utilisées par l'intervenant sont en relation avec le dossier de santé électronique de l'utilisateur, lui-même relié au système d'identification des usagers et des intervenants ;
- l'accès aux systèmes est sécurisé par des mécanismes appropriés de gestion de la sécurité ;
- l'utilisateur doit consentir au partage de l'information de son dossier.

35. Claude POIRIER, *La télésanté au Québec : Vision et orientations*, document présenté dans le cadre du colloque sur les ressources informationnelles organisé par le ministère de la Santé et des Services sociaux le 13 juin 2001, p. 7.

Diagramme 16 : Contexte d'utilisation des téléservices

Tout en prenant en considération les relations entre les différents systèmes, les présentes orientations portent plus particulièrement sur les applications spécialisées de téléservices ainsi que sur celles se rapportant à la formation et à la collaboration (représentées par des ovales à fond blanc dans le diagramme). Les autres systèmes (ovales à fond gris) sont couverts dans les sections 3.1 et 3.5, qui portent respectivement sur le dossier électronique de l'utilisateur et sur la sécurité.

3.2.1 Éléments de contexte

Organisation des téléservices

L'arrivée du RTSS et l'évolution technologique récente liée à la numérisation des images, aussi bien animées que fixes, ont suscité une recrudescence marquée des projets de téléservices dans le réseau sociosanitaire québécois. D'abord déployées sur la base de projets d'expérimentation avant d'être considérées en activité, des applications de téléservices ont été conçues pour plusieurs spécialités telles que la cardiologie pédiatrique, la radiologie, la psychiatrie, l'orthophonie et la dermatologie. Des projets ont également permis de mettre en place des infrastructures de téléservices pour la formation et la recherche.

Sur le plan organisationnel, ces initiatives ont amené la création de réseaux actifs de téléservices, comme le Réseau québécois de télésanté pour enfants (RQTE) et le Réseau mère-enfant instauré par l'hôpital Sainte-Justine. Il existe également quelques réseaux internationaux, soit :

- le Centre hospitalier universitaire de Québec avec le CHU de Grenoble ;
- le Centre hospitalier universitaire de Montréal avec Toulouse-Strasbourg ;
- l'hôpital Sainte-Justine avec le CHU de Lille.

Chaque réseau est une structure d'organisation de services auxquels participent plusieurs établissements. Ceux d'entre eux qui disposent de spécialistes offrent leurs services à distance aux autres établissements. Des technologies spécialisées et des infrastructures de télécommunications sont déployées afin de permettre les communications audiovisuelles et les échanges de données nécessaires au réseau de services. Sauf pour les communications externes au réseau sociosanitaire, le RTSS fournit les services requis de télécommunications.

Bien qu'il soit mis en place pour réaliser une expérimentation dans un secteur donné d'activités, un réseau de téléservices, une fois opérationnel, peut être considéré comme une plate-forme autour de laquelle se grefferont d'autres projets.

Les réseaux de téléservices utilisent différentes solutions conçues par des fournisseurs tels que CIFRA Médical, Polycom et Tandberg. Comme ce sont des applications spécialisées, le soutien à l'utilisation et à l'exploitation est généralement offert par le fournisseur.

En ce qui a trait aux télécommunications, la gestion d'ensemble est assurée par le Ministère alors que le soutien de premier niveau est offert par le technocentre national. La gestion des opérations du réseau ainsi que le soutien de deuxième niveau sont sous la responsabilité du Groupe des Télécommunicateurs du Québec (GTQ).

Des structures de gestion ont aussi été mises en place pour ce qui est de l'encadrement général des projets de téléservices, notamment la Table ministérielle en télésanté et le Comité directeur technique en télésanté. De plus, le Bureau d'accueil des applications et son Centre de certification participent aux projets de téléservices pour s'assurer, entre autres, de la performance de ces systèmes sur le RTSS.

État de situation des applications

Comme il a été mentionné à la section précédente, les applications de téléservices sont d'abord déployées sur la base de projets d'expérimentation avant d'être considérées en activité. À l'heure actuelle, un ensemble d'applications est donc

considéré en activité tandis qu'un autre ensemble en est plutôt à la phase de développement dans le cadre de projets d'expérimentation. Ces diverses applications utilisent principalement des technologies de vidéoconférence, d'imagerie médicale, de stockage de vidéos, d'images et de sons ainsi que des technologies de télésurveillance.

Les applications mises en place jusqu'à maintenant tiennent généralement leurs propres dossiers d'utilisateurs. L'intégration au dossier électronique élargi de l'utilisateur et à son dossier réseau est perçue comme un défi à relever.

Le tableau 2 montre la situation des applications actuellement en activité. Il indique aussi les types de technologies utilisées et, le cas échéant, l'existence d'une interface à un dossier électronique élargi d'utilisateur.

Tableau 2 : Applications de téléservices en activité et leur technologie

Applications	Vidéo- conférence	Technologies					
		Imagerie médicale		Conservation		Interface au dossier électronique	Télémétrie et autres
		Fixe	Animée	Vidéo	Image		
Téléconsultation :							
Cardiologie	X	X	X		X		
Cardiologie pédiatrique	X	X	X		X		
Radiologie	X	X		X	X	À court terme	
Psychiatrie	X			non			
Traumatologie	X	X	X	X	X		
Télétraitement en orthophonie	X			X			
Télédermatologie	X	X		non			
Télésurveillance (ex. grossesses à risque)	X			non			X
Téléformation	X	X	X	X			
Recherche	X	X	X	non			

Quant à la situation des applications encore en développement, elle est présentée au tableau 3.

Tableau 3 : Applications de téléservices en développement et leurs technologies

Applications	Vidéo- conférence	Imagerie médicale		Conservation		Interface au dossier électronique	Télémétrie et autres
		Fixe	Animée	Vidéo	Image		
Télénéphrologie	X	X					
Télépathologie		X	X		JPEG		
Téléophtalmologie		X			JPEG		
Téléradio-oncologie		X	X		X		
Télé mammographie		X			X		
Télétraumatologie	X	X	X		X		
Télésurveillance à domicile :							
Personnes âgées	Web						X
Fibrose kystique	Web						X
Soins palliatifs	Web						X
Maladies chroniques	Web						X
Téléadaptation	Web						

Enjeux relatifs aux téléservices

Les travaux de la Table ministérielle en télésanté ont mis en évidence des enjeux organisationnels, socioéconomiques et médico-légaux importants quant aux applications de téléservices³⁶. À cela s'ajoutent plusieurs enjeux technologiques soulevés à l'occasion des ateliers qui ont eu lieu dans le cadre du projet d'actualisation des orientations technologiques du réseau. Ces derniers sont de deux types :

- ceux qui ont trait à la gestion des technologies, comme le besoin de définir des processus pour gérer les paramètres d'acceptabilité des solutions technologiques, l'intégration des partenaires participant à la prestation de services (cliniques privées et autres), le télétravail, la sécurité et la conservation de l'information ;
- ceux de nature plus technique, qui concernent par exemple les stratégies de stockage des informations, l'automatisation de la gestion de la bande passante dans un contexte d'applications multiples et la communication simultanée entre plusieurs utilisateurs, notamment pour la formation et les téléconsultations.

36. Ces enjeux sont décrits dans le rapport *Vision, orientations et stratégies de développement de la télésanté au Québec*, préparé par la Table ministérielle en télésanté et publié en janvier 2001 par le ministère de la Santé et des Services sociaux.

Le tableau 4 résume l'ensemble des enjeux concernant les téléservices.

Tableau 4 : Enjeux propres aux projets de téléservices

Enjeux organisationnels
- Rôles et responsabilités des intervenants - Coordination des multiples organisations (établissements, RRSSS, MSSS) - Initiatives individuelles - Nouvelles pratiques en télésanté - Répercussions sur l'organisation du travail - Motivation des intervenants
Enjeux socioéconomiques
- Importance des investissements requis - Difficulté de trouver du financement - Réceptivité des utilisateurs - Rémunération des professionnels - Avantages pour les participants - Absence de rentabilité immédiate - Projets structurants
Enjeux médico-légaux
- Lieux de pratique - Responsabilité professionnelle - Responsabilité de l'établissement - Consentement de l'utilisateur - Contenu du dossier médical - Encadrement de la délégation des actes médicaux

Enjeux de gestion des technologies

- Applicabilité des solutions technologiques à la pratique professionnelle
- Intégration des cliniques privées
- Utilisation en mode télétravail
- Sécurité des échanges d'informations
- Passage du mode expérimental à un mode d'utilisation courante
- Veille stratégique et technologique
- Gestion de la conservation de l'information (responsabilités, gestion des copies de sécurité, optimisation de l'accès aux images et aux données, archivage)
- Simplicité d'utilisation et mécanismes d'aide en ligne
- Nombre adéquat des ressources de soutien

Enjeux de nature technique

- Stockage local versus concentré
- Gestion de la bande passante dans un contexte d'applications multiples
- Résolution des images et de la vidéo
- Utilisation simultanée par plusieurs utilisateurs
- Communication à l'extérieur du RTSS
- Interopérabilité des équipements (opérabilité entre différentes marques et entre différents types d'équipement)
- Intégration de l'architecture du réseau de téléservices et de l'architecture du réseau du domaine médico-administratif

Tendances technologiques

Les tendances technologiques plus particulières au domaine des téléservices touchent les aspects de la normalisation des protocoles de vidéoconférence et d'imagerie médicale, l'intégration avec les technologies du type Web et la gestion des diverses formes d'information.

Les protocoles suivants sont les points de référence de l'industrie :

- pour la vidéoconférence, la suite de standards H.3xx³⁷ distribuée par l'ITU³⁸ est définie afin de permettre des échanges d'informations basés sur différents protocoles de réseau (par exemple, MTA et Ethernet) ;
- pour l'imagerie médicale, la majorité des applications respectent la norme DICOM et des composantes de type DICOMobject peuvent donner lieu à de nouveaux développements ;
- pour le son, le format MP3 s'est imposé dans le marché et son usage est déjà répandu ;
- pour l'interface au dossier électronique, plusieurs logiciels sont compatibles avec les standards HL7.

Enfin, de plus en plus de produits fonctionnant en mode Web apparaissent sur le marché. Plusieurs de ces produits respectent les normes du domaine, dont les standards H.323 pour la vidéoconférence et DICOM pour l'imagerie médicale. Ce type de solutions devrait connaître une croissance significative pour les téléservices dans les prochaines années car :

- elles permettent d'intégrer la vidéoconférence ainsi que l'imagerie animée et fixe à d'autres applications ;
- certaines d'entre elles favorisent les échanges en multipoint et permettent également l'utilisation d'outils complémentaires, notamment pour l'affichage d'images ;
- elles ont en général les avantages de diminuer les coûts, d'être facilement accessibles, de faciliter l'intégration à d'autres applications, de permettre une plus grande mobilité à l'utilisateur et d'éviter l'utilisation de locaux spécialement aménagés ;
- elles sont accessibles, comme tout autre service électronique, à partir du portail.

37. Où xx renvoie à la numérotation des différents standards comme H.320 ou H.323.

38. International Telecommunications Union.

Par ailleurs, tout comme les technologies plus spécialisées, les technologies Web sont tributaires de la capacité du réseau de télécommunications à fournir de la bande passante d'une façon adéquate. La qualité des images dépend principalement de la bande passante disponible.

En outre, les technologies de *content management*, qui permette de gérer toutes sortes de contenus (image, voix, dossier numérisé, etc.), sont en plein essor.

Enfin, une tendance à la certification, entre autres pour la qualité des images, est observée. Selon cette tendance, la certification des équipements préciserait les conditions dans lesquelles ils sont recommandés par les cliniciens.

Principaux constats

La situation actuelle en matière de téléservices et les grandes tendances technologiques de ce domaine permettent d'établir des constats en matière d'encadrement ainsi qu'en matière de systèmes et de technologies.

Deux principaux constats ressortent quant à l'encadrement de gestion des téléservices :

- une stratégie d'évolution des téléservices et des orientations administratives doivent être élaborées pour répondre aux enjeux organisationnels, socioéconomiques et médico-légaux en définissant :
 - les rôles, les responsabilités et la politique de rémunération qui s'appliquent aux professionnels de la santé utilisant ces technologies,
 - le processus de gestion des projets de téléservices (planification d'ensemble, établissement des priorités, mécanismes de soutien, gestion des résultats et évaluation, par exemple),
 - les règles de conservation de l'information des téléservices (vidéoconférence, imagerie médicale, données sur l'utilisateur, information de gestion),
 - la façon de gérer les conséquences du transfert des coûts vers la population dans le contexte des téléservices à domicile, télésurveillance, par exemple ;
- le processus de certification des applications permettant d'assurer la performance et la sécurité des services sur le RTSS et une meilleure interopérabilité des applications doit aussi prévoir des volets complémentaires, ceux-ci étant :

- la définition des spécifications fonctionnelles, par les experts en télésanté, pour chaque modalité ou spécialité (cardiologie, radiologie, psychiatrie, entre autres), soit les fonctions nécessaires et optionnelles ainsi que la qualité requise selon les usages (vidéo, audio, imagerie),
- une veille stratégique et technologique permettant l'actualisation périodique de la stratégie d'évolution des téléservices en relation avec les orientations technologiques, les conditions d'intégration au RTSS et les spécifications fonctionnelles propres à la télésanté.

Quant aux aspects systémiques et technologiques, les constats sont les suivants :

- le RTSS est une infrastructure technologique d'importance majeure pour le développement des téléservices ;
- un ensemble de standards reconnus sur le plan international régit la vidéoconférence et l'imagerie médicale (H.3xx, DICOM) ;
- les liens entre les applications de téléservices, le dossier électronique de l'usager et son dossier réseau (DERUS) sont à faire ;
- l'utilisation des technologies Web en mode intranet ouvre de nouvelles perspectives encore peu considérées et explorées dans les expérimentations faites jusqu'à présent ;
- les projets de téléservices comportent plusieurs enjeux de nature technique devant être gérés, dont :
 - la performance locale des sessions de téléconférence,
 - la communication simultanée entre plusieurs utilisateurs (mode multipoint),
 - la gestion de la bande passante,
 - la qualité variable des équipements et des résultats, en fonction des besoins de qualité sur le plan clinique,
 - l'interopérabilité des applications et des équipements,
 - les stratégies de stockage et de gestion de la conservation des informations,
 - les communications hors RTSS.

3.2.2 Principes directeurs en matière de téléservices

Pour la détermination des orientations technologiques spécifiques en matière de téléservices, il est pris pour hypothèse qu'une stratégie d'évolution et des orientations administratives seront définies pour les téléservices et que le cadre de gestion qui en découlera prévoira les mécanismes permettant de :

- réaliser une révision architecturale *a priori* des projets, aussi bien sur le plan clinique (selon les exigences définies par les utilisateurs) que sur le plan technologique (par des essais ou une preuve de concept) ;
- poursuivre le processus systématique de certification *a posteriori* des applications de téléservices pour assurer l'interopérabilité des technologies ainsi que le respect des normes techniques et des spécifications fonctionnelles sur le plan clinique adoptées par le réseau ;
- faciliter les expérimentations dans de nouveaux champs de pratique tout en s'assurant du respect de l'encadrement, dont :
 - une définition de projet conforme au *Guide de présentation des projets de télésanté*,
 - les mesures adéquates de soutien (financement, expertise),
 - une évaluation post-expérimentation.

Sur le plan technologique, une architecture d'ensemble des téléservices doit être réalisée à partir de l'évolution des besoins observée autant au niveau clinique qu'au niveau administratif. Cette architecture permettra de déterminer les façons d'atteindre l'utilisation optimale des applications déjà implantées dans le réseau et d'éviter le dédoublement des investissements dans ce type d'infrastructures technologiques. Par exemple, la vidéoconférence peut être utilisée autant à des fins cliniques, comme une téléconsultation, qu'à des fins administratives, comme des rencontres de comités nationaux ou régionaux. Une fonction de coordination (à portée nationale ou régionale) des sessions de vidéoconférence permettrait d'élargir l'offre de services pour de telles conférences à l'ensemble du réseau. De même, le partage d'infrastructures peut être envisagé au moment du déploiement d'applications PACS dans le réseau, et ce, selon des modes qui respectent le cadre légal et juridique.

De façon générale, les applications de téléservices doivent tendre à s'inscrire dans les orientations technologiques générales du réseau socio sanitaire en interagissant avec leur environnement à l'aide des services communs selon les conventions établies. En ce sens, les applications de téléservices devront s'intégrer au portail intranet et utiliser des technologies du type Web, lorsque la situation s'y prête, partout où elles s'avèrent pertinentes et performantes. De plus, tout comme les

autres applications de soutien aux intervenants, les données issues des applications de téléservices devront s'intégrer au dossier électronique de l'utilisateur à l'aide des services communs.

Elles devront également utiliser les services communs de sécurité. Les technologies qui comportent des fonctions évoluées de gestion de sécurité et qui utilisent le protocole LDAP devront être privilégiées. Cela permettra l'intégration aux répertoires de sécurité des environnements de base et globaux (définis dans le modèle de référence des orientations technologiques générales du chapitre 2).

Les infrastructures de soutien aux applications de téléservices devront enfin faire appel aux services communs de gestion d'infrastructures partagées et respecter les normes nécessaires à la gestion de réseau, soit le protocole SNMP ou un protocole conforme au CIM.

Quant aux solutions de conservation des informations, elles devront s'aligner sur la stratégie d'évolution qui sera retenue. Elles devront également respecter les normes et les protocoles d'échanges avec les services électroniques communs du réseau. Un principe de hiérarchisation du stockage est recommandé afin de rentabiliser les investissements technologiques et d'assurer la continuité opérationnelle.

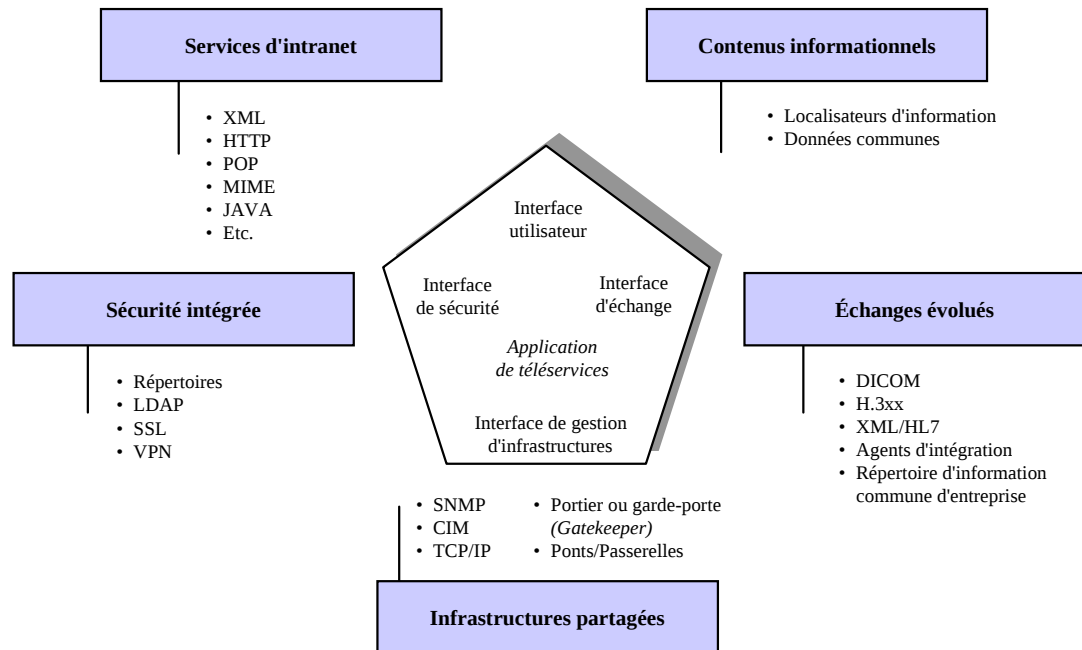
Les orientations relatives aux télécommunications dans le contexte des téléservices sont spécifiées à la section 3.6.

3.2.3 Perspectives conceptuelles

En complément aux perspectives conceptuelles du modèle technologique de référence présenté au chapitre 2, les concepts et les modèles abordés dans la présente section sont ceux qui ont été retenus pour la mise en place d'infrastructures technologiques et de services électroniques communs capables de les supporter afin d'assurer les téléservices. Une vue des services électroniques communs et une vue des infrastructures technologiques sont présentées ci-après.

Vue des services communs

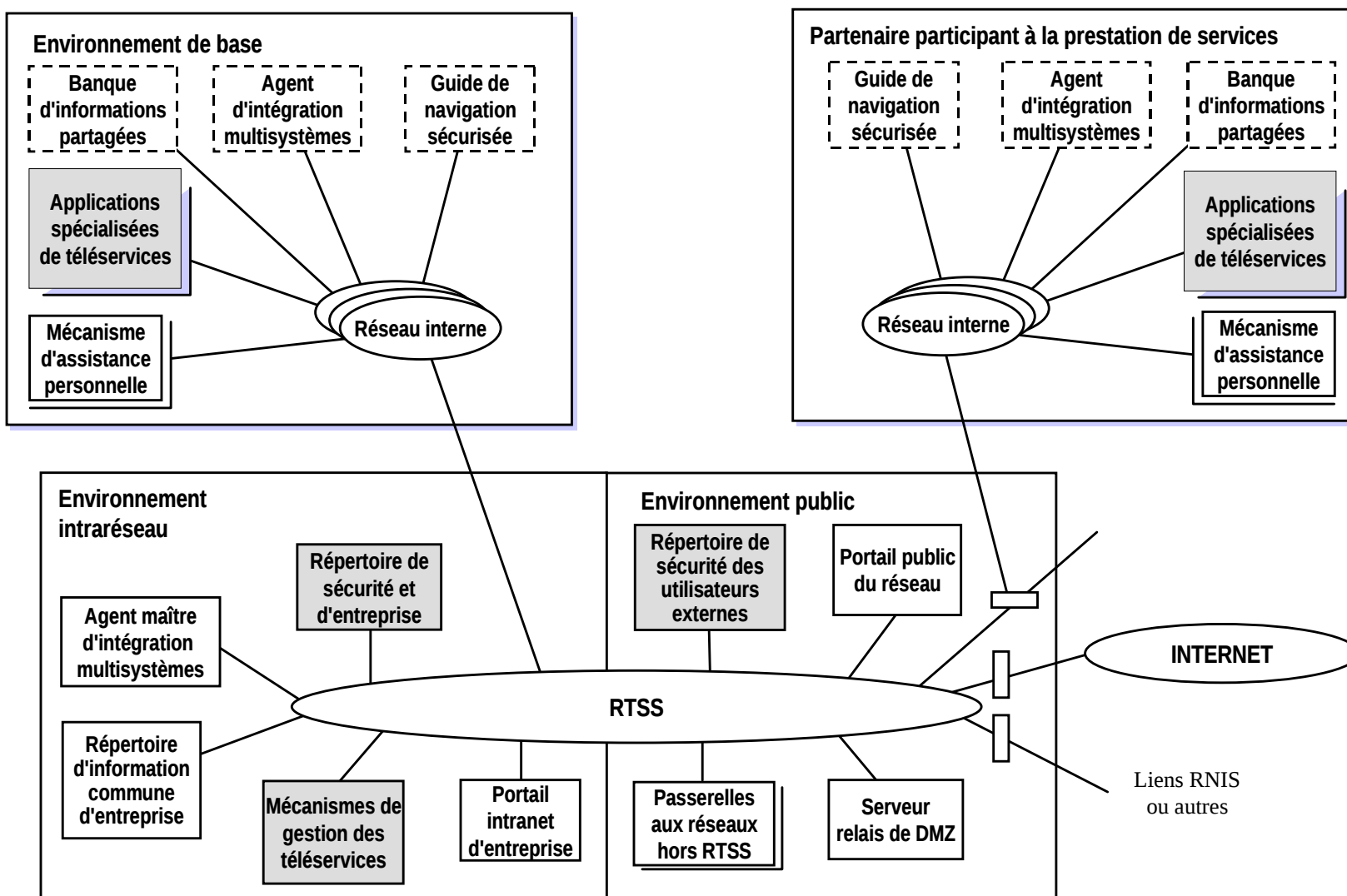
Les concepts et les modèles de services communs définis dans le modèle technologique de référence présenté au chapitre 2 permettent de soutenir la mise en œuvre des téléservices. Le diagramme 17 rappelle la vue d'ensemble des services communs et il indique, pour chaque classe de services, les concepts et les types de standards associés au soutien des téléservices. Les protocoles d'échanges évolués DICOM et H.3xx se rapportent plus particulièrement aux applications de téléservices.

Diagramme 17 : Vue des services communs pour les téléservices*Vue des infrastructures technologiques*

La vue des infrastructures technologiques est illustrée par le diagramme 18. Elle est complémentaire à la vue de second niveau des infrastructures technologiques présentée dans le modèle technologique de référence du chapitre 2 et elle utilise le même symbolisme de représentation.

Conformément aux principes directeurs abordés dans la présente section sur les téléservices, la vue des infrastructures fait apparaître un nouveau type d'applications spécialisées dans les environnements de base et globaux ainsi que des mécanismes de gestion des téléservices.

Diagramme 18 : Vue des infrastructures technologiques pour les téléservices



Les composantes technologiques se définissent comme suit.

- Applications spécialisées de téléservices :

Ce sont des applications faisant appel à des technologies d'imagerie animée ou fixe, ou encore à la vidéoconférence. Ces applications sont caractérisées par :

- l'utilisation par les membres d'un regroupement d'utilisateurs ou d'une communauté de pratique, qu'ils soient internes ou externes au RTSS ;
- une interface Web s'intégrant au guide de navigation sécurisée lorsqu'une telle intégration est possible et pertinente ;
- la possibilité de soutenir des échanges multipoints entre plusieurs utilisateurs pour les applications qui le requièrent ;
- le respect des standards retenus, dont H.3xx et DICOM ;
- la capacité de répondre à une requête standard en provenance de l'agent d'intégration (en HL7/XML) ;
- l'utilisation, le cas échéant, d'une largeur de bande fixe pour la durée d'une session d'échange.

- Mécanismes de gestion des téléservices :

Ces mécanismes de gestion comprennent des fonctions de gestion des sessions de téléservices, telles que la réservation de ressources (équipements, salles, bandes passantes, soutien technique, etc.) dans le cas de la vidéoconférence. Il permet de gérer la sécurité des sessions de téléservices à partir du répertoire de sécurité et d'entreprise. Ces mécanismes peuvent comprendre plusieurs composantes technologiques, dont :

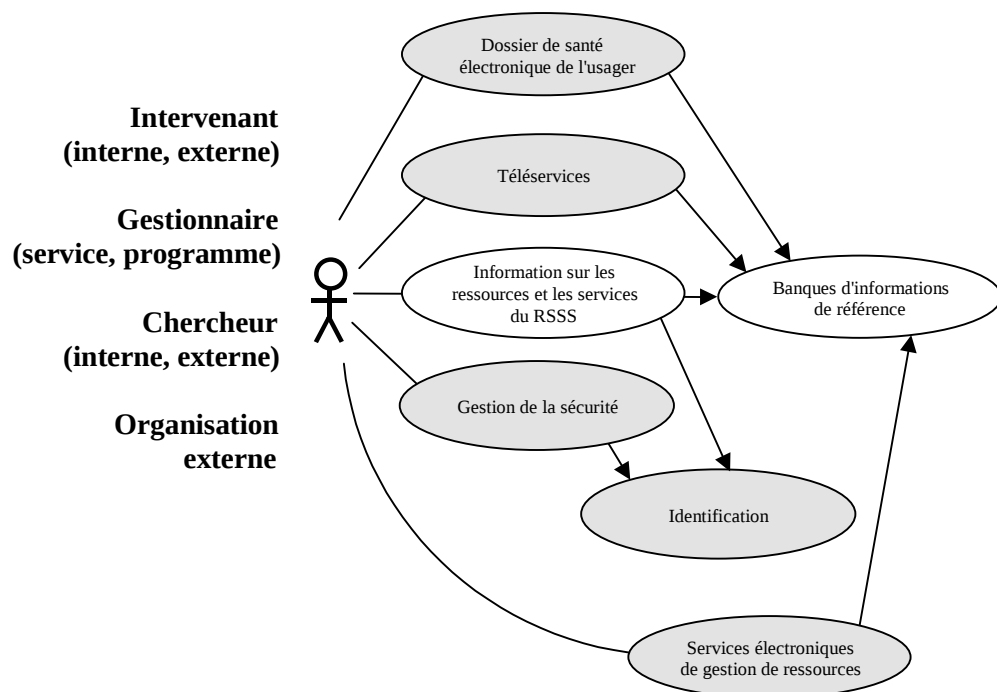
- un serveur sur lequel se retrouvent une ou plusieurs applications particulières, pour soutenir la gestion des sessions de téléservices ;
- un portier (ou garde-porte), pour permettre la gestion des disponibilités, des réservations et des priorités ;
- des ponts et des passerelles permettant l'établissement de session intraréseau RTSS sur des liens MTA ou IP ainsi que des liaisons externes (avec le RISQ et des partenaires internationaux).

3.3 Les orientations en matière de services électroniques d'information sur les ressources et les services

Le domaine des services électroniques d'information sur les ressources et les services regroupe les banques de données et les systèmes d'information utilisés aux fins d'analyse et de gestion d'ensemble, et ce, aussi bien pour les *ressources* financières, humaines et matérielles que pour les *services* aux usagers du réseau. Ces systèmes, souvent appelés *informationnels*,³⁹ comprennent notamment des systèmes d'aide à la décision et de tableaux de bord ainsi que des comptoirs et des entrepôts de données. Ils utilisent diverses technologies, allant des outils les plus conventionnels jusqu'aux outils d'exploitation de données dits d'intelligence stratégique (*Business Intelligence*), en passant par les outils de modélisation, de collecte et de stockage de données, qui servent à constituer des dépôts de données faciles à exploiter.

Le diagramme 19 montre le contexte d'utilisation des systèmes d'information sur les ressources et les services.

Diagramme 19 :
Contexte d'utilisation des systèmes de type informationnel



39. Les expressions *système d'information sur les ressources et les services* et *système informationnel* seront utilisées comme des équivalents dans la présente section du document.

Le diagramme 19 suppose que les systèmes informationnels répondent aux besoins de plusieurs classes d'utilisateurs (intervenant, gestionnaire, chercheur, organisation externe au réseau). Ces systèmes utilisent des *banques d'information de référence*. Ces dernières sont aussi utilisées par plusieurs autres systèmes, comme ceux qui traitent les dossiers de santé électroniques de l'utilisateur, les téléservices et la gestion des ressources⁴⁰. En fait, les informations de référence comprennent :

- les données de référence pour l'ensemble des systèmes d'information, comme le découpage territorial, l'identification des établissements, les centres d'activité, les données sur la population, les systèmes de classification comme CIM 10, les référentiels cliniques, et les référentiels de pratique ;
- les métadonnées informationnelles, qui décrivent les données des systèmes d'information et leur contexte de saisie ; ces métadonnées font l'objet de produits documentaires qui comprennent des cadres normatifs de données, des dictionnaires de données et des classifications.

Comme l'indiquent les deux ovales à fond blanc dans le diagramme 19, les orientations en matière de services électroniques d'information sur les ressources et les services s'intéressent plus particulièrement aux systèmes informationnels, ce qui inclut les *banques d'information de référence*, tout en prenant en considération les différents systèmes.

La présente section précise le contexte des systèmes informationnels et les orientations retenues à cet égard pour le réseau socio-sanitaire québécois.

3.3.1 Éléments de contexte

Chaque organisation du réseau est susceptible d'avoir des systèmes informationnels pour ses fins propres. Le Ministère et les régies régionales utilisent aussi leurs systèmes informationnels pour fournir des informations ou des données à leurs clientèles.

De son côté, la RAMQ gère un ensemble de banques de données offrant un fort potentiel informationnel.

Les paragraphes qui suivent décrivent sommairement l'état de situation pour le Ministère, la RAMQ, les régies régionales et les établissements. Ils présentent aussi certains faits saillants généraux, les tendances technologiques liées au domaine et un ensemble de constats.

40. Les systèmes de gestion de ressources correspondent à des applications de nature administrative permettant de gérer les ressources financières (comptabilité, paie, etc.), humaines (horaires de travail, assignation, etc.) et matérielles (inventaires de médicaments et de fournitures, par exemple).

Situation du Ministère

Le Ministère a un rôle de gestion d'ensemble des informations en matière de services de santé et de services sociaux. Il doit définir les orientations et les architectures d'information et de systèmes, et il doit également voir à la définition, au maintien et au soutien de métadonnées informationnelles. C'est à ce titre qu'il gère les cadres normatifs et les dictionnaires de données des systèmes, qu'il constitue des banques d'information de référence et qu'il a amorcé depuis peu un projet d'architecture globale de l'information.

En plus de son rôle de gestion d'ensemble des informations, le Ministère gère :

- la consolidation des données sur les ressources financières, humaines et matérielles (par exemple, les rapports financiers annuels) ainsi que sur les services aux usagers du réseau (par exemple, les soins de courte durée) ;
- des services de diffusion d'informations.

Les services de diffusion consistent à extraire les données de différentes banques et à produire les informations nécessaires afin de répondre aux requêtes des utilisateurs. À titre indicatif, le Service de l'infocentre du Ministère (à la Direction des technologies de l'information et des télécommunications) a traité environ 600 demandes en 1999-2000. Le tableau 5 montre la répartition de ces demandes par client.

Les principales technologies utilisées pour la consolidation de données et les services de diffusion sont des outils conventionnels pour les banques de données sur ordinateur central (OS/390), une plate-forme Teradata et des outils du type Web.

Tableau 5 :
Répartition des demandes faites au Service de l'infocentre par client

Requérant	%
Ministère de la Santé et des Services sociaux	40 %
Régies régionales	5 %
Directions régionales de la santé publique	5 %
Centres hospitaliers	13 %
Autres organisations de l'administration publique	13 %
Individus et universités	12 %
Firmes privées	8 %
Autres requérants	4 %

Situation de la RAMQ

La RAMQ offre deux types de services d'intérêt au regard des systèmes informationnels :

- des services de diffusion pour ses propres banques de données ;
- des services de gestion de banques de données déposées par le Ministère et d'autres organisations du réseau.

La Régie rend disponibles des informations et des données à travers ses services de diffusion⁴¹. À cette fin, elle puise dans ses propres banques de données, soit celles qui portent sur :

- la rémunération et les services rendus (services rendus à l'acte, services rendus à salaire, etc.) ;
- l'identification (fichier d'inscription des personnes assurées, fichier d'inscription des professionnels, fichier RAMQ des établissements) ;
- les données de référence (liste des services médicaux assurés, liste des médicaments assurés, fichier RAMQ des lieux géographiques).

La RAMQ exploite également les banques de données déposées par le Ministère, soit celles qui portent sur :

- les données statistiques (rapport statistique annuel des centres de la protection de la jeunesse, rapport statistique annuel des centres hospitaliers et des centres hospitaliers de soins de longue durée, etc.) ;
- les données financières (rapport financier annuel des établissements) ;
- les données médico-hospitalières (hygiène mentale, données d'hospitalisation, etc.) ;
- d'autres données (données sur la population, recensements).

Les services de diffusion de la RAMQ produisent des extractions sous forme de fichiers. Ces services sont facturés à ses clients.

Les principales technologies utilisées à la RAMQ pour les systèmes informationnels sont une plate-forme centrale de type OS/390 et une plate-forme Teradata.

41. La description sommaire des banques de données disponibles à la RAMQ est tirée du document *Portrait des banques de données disponibles à la Régie de l'assurance maladie du Québec*, Québec, RAMQ, 2000.

Situation des régions régionales

La situation des systèmes du type informationnel au sein des régions régionales est marquée par :

- l'existence de plusieurs systèmes de gestion régionale de ressources (système de suivi budgétaire et financier régional – SBF-R –, systèmes de gestion du transport ambulancier et plusieurs autres) ;
- des services d'exploitation de données exclusifs aux directions régionales de la santé publique ;
- la mise en place progressive des infocentres régionaux, surtout depuis 1996.

Dans le cadre du projet des infocentres régionaux, les régions régionales se sont dotées d'une typologie des données qui est indicative de leurs besoins⁴². Cette typologie est résumée dans le tableau qui suit.

Tableau 6 : Typologie des données des régions régionales

Données de l'environnement socio-sanitaire	Données sur la production des services
- Données démographiques - Données socioéconomiques - Données propres à la santé - Données environnementales	- Données sur les clientèles - Données de facturation des professionnels de la santé
Données sur les ressources	Données de référence
- Données budgétaires et financières - Données sur les ressources humaines - Données sur les ressources matérielles - Données sur les activités de coordination	- Réseau, secteur et partenaires - Territoires - Table de références diverses - Métadonnées

42. Selon le *Guide d'accompagnement pour l'implantation des entrepôts régionaux de données*, 2000.

Des infocentres sont déjà en place dans certaines régions. En général, ces infocentres sont caractérisés par :

- l'utilisation de sous-ensembles de données couvrant le plus souvent une partie restreinte des besoins ;
- une convention initiale d'utilisation du SGBD Oracle sous Unix (orientation en évolution) ;
- différents outils d'exploitation des données, dont :
 - Excel, Access,
 - SAS, SPSS,
 - Média, de Speedware, pour quelques utilisateurs,
 - Impromptu, de Cognos, pour quelques utilisateurs.

Le projet des infocentres régionaux a permis de mettre en place des banques de données et des outils utiles. Cependant, le développement de ces infocentres s'est heurté à plusieurs difficultés :

- le faible niveau d'investissement ;
- les contraintes légales ne permettant que la conservation de données non nominatives ;
- les disparités et les faiblesses structurelles des systèmes fournisseurs de données, en particulier en ce qui a trait à l'utilisation de données de référence ;
- la dépendance vis-à-vis des fournisseurs de données, tels que le MSSS, la RAMQ, les établissements et d'autres organisations externes (Société de l'assurance automobile du Québec, Ministère de la Solidarité sociale, Institut de la statistique du Québec, Statistique Canada, etc.).

Situation des établissements

De façon générale, la situation des établissements, en ce qui a trait aux systèmes informationnels, se caractérise comme suit :

- la possibilité d'obtenir des données nominatives sur les usagers à partir des systèmes opérationnels locaux ;
- l'accès aux données que ces établissements possèdent sur les ressources à partir de systèmes de gestion des ressources financières, humaines et matérielles. Ces systèmes souvent locaux sont disparates ;

- les possibilités de couplage de données sont généralement limitées aux données de l'établissement ;
- des rapports statutaires sont fournis par certains systèmes locaux (par exemple Med-Echo et I-CLSC) ;
- l'accès à l'infocentre régional lorsqu'il est implanté ;
- l'accès aux services de diffusion du Ministère et de la RAMQ.

Par ailleurs, certains établissements exploitent plus systématiquement leurs propres banques de données avec des outils spécialisés de génération récente. Ces outils rendent possible une certaine intégration des données de l'établissement afin de pouvoir fournir plus rapidement de meilleures informations sur les ressources, les services et les usagers.

Faits saillants de nature générale

Certains faits saillants de nature générale doivent être pris en considération en ce qui a trait aux systèmes informationnels.

D'abord, l'exploitation des données est actuellement soumise à un encadrement légal contraignant. Conformément à l'avis de la Commission d'accès à l'information du Québec (CAIQ), les renseignements nominatifs détenus par un établissement ne peuvent être transmis à l'extérieur, sauf à la demande du ministre ou à la suite d'une entente entre établissements ou avec la RAMQ.

Ensuite, exception faite des projets portant sur la constitution de banques de données informationnelles, la conception des systèmes d'information met souvent peu d'accent sur les contributions en matière d'information de gestion et d'information de référence. Cette situation rend plus difficile l'utilisation éventuelle des données à des fins administratives.

Notons également que la diffusion des informations et des données s'effectue non seulement à l'intérieur du réseau mais aussi avec des clients externes. D'ailleurs, la mise en place de l'infrastructure canadienne de la santé accentuera probablement les échanges de données de type informationnel avec les clients externes.

Soulignons enfin que les communications électroniques favorisent la diminution des délais de diffusion et l'autoservice par les utilisateurs.

Tendances technologiques

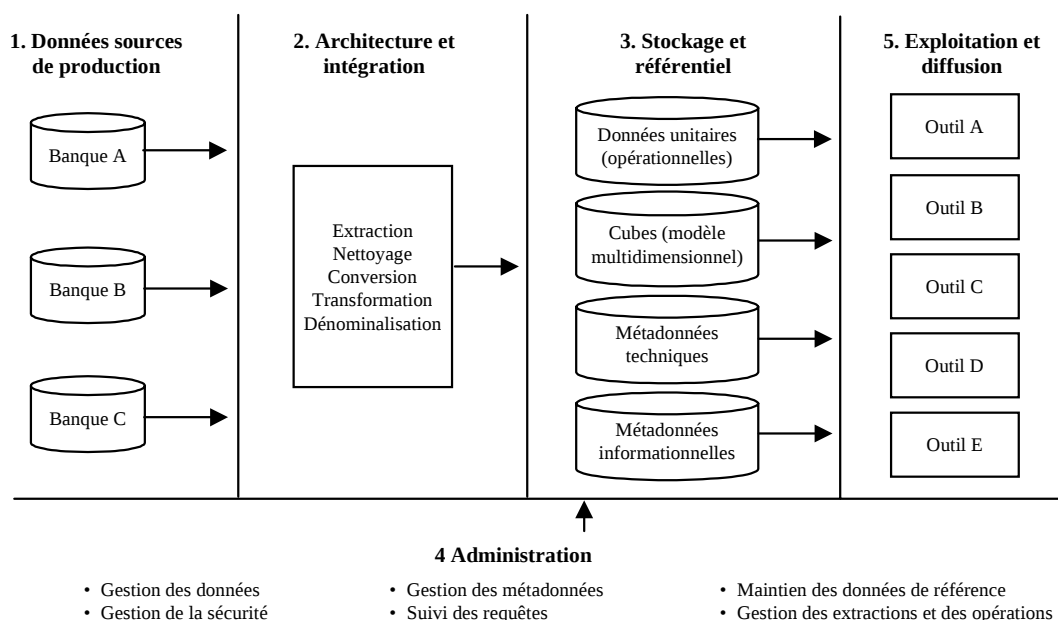
Le diagramme 20 présente une architecture simplifiée du fonctionnement d'un entrepôt de données. Cette architecture montre deux types de dépôts de données :

- les banques de données sources de production (point 1 du diagramme) ;
- les banques de données exploitables en mode informationnel (point 3 du diagramme).

Cette même architecture montre aussi trois catégories d'outils et d'applications :

- les outils d'architecture et d'intégration (point 2 du diagramme), qui permettent de constituer les banques de données exploitables à partir des banques de données sources ;
- les outils d'administration (point 4 du diagramme), qui servent à gérer les données, la sécurité, les métadonnées et l'opération de l'entrepôt de données ;
- les outils d'exploitation et de diffusion (point 5 du diagramme), qui sont soit des logiciels mis à la disposition de l'utilisateur pour exploiter les données et obtenir des informations, soit des applications qui exploitent les données pour fournir des résultats aux utilisateurs.

Diagramme 20 :
Architecture générique du fonctionnement d'un entrepôt de données



Les concepts de cette architecture simplifiée permettent de présenter ici les différentes catégories de produits offerts par les fournisseurs dans le domaine des systèmes informationnels. En fait, ces produits appartiennent à deux catégories principales :

- celle des *outils* d'intelligence stratégique (*Business Intelligence*), qui comprennent généralement des outils de requête et de reportage, des outils avancés d'analyse de type OLAP, des portails d'entrepôt de données (*BI Portals*) et parfois des outils de développement d'applications ;
- celle des *plates-formes* d'intelligence stratégique, qui comprennent généralement une suite complète de logiciels couvrant les outils d'architecture et d'intégration, les outils d'administration ainsi que les outils d'intelligence stratégique. Ces plates-formes peuvent également comprendre un système de gestion de bases de données (SGDB) et des outils de développement d'applications.

Plusieurs normes d'échanges électroniques d'information peuvent être supportées aussi bien par les outils que par les plates-formes, dont les normes LDAP, XML, OLE DB for OLAP, CORBA et COM/DCOM ou encore les normes d'Internet, comme HTTP et SSL.

Quelques tendances générales se dégagent de l'analyse des outils et des plates-formes :

- la plupart des outils OLAP permettent de travailler avec une structure de données multidimensionnelle, souvent appelée cube ;
- les mécanismes OLAP sont intégrés dans les SGBD sous différentes formes : ROLAP, MOLAP et HOLAP⁴³ ;
- il existe actuellement une inconsistance entre les métadonnées techniques de fournisseurs différents. De nouvelles normes seront bientôt établies afin de réduire ces inconsistances, dont le Common Warehouse Metamodel, ou CWM, et le XML Metamodel Interface, ou XMI (qui fonctionne de concert avec XML et UML) ;
- les fournisseurs de technologies du type OLAP se sont tournés vers les technologies d'Internet et ils offrent de plus en plus de produits fonctionnant sur plate-forme Web.

Principaux constats

L'état de situation, les faits saillants généraux et les tendances technologiques permettent de formuler plusieurs problèmes liés aux systèmes d'information sur les ressources et les services, dont les suivants :

43. Le ROLAP est un modèle fonctionnant avec un SGBD relationnel. Le MOLAP fonctionne avec un SGBD conçu pour supporter un modèle multidimensionnel. Enfin, le HOLAP est un hybride des deux approches.

- la faible couverture actuelle pour plusieurs catégories d'usagers (patients ambulatoires, clientèles du CLSC, personnes âgées en perte d'autonomie et enfants en difficulté, entre autres) ainsi que pour les prix de revient et le financement (par service et activité) ;
- le besoin d'information de comparaison avec d'autres provinces et d'autres pays ;
- les difficultés liées au besoin de saisir l'information utile à la gestion sans alourdir les tâches des intervenants ;
- le besoin de responsabiliser davantage les producteurs de données, notamment au regard de la qualité requise ;
- la saisie multiple des mêmes données ;
- la fermeture des progiciels des fournisseurs privés qui ne permet pas l'utilisation des données en mode informationnel ;
- l'absence d'outils de mesure en ce qui concerne de nombreux indicateurs de gestion ;
- la variabilité des fréquences de saisie et de transmission des données ;
- l'utilité moindre de l'information en raison de longs délais d'obtention ;
- le manque de ressources pour répondre aux demandes d'information ;
- les règles variables quant à la pratique de facturation des services de diffusion.

L'examen de la situation fait aussi ressortir des disparités importantes quant à l'utilisation des informations de référence dans les systèmes opérationnels. Ces disparités ont pour effet de réduire considérablement le potentiel informationnel des données en rendant ces données irréconciliables, elles empêchent des validations en ligne qui amélioreraient la qualité des données (fiabilité, validité et comparabilité) et elles entraînent des coûts élevés en matière d'échange d'information.

Ces problèmes mettent en lumière la nécessité d'une stratégie propre aux systèmes d'information sur les ressources et les services, et comportant une planification d'ensemble, afin de s'assurer :

- de la couverture suffisante des besoins d'information de gestion au moment de la conception des systèmes d'information ;
- de la mise en relation des données sur les ressources et les services ;
- de l'exploitation de données provenant des dossiers de santé électroniques des usagers ;

- de la cohérence entre les projets majeurs de système d'information reliés à l'IPP, au DPP, au système de RRG, à la carte d'accès santé, au Portail santé, etc. ;
- de la capacité de suivi du continuum des soins et services dans un contexte de mobilité des usagers.

Il apparaît par ailleurs que le manque de convergence entre les systèmes du type informationnel résulte, entre autres, d'une concertation insuffisante qui conduit à une compartimentation des systèmes par organisation, par région et par dimension (vision du même client selon plusieurs angles non reliés).

À cet égard, il est prévu que le projet d'architecture globale de l'information et la Table ministérielle sur le dossier patient provincial (DPP) mise en place en mai 2001 apportent une contribution substantielle.

Quant aux technologies, elles devront être en mesure de soutenir les stratégies qui seront adoptées.

Selon un article de GartnerGroup⁴⁴, la majorité des utilisateurs de systèmes informationnels ont seulement besoin d'informations générales qui consistent dans une large mesure en des rapports statiques et des vues préprogrammées. Un certain nombre d'utilisateurs dont le travail est plus axé sur l'information, et un nombre encore plus restreint d'analystes de l'information ont des besoins que peuvent satisfaire partiellement des rapports paramétrés ainsi que des requêtes *ad hoc* et des outils OLAP. C'est donc dire que ce type d'outils est destiné à une clientèle restreinte d'utilisateurs.

Sur cette base, et compte tenu du contexte décrit précédemment, il est prévisible :

- que la gamme de technologies utilisées pour les systèmes de type informationnel ira du produit de nature générique au produit sur mesure ;
- que les besoins de la majorité des utilisateurs seront satisfaits par des rapports et des requêtes paramétrables préparés par des services de diffusion ;
- qu'un nombre limité d'utilisateurs aura besoin d'outils sophistiqués d'intelligence stratégique.

Soulignons l'importance du RTSS comme instrument de soutien à la gestion des ressources et des services, et ce, sous plusieurs aspects, dont la collecte des informations, la diffusion de rapports et de fichiers d'extraits de données et la facilité d'accès aux outils d'exploitation des données.

44. « Business Intelligence Tools: Perspective Update », GartnerGroup, 1^{er} novembre 2000.

Enfin, la compatibilité des technologies avec les normes de l'industrie et l'évolution des produits vers la plate-forme Web devraient faciliter l'interopérabilité des systèmes d'information sur les ressources et les services et des systèmes de nature plus opérationnelle.

3.3.2 *Principes directeurs pour les services électroniques d'information sur les ressources et les services*

Les orientations en matière de services électroniques d'information sur les ressources et les services sont définies en fonction des présuppositions suivantes :

- la constitution des dépôts de données sur les ressources et les services du réseau sociosanitaire, exploitables à des fins de gestion, doit faire l'objet de stratégies précises tenant compte notamment :
 - de scénarios de consolidation de données cliniques, qui soient acceptables sur les plans légal et social et réalisables sur les plans administratif et technique,
 - de l'imposition possible de règles administratives pour l'alimentation de dépôts communs de données,
 - de la gestion du consentement de l'utilisateur à l'utilisation des informations qui le concernent,
 - des orientations technologiques favorisant l'intégration des informations,
- un dépôt de données comportant des données personnelles sur les usagers est nécessairement localisé dans les bureaux d'une organisation autorisée selon les lois actuelles (établissement, MSSS ou RAMQ), ce qui exclut la possibilité de le localiser chez un fournisseur externe au réseau aux fins d'exploitation en mode ASP ;
- l'exploitation des dépôts autorisés de données sur les ressources et les services doit être soumise aux règles suivantes :
 - les accès aux données unitaires sur les usagers sont limités à un groupe restreint de personnes dûment autorisées,
 - les accès aux données dénominalisées des usagers sont contrôlés et chaque utilisateur doit s'engager formellement à assurer la protection des renseignements personnels (en raison notamment des risques d'identification par recoupement de données) ;

- les stratégies de constitution et d'exploitation de dépôts consolidés de données devraient faire l'objet d'un avis favorable de la part des instances gouvernementales concernées par la protection des renseignements personnels.

Les stratégies qui seront adoptées pour les systèmes d'information sur les ressources et les services soit dans le cadre du projet d'architecture globale de l'information, soit par la Table ministérielle sur le DPP, ou encore dans le cadre d'autres projets ou par d'autres instances, permettront de préciser davantage les orientations technologiques.

En parallèle à la définition des stratégies, des actions seront nécessaires pour permettre la mise en place de systèmes et de technologies engendrant une plus-value en considération de l'évolution future. Ces actions portent sur :

- la constitution de *banques d'informations de référence* et la systématisation de leur utilisation en vue d'améliorer la qualité des données, ce qui implique :
 - la définition de métadonnées, de données de référence et de valeurs normalisées,
 - l'intégration des données de référence aux systèmes de toute nature et la validation en ligne des données,
 - la généralisation du mécanisme de mise à jour des banques d'informations de référence ;
- l'alignement sur les orientations stratégiques déjà définies, en particulier pour les besoins d'information relatifs au suivi et à l'évaluation de prix de revient, ce qui suppose :
 - des ajustements à la structure normalisée des données selon les besoins de gestion d'ensemble,
 - une généralisation du mécanisme de transfert d'information pour les données financières, humaines et matérielles ;
- l'amélioration des processus de gestion et d'exploitation des données au regard des dépôts d'information existants en vue de réduire les délais d'obtention de l'information par les utilisateurs.

Sur un plan plus technique, les systèmes d'information sur les ressources et les services doivent généralement faire en sorte :

- que les applications ainsi que les outils d'exploitation des données et de diffusion soient basés sur un serveur Web, supportent un client du type Web (fureteur) et s'intègrent au portail intranet du réseau ;

- que les mécanismes de sécurité logique du système d'information sur les ressources et les services utilisent le protocole LDAP et respectent la structure de rôles définie pour les services communs de sécurité ;
- que les infrastructures des systèmes d'information sur les ressources et les services soutiennent l'utilisation d'un protocole normalisé de gestion conforme à SNMP ou au CIM afin de pouvoir être gérées par les services communs d'exploitation ;
- que les communications avec d'autres applications utilisent les services communs d'échange électronique prévus dans les orientations technologiques (dont l'agent d'intégration multisystèmes et les contenus informationnels normalisés) ;
- que les échanges électroniques devant transiter par un réseau étendu utilisent le RTSS et en respectent les conditions d'intégration.

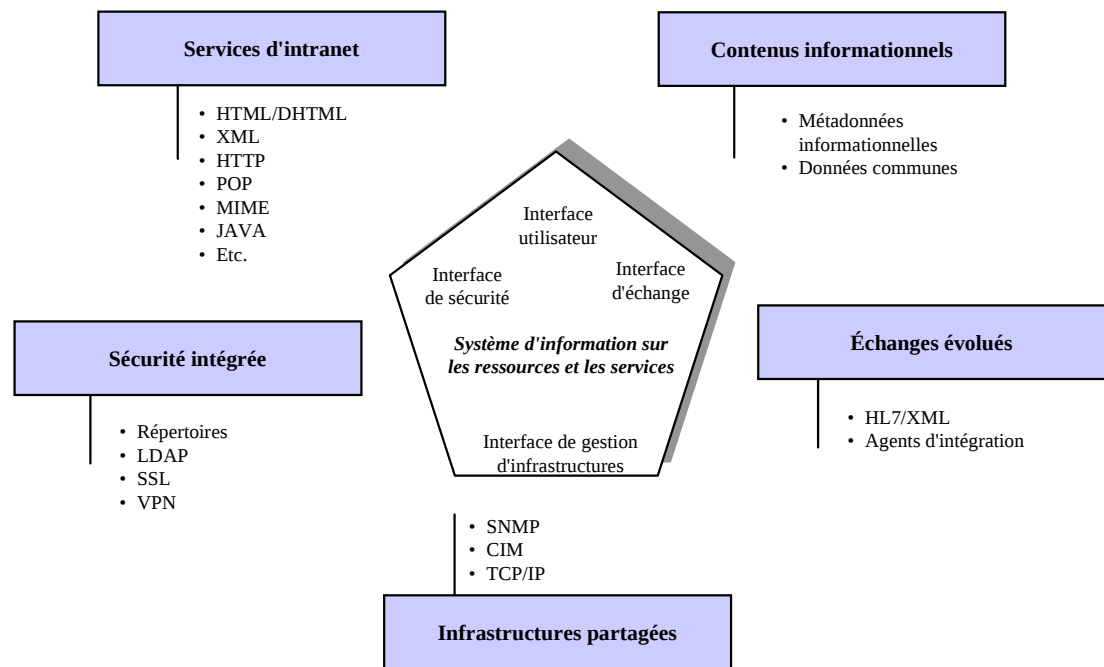
3.3.3 Perspectives conceptuelles

Les concepts et les modèles abordés dans la présente section sont complémentaires aux perspectives conceptuelles du modèle technologique de référence présenté au chapitre 2. Ils sont retenus comme orientations pour les systèmes d'information sur les ressources et les services en vue de la mise en place d'infrastructures technologiques et de services électroniques communs capables de les supporter. Une vue des services électroniques communs et une vue des infrastructures technologiques sont présentées ci-après.

Vue des services communs

Les concepts et les modèles de services communs définis dans le modèle technologique de référence au chapitre 2 permettent de soutenir la mise en œuvre des systèmes d'information sur les ressources et les services. Le diagramme 21 donne une vue d'ensemble des services communs et il indique, pour chaque classe de services, les concepts et les types de standards associés au soutien de ces systèmes.

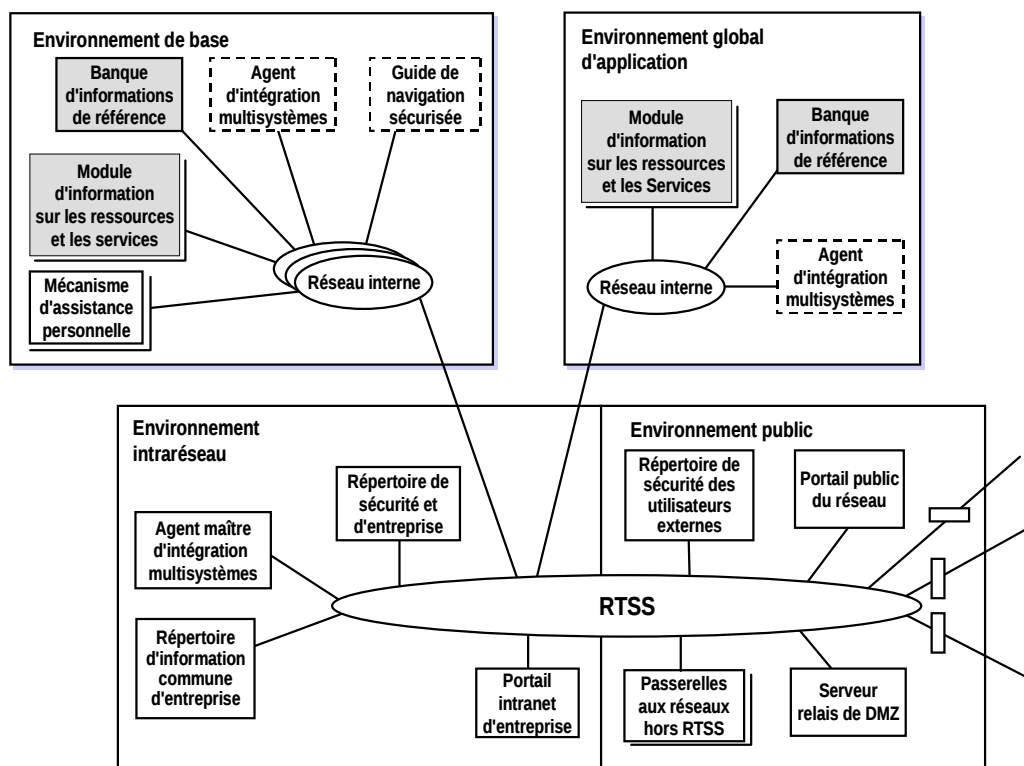
Diagramme 21 :
Vue des services communs pour les systèmes de type informationnel



Vue des infrastructures technologiques

La vue des infrastructures technologiques est illustrée par le diagramme 22. Elle est complémentaire à la vue de second niveau des infrastructures technologiques présentée dans le modèle technologique de référence du chapitre 2 et elle utilise le même symbolisme de représentation.

Diagramme 22 : Vue des infrastructures technologiques pour les services du type informationnel



Conformément aux principes directeurs énoncés dans la présente section concernant les systèmes d'information sur les ressources et les services, la vue des infrastructures fait apparaître une nouvelle composante dans les environnements de base et globaux : les banques d'informations de référence. Elle montre aussi un nouveau type d'application spécialisée, soit le module d'information sur les ressources et les services. Ces composantes technologiques se définissent comme suit.

- Banques d'information de référence :

Cette composante consiste en un ou plusieurs dépôts de données de référence, localisés dans l'environnement de base pour répondre aux besoins des systèmes et des utilisateurs d'un regroupement ou d'une communauté de pratique, ou localisé dans un environnement global d'application pour répondre aux besoins des systèmes et des utilisateurs d'un ensemble de regroupements ou de communautés de pratique. Une banque d'information de référence peut également être localisée dans un environnement de partenaire participant à la prestation de services et dans un environnement de services externes, bien que le diagramme n'illustre pas ces possibilités. Notons que le

répertoire d'information commune d'entreprise contient les paramètres que requiert la distribution des versions de banques d'information de référence.

- Module d'information sur les ressources et les services :

Cette composante consiste en des banques de données et des applications du type informationnel faisant appel à des technologies de type OLAP pour l'exploitation et l'analyse de données. Le module d'information sur les ressources et les services est caractérisé par :

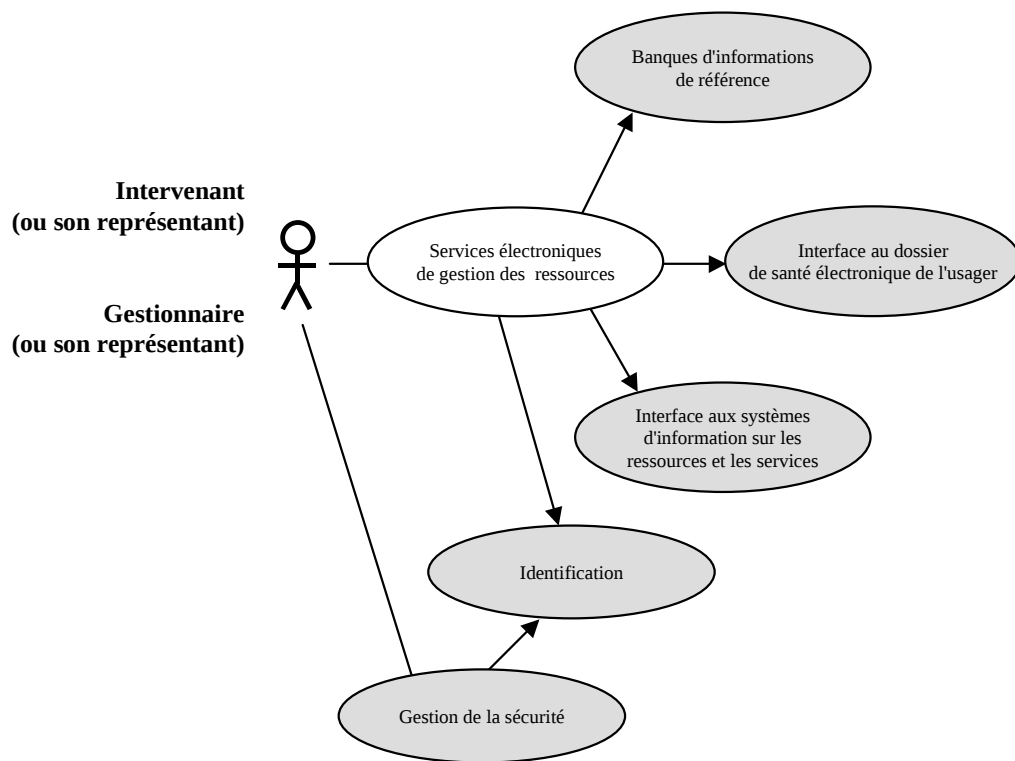
- l'utilisation de l'environnement de base ou global par les personnes autorisées ;
- une interface Web s'intégrant au guide de navigation sécurisée ;
- l'utilisation du protocole LDAP et des services communs de sécurité ;
- des infrastructures respectant les standards de gestion SNMP ou CIM et utilisant les protocoles de TCP/IP pour les télécommunications ;
- la capacité d'échanger sur la base de requêtes standard avec l'agent d'intégration.

3.4 Les orientations en matière de services électroniques de gestion des ressources

Les services électroniques de gestion des ressources renvoient aux systèmes administratifs qui soutiennent la gestion des ressources financières, humaines et matérielles. Ces systèmes incluent les progiciels du type ERP (Entreprise Ressource Planning) et les progiciels de gestion des approvisionnements.

Le diagramme 23 montre le contexte d'utilisation des systèmes de gestion des ressources.

Diagramme 23 :
Contexte d'utilisation des systèmes de gestion des ressources



Le diagramme 23 suppose que les systèmes de gestion des ressources sont principalement utilisés par les intervenants autorisés ou leurs représentants ainsi que par les gestionnaires autorisés ou leurs représentants (par exemple, un préposé, un commis ou un employé d'une autre catégorie de personnel). Ces systèmes utilisent :

- des banques d'informations de référence, soit des données de référence communes à l'ensemble des systèmes d'information (ex. : découpage territorial, CIM 10, centres d'activité) ainsi que des métadonnées informationnelles (produits documentaires, tels que les cadres normatifs, les dictionnaires de données et les classifications) ;
- une interface au dossier de santé électronique de l'utilisateur permettant des échanges électroniques, par exemple entre les données du dossier concernant la médication et le système d'approvisionnement en médicaments ;
- une interface aux systèmes d'information sur les ressources et les services permettant des échanges électroniques, comme LPRG pour les échanges avec SBF-R et Med-Echo local pour les échanges avec la banque globale de Med-Echo.

Le diagramme 23 illustre aussi le fait que l'accès aux systèmes de gestion de ressources doit être sécurisé sur la base de l'identification de l'utilisateur.

Cette section précise le contexte des systèmes de gestion de ressources et les orientations particulières retenues à cet égard pour le réseau socio-sanitaire québécois.

3.4.1 Éléments de contexte

Les systèmes de gestion de ressources utilisés par les organisations du réseau sont généralement des progiciels. Ces systèmes peuvent être :

- génériques, soit des solutions générales telles que des progiciels de grands fournisseurs dans ce domaine qui doivent être adaptées aux besoins des organisations du réseau socio-sanitaire ;
- dédiés, soit des solutions qui répondent aux besoins particuliers d'organisations du secteur socio-sanitaire. Le marché québécois compte plusieurs fournisseurs de progiciels dédiés.
- spécialisés, soit des solutions qui répondent à un besoin précis et pouvant interfacer avec des progiciels génériques ou dédiés de gestion de ressources. Les progiciels de gestion des approvisionnements sont représentatifs de cette catégorie de progiciels.

Les modes d'exploitation usuels des systèmes de gestion des ressources sont le mode « clé en main », ou mode local, et le mode ASP (Application Service Provider), ou mode partagé à distance.

Le mode « clé en main » consiste à installer les progiciels sur une infrastructure locale et à en assurer le soutien. Cette approche est largement répandue avec

plusieurs fournisseurs et plusieurs générations de produits, de sorte que les technologies sont diversifiées.

Le mode ASP consiste à installer les progiciels sur les infrastructures d'un fournisseur (nécessairement à l'extérieur du RTSS) qui vend ces mêmes services à plusieurs organisations afin de rentabiliser ses activités. Ce mode d'exploitation est largement répandu pour la paie des employés. Il est en croissance pour les progiciels financiers, de gestion de ressources humaines et de gestion de ressources matérielles.

En ce qui a trait aux systèmes d'approvisionnement, des projets d'utilisation de technologies Web ont été amorcés dans certaines régions. Les orientations relatives à ces projets consistent généralement en une mécanisation des processus d'approvisionnement déjà en place.

Tendances technologiques

Les principaux progiciels génériques offerts sur le marché comportent de nombreuses fonctions de gestion de ressources financières, humaines et matérielles. Ils sont offerts sous différentes plates-formes technologiques et permettent d'utiliser un client Web (fureteur). Les coûts d'acquisition et d'entretien de certains des progiciels les plus évolués sont souvent assez élevés, ce qui les rend moins accessibles aux organisations de plus petite taille.

Le mode d'exploitation ASP offre la possibilité de réduire les coûts d'acquisition et d'entretien en les partageant entre plusieurs organisations. Il permet également de partager les coûts d'exploitation. Comme les systèmes basés sur ces progiciels demandent le soutien de personnel spécialisé, le mode ASP a aussi pour effet de créer la concentration suffisante pour rentabiliser la présence continue de personnel de soutien.

La vague ASP basée sur les progiciels génériques est en progression, bien qu'elle semble connaître une popularité moindre que celle qui a été annoncée voilà un an ou deux. À l'examen, plusieurs projets permettent de constater les avantages de l'implantation de différents progiciels génériques, mais aussi les risques qu'elle comporte. Ceux-ci sont reliés à la gestion du changement (formation du personnel et adaptation des processus de travail au fonctionnement du progiciel, par exemple), à la confidentialité des informations qui sont conservées hors des locaux du propriétaire, aux coûts de personnalisation et à la facture totale, compte tenu des coûts élevés des progiciels, des infrastructures et des spécialistes nécessaires à l'entretien et à l'évolution du système.

En ce qui a trait aux nouvelles solutions de gestion d'approvisionnement du type commerce électronique, elles peuvent contribuer à accélérer le cycle d'acquisition par appel d'offres et à faire jouer la compétition plus souvent. Ces solutions connaissent du succès dans certaines industries à forte normalisation, par exemple

celle des produits électroniques. D'autres solutions s'intègrent à la gestion d'inventaire en s'appuyant sur des seuils pour automatiser les commandes de matériel ou de fournitures.

Principaux constats

En ce qui concerne les systèmes de gestion de ressources, les faits saillants et les tendances technologiques mettent surtout en évidence :

- une évolution vers l'utilisation de technologies Web, aussi bien pour les progiciels de gestion des ressources que pour les solutions d'approvisionnement ;
- la nécessité de déterminer des normes d'échanges électroniques d'information sur les ressources pour les interfaces avec les dossiers de santé électroniques des usagers, les données de référence et les systèmes d'information sur les ressources et les services. Dans les faits, les échanges de données financières sont normalisés par le système LPRG, mais cela ne suffit pas à permettre le suivi des coûts de revient. Par ailleurs, la normalisation est à établir pour les ressources humaines et matérielles ;
- la nécessité que les systèmes de gestion de ressources respectent des conditions d'intégration des applications au RTSS, particulièrement en ce qui concerne la sécurité. Les communications avec les fournisseurs de solutions de gestion de ressources ou d'approvisionnement en mode ASP (nécessairement à l'extérieur du RTSS) doivent être sécurisées, de même que l'environnement technologique des fournisseurs ;
- l'intérêt, dans l'utilisation de technologies de commerce en ligne, de tenir compte du marché hors Québec. Les traités de libre-échange et les autres accords économiques en vigueur, par exemple avec l'Ontario, doivent être respectés.

3.4.2 Principes directeurs pour les services électroniques de gestion des ressources

La définition des présentes orientations sur les services électroniques de gestion des ressources, présuppose que :

- sur le plan stratégique, de nouvelles avenues d'évolution doivent être considérées compte tenu des bénéfices potentiels qu'elles peuvent apporter, notamment en ce qui a trait aux possibilités :
 - d'étendre davantage le partage d'infrastructures et de progiciels en mode TCR à l'intérieur du réseau socio-sanitaire,

- de faire appel à des fournisseurs externes au réseau en mode ASP hors RTSS,
- de réviser les processus d'approvisionnements afin de tirer les meilleurs avantages du commerce électronique par Internet. À cet égard, un arrimage au projet de portail québécois de marchés publics doit être analysé;
- les interfaces aux dossiers de santé électroniques des usagers, aux données de référence et aux systèmes d'information sur les ressources et les services devront être alignées aux orientations stratégiques et aux orientations de l'architecture globale de l'information.

Les stratégies qui seront adoptées pour les systèmes de gestion des ressources dans le cadre des futurs travaux d'architecture d'information et de systèmes permettront de préciser davantage les orientations technologiques. Dans le contexte actuel, l'accent doit être mis sur l'arrimage des systèmes de gestion des ressources aux orientations technologiques générales. Cet arrimage doit faire en sorte :

- que les applications soient disponibles à partir d'un client du type Web (fureteur) et qu'elles s'intègrent au portail intranet du réseau, et qu'elles utilisent un agent d'intégration multisystèmes conforme aux orientations technologiques ;
- que les mécanismes de sécurité logique de l'application utilisent le protocole LDAP et respectent la structure de rôles définie pour les services communs de sécurité ;
- que les infrastructures du système de gestion de ressources soutiennent l'utilisation d'un protocole normalisé de gestion conforme à SNMP ou au CIM afin de pouvoir être gérées par les services communs d'exploitation ;
- que les communications avec d'autres applications utilisent les mécanismes d'échange électronique prévus dans les orientations technologiques (dont l'agent d'intégration multisystèmes et les contenus informationnels normalisés).

En ce qui a trait à l'utilisation d'une application en mode ASP chez un fournisseur externe au réseau de la santé et des services sociaux, les orientations de sécurité propres à ce type de services doivent être appliquées. Ces orientations, décrites plus en détail à la section 3.5 portant sur la sécurité, concernent les éléments suivants :

- l'utilisation d'une passerelle entre le RTSS et le réseau du fournisseur pour des échanges transactionnels performants lorsque ceux-ci atteignent un certain volume ;

- l'accès aux services du fournisseur par Internet lorsque les échanges sont sporadiques ;
- l'utilisation d'un VPN pour la transmission de données vers le RTSS à partir du système d'un fournisseur externe ;
- l'évitement de toute interconnexion directe par lien dédié ou par Internet entre le réseau interne d'une organisation reliée au RTSS et le réseau interne d'une organisation qui est à l'extérieur du RTSS.

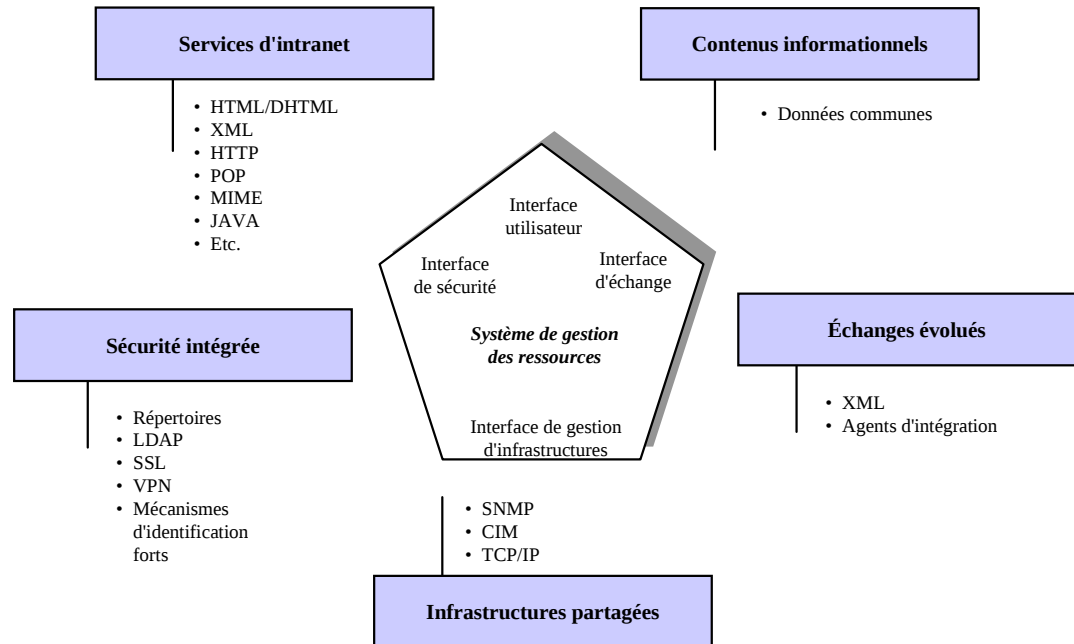
3.4.3 Perspectives conceptuelles

Les concepts et les modèles abordés dans la présente section sont complémentaires aux perspectives conceptuelles du modèle technologique de référence présenté au chapitre 2. Ils sont retenus comme orientations pour les systèmes de gestion des ressources en vue de la mise en place d'infrastructures technologiques et de services électroniques communs capables de les supporter. Une vue des services électroniques communs et une vue des infrastructures technologiques sont présentées ci-après.

Vue des services communs

Les concepts et les modèles de services communs définis dans le modèle technologique de référence présenté au chapitre 2 permettent de soutenir la mise en œuvre des systèmes de gestion des ressources. Le diagramme 24 rappelle la vue d'ensemble des services communs et il indique, pour chaque classe de services, les concepts et les types de standards associés au soutien de ces systèmes.

Diagramme 24 :
Vue des services communs pour les systèmes de gestion de ressources



Vue des infrastructures technologiques

La vue des infrastructures technologiques est illustrée par le diagramme 25. Elle est complémentaire à la vue de second niveau des infrastructures technologiques présentée dans le modèle technologique de référence du chapitre 2 et elle utilise le même symbolisme de représentation.

Conformément aux principes directeurs énoncés dans la présente section concernant les systèmes de gestion des ressources, la vue des infrastructures montre un nouveau type d'application spécialisée, soit les applications de gestion des ressources. Ces composantes technologiques se définissent comme suit.

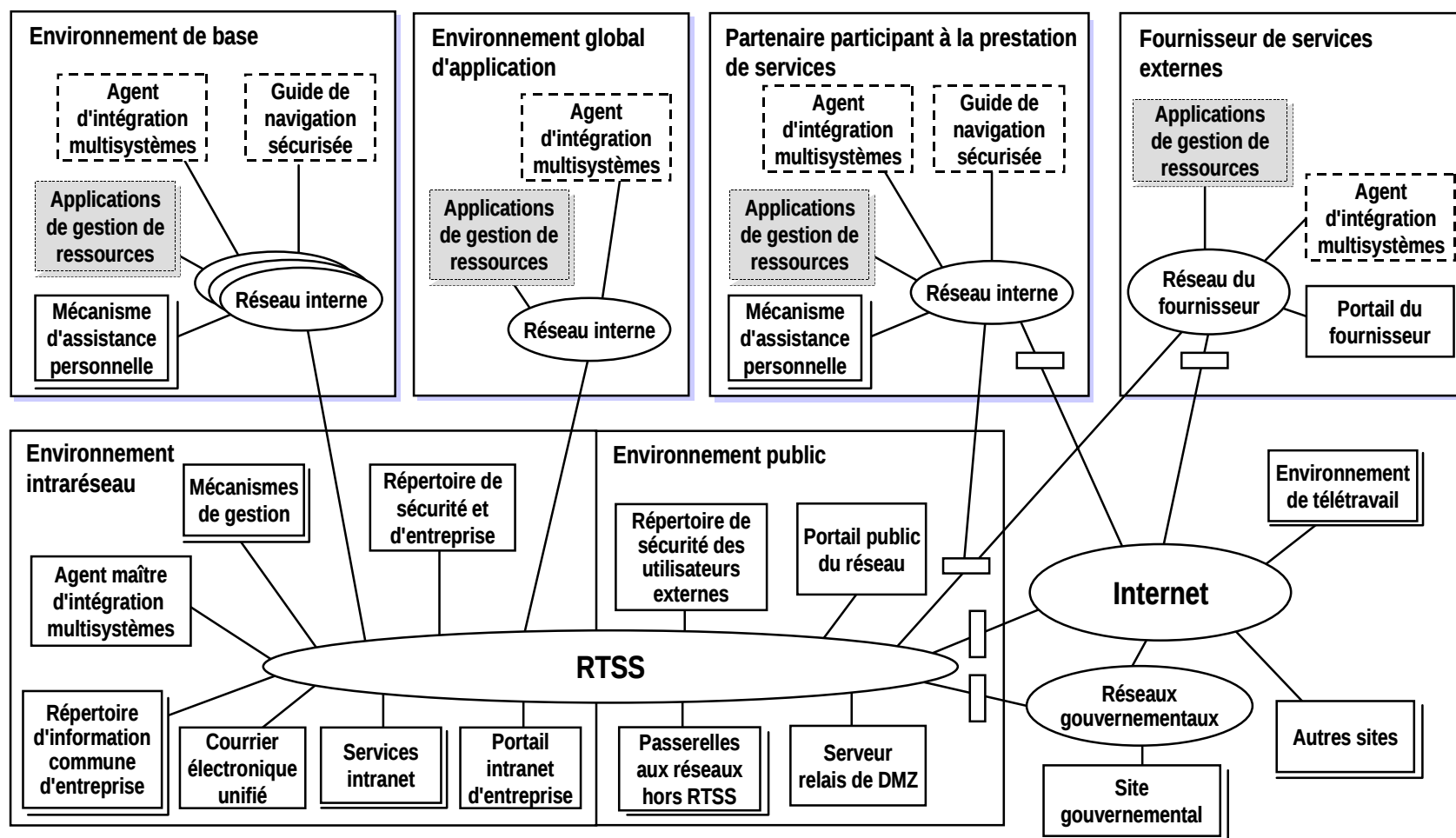
- Applications de gestion des ressources :

Ces applications, basées sur des progiciels de gestion des ressources, se caractérisent par :

- trois modes d'exploitation possibles soit un mode d'exploitation local, un mode de partage d'infrastructures et de progiciels en TCR, ou un mode ASP ;

- une interface Web s'intégrant au portail intranet par l'entremise du guide de navigation sécurisée ;
- l'utilisation du protocole LDAP et des services communs de sécurité ;
- des infrastructures respectant les standards de gestion SNMP ou CIM et utilisant les protocoles de TCP/IP pour les télécommunications ;
- la capacité d'échanger sur la base de requêtes standards avec un agent d'intégration tel qu'il est défini dans les orientations technologiques générales.

Diagramme 25 : Vue des infrastructures technologiques pour les services de gestion des ressources



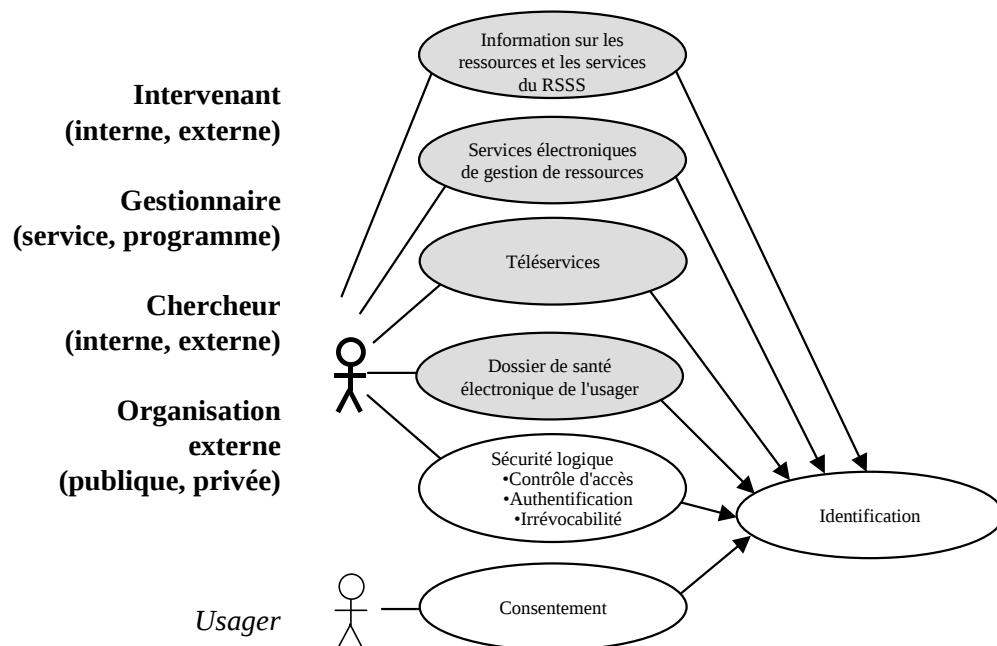
3.5 Les orientations en matière de sécurité et de passerelles d'échanges électroniques

L'importance de la sécurité a été soulignée tout au long des autres chapitres et sections des orientations technologiques. Au premier chapitre, la sécurité est mise en évidence comme un des grands domaines de gestion. Au second chapitre, les principes directeurs 4 et 9 couvrent les aspects légaux, la protection des renseignements personnels et la fiabilité des systèmes d'information. Le modèle technologique de référence fait aussi ressortir les besoins relatifs aux services communs et aux composantes technologiques de sécurité.

La présente section rassemble les orientations en matière de sécurité et les précise davantage. Elle couvre également les passerelles d'échanges électroniques du point de vue de la sécurité, car ces passerelles doivent assurer l'étanchéité du RTSS par rapport aux réseaux externes de télécommunications.

Le diagramme 26 montre le contexte d'utilisation des mécanismes de sécurité en relation avec les systèmes d'information.

Diagramme 26 : Contexte d'utilisation des fonctions de sécurité logique



Le diagramme 26 suppose que chaque utilisateur (intervenant, gestionnaire, chercheur, organisation externe) de systèmes doit s'identifier de façon non équivoque par des mécanismes de sécurité logique. Ces mécanismes permettent notamment de s'assurer de l'authenticité de l'utilisateur, de contrôler l'accès aux ressources selon les autorisations accordées à cet utilisateur, et de gérer l'irrévocabilité des transactions. Le diagramme montre aussi que chaque système, y compris les mécanismes de sécurité logique, fait appel à l'identification de l'utilisateur. En effet, la connaissance de l'identité de l'utilisateur est essentielle à la gestion de ses privilèges d'accès pour tous les systèmes.

Le diagramme illustre enfin que l'usager du réseau de services de santé et de services sociaux participe aux mécanismes de sécurité par le consentement à l'utilisation des informations qui le concernent.

Les présentes orientations portent particulièrement sur les aspects de sécurité logique, d'identification et de consentement selon un point de vue technologique. Les aspects organisationnels et administratifs concernant la sécurité des systèmes d'information relèvent donc d'autres travaux.

3.5.1 Éléments de contexte

Quelques faits saillants à l'échelle internationale et canadienne

En septembre 1998, Santé Canada publiait les résultats d'une enquête internationale en matière de dossiers médicaux électroniques. Cette enquête montre qu'en Europe, les dossiers conventionnels sur support papier sont encore la norme. Cependant, plusieurs projets de recherche et développement concernant les dossiers médicaux électroniques sont en cours, dont des projets se rapportant à l'identification des patients basée sur la technologie des cartes à mémoire.

À la Commission européenne, l'initiative EUROCARD a révélé que de nombreux pays envisagent de créer des cartes à mémoire pour leur système de soins de santé. Le Québec participe d'ailleurs au projet Netlink pour la définition des normes techniques sur les cartes à microprocesseur.

En France, le projet de cartes familiales VITALE 1 est aussi en cours. Ces cartes servent à contrôler l'accès à l'information et ne contiennent aucune donnée médicale. La phase suivante du projet prévoit la distribution de cartes personnelles VITALE 2 au plus tôt en 2003.

Dans la même enquête de Santé Canada, le volet sur les infrastructures à clés publiques (ICP) indique que les États-Unis, par l'entremise du National Institute of Standards and Technology (NIST), sont à déployer une ICP fédérale. Les travaux portent sur plusieurs questions importantes liées à la mise en œuvre de

l'ICP : l'architecture, l'interopérabilité, les besoins de sécurité des composantes d'ICP, les applications que rendraient possibles l'ICP et la mise en place d'une autorité de certification.

L'Union européenne a démarré, en 1996, le projet ISHTAR⁴⁵ (Implementing Secure Healthcare Telematics Applications in Europe). Ce projet est une initiative menée par douze pays pour la transmission protégée de renseignements médicaux. Les objectifs sont d'améliorer les normes de sécurité, de sensibiliser le public et de cerner les problèmes tant légaux que sociaux.

L'enquête de Santé Canada révèle aussi que plusieurs groupes de travail ont amorcé des projets de définition de politiques d'ICP, notamment en Suède, en Nouvelle-Zélande, en Australie et au Japon.

À l'échelle canadienne, le gouvernement fédéral et les provinces ont préconisé le concept d'infrastructure de la santé, qui vise à favoriser l'utilisation d'un dossier électronique de santé⁴⁶. Les moyens prévus consistent, entre autres, à mettre en place des mécanismes de sécurisation de l'information de santé par l'adoption de mesures législatives ou normatives. Un projet d'accord national sur les politiques d'ICP (National PKI Policy Accord) a été proposé. Par ailleurs, Santé Canada a publié un cadre de référence de l'ICP Santé (National PKI Framework for Health).

Quelques faits saillants à l'échelle québécoise concernant l'encadrement légal et réglementaire

Au Québec, le cadre législatif et réglementaire touchant la gestion de l'information comporte des dispositions générales qui s'appliquent à tous les secteurs d'activité ainsi que des dispositions particulières au secteur de la santé et des services sociaux. Les lois et règlements généraux comprennent :

- des lois fédérales (par exemple, la Loi uniforme sur la preuve électronique, la Loi uniforme sur le commerce électronique, la Loi sur les droits d'auteur, le chapitre 5 des Lois du Canada) ;
- des lois québécoises (par exemple, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, la Loi sur la fonction publique, la Loi sur les archives, la Charte de la langue française, la Loi concernant le cadre juridique des technologies de l'information) ;
- la directive du Secrétariat du Conseil du trésor (SCT) concernant la sécurité de l'information numérique et des échanges électroniques dans l'administration publique.

45. L'adresse électronique du projet est : <http://ted.see.plym.ac.uk/ishtar/overview.htm>

46. Voir le document intitulé *Vers les dossiers de santé électroniques*, Op. cit.

Quant aux lois et règlements plus particulières au secteur de la santé et des services sociaux, ils comprennent notamment :

- la Loi sur les services de santé et les services sociaux (LSSSS) ;
- les modifications à la LSSSS au regard de la gouvernance du réseau de la santé et des services sociaux ;
- la Loi sur l'assurance maladie ;
- la Loi sur la Régie de l'assurance maladie du Québec, modifiée en novembre 1999, qui permet à la RAMQ d'être dépositaire par entente de données sur les usagers ;
- les exigences minimales de la Commission d'accès à l'information du Québec (CAIQ) concernant la sécurité des dossiers informatisés des usagers ;
- les codes de déontologie régissant les différentes professions du domaine ;
- le cadre global de gestion sur la sécurité des actifs informationnels du réseau ;
- les mécanismes de certification du RTSS.

L'examen de ce cadre législatif et réglementaire fait ressortir plusieurs règles :

- les renseignements nominatifs détenus par un établissement ne peuvent être transmis à l'extérieur, sauf à la demande du ministre ou à la suite d'une entente particulière ;
- sauf exception, le partage d'information sur l'utilisateur est sujet à son consentement. L'utilisateur a en outre le droit d'être informé de la nature et du but de la collecte de renseignements personnels, de l'utilisation qui sera faite de ces renseignements ainsi que des catégories de personnes qui y auront accès ;
- l'utilisateur a le droit d'accéder aux renseignements personnels qui le concernent et de les faire rectifier.

Par ailleurs, plusieurs mesures relatives aux technologies sont déjà énoncées dans divers documents, dont les suivants :

- les *Exigences de la CAIQ concernant les dossiers des usagers du réseau* ;
- les mesures du *Cadre global de gestion sur la sécurité des actifs informationnels du réseau* ;
- les *Conditions d'intégration des applications au RTSS* ainsi que les *Exigences minimales pour le raccordement au RTSS*.

Le contexte légal et réglementaire est en évolution, autant dans le secteur de la santé et des services sociaux que dans l'ensemble du gouvernement, et il est susceptible de changer à court ou moyen terme compte tenu des divers travaux en cours :

- ceux qui sont réalisés par le Ministère en relation avec différents projets de systèmes d'information ;
- le projet de loi relatif à la carte accès santé Québec ;
- le projet d'architecture gouvernementale de la sécurité de l'information numérique et des échanges électroniques (AGSIN) découlant de l'Architecture d'entreprise gouvernementale et du modèle de prestations des services électroniques ;
- les différents projets d'infrastructures à clés publiques (ICP) dans certaines applications gouvernementales au ministère de la Justice, à la CSST et au ministère du Conseil exécutif.

Éléments de contexte organisationnel particuliers au réseau de la santé et des services sociaux

L'organisation actuelle de la gestion de la sécurité est définie par le *Cadre global de gestion sur la sécurité des actifs informationnels du réseau*. Ce cadre énonce les rôles et les responsabilités du Ministère, des régies régionales, des établissements et de la RAMQ. Ces rôles et responsabilités se résument comme suit.

Le Ministère a une responsabilité d'encadrement général. Il définit les orientations, les stratégies et les politiques en matière de technologie de l'information, ce qui inclut la sécurité et la protection des renseignements personnels. Les principales instances de gestion sont un responsable de la sécurité des actifs informationnels du réseau, le Comité national sur la protection des renseignements personnels et sur la sécurité (CNPRPS) ainsi que le Bureau d'accueil des applications et son centre de certification.

Les régies régionales sont responsables de l'actualisation régionale des orientations, des stratégies et des politiques nationales en technologie de l'information, dont celles qui ont trait à la sécurité. Un responsable régional de la sécurité est nommé au sein de chacune des régies.

Quant à l'établissement, il est responsable de l'application des divers cadres de gestion en technologie de l'information, ce qui inclut la sécurité. Cette responsabilité est assumée par le conseil d'administration, les dirigeants et le responsable de la sécurité des actifs informationnels de l'établissement.

En vertu de l'article 2 de la Loi sur la Régie de l'assurance maladie telle qu'elle a été modifiée en novembre 1999, la RAMQ peut recevoir en dépôt des données provenant du réseau de la santé et des services sociaux qui lui sont confiées par entente et assurer la gestion sécuritaire. À cet égard, elle applique les dispositions dévolues par le ministre en matière de sécurité, en collaboration avec le responsable ministériel de la sécurité de l'information du réseau et en concertation avec les partenaires visés. Elle doit tant assurer la mise en place de services permettant un accès sélectif et fiable aux dépôts provinciaux des données sociosanitaires que garantir la transmission sécuritaire des données nécessaires aux usagers, aux professionnels et aux organismes du réseau sociosanitaire.

Une structure organisationnelle de gestion de la sécurité du RTSS a aussi été mise en place. Cette structure regroupe le Ministère, la Sogique, les technocentres national et régionaux ainsi que le GTQ.

Aperçu sommaire des mécanismes de gestion en place

L'article 520.4 de la Loi sur les services de santé et les services sociaux oblige toute organisation du réseau à utiliser les services du fournisseur retenu pour les télécommunications. Les services de télécommunications⁴⁷ sont donc assurés par le RTSS pour l'ensemble des organisations du réseau de la santé et des services sociaux. Le RTSS offre les services d'échanges électroniques internes au réseau sociosanitaire ainsi que les services de communications avec les réseaux et les organisations externes.

La sécurité des échanges est assurée par les mécanismes du RTSS. Ceux-ci comprennent notamment des passerelles d'échanges électroniques, dont celles qui sont déjà en place pour les accès à Internet, à la CSST et au RISQ. D'autres sont à venir, notamment avec le RICIB ou le RETEM.

L'accès à des données sensibles à partir d'un point à l'extérieur du RTSS requiert l'utilisation d'une identification forte. Les mécanismes de protection consistent en une DMZ pour la sécurisation des accès au RTSS, combinée à l'un ou l'autre des moyens suivants :

- un VPN (réseau virtuel privé) sans jeton électronique ;
- un VPN avec jeton électronique ;
- l'utilisation d'un lien SSL.

La DMZ comprend un serveur relais qui empêche de se relier directement à un des serveurs du RTSS. Elle masque donc les adresses internes du RTSS pour un usager de l'extérieur. Le Ministère, la RAMQ et le CHUM ont leurs propres mécanismes d'isolement en plus de la DMZ du RTSS.

47. C'est-à-dire les télécommunications de données numériques, à l'exclusion des communications téléphoniques.

En ce qui a trait aux services fonctionnant sous Lotus Notes, tels que le courrier électronique et les forums, les mécanismes standard de Notes (actuellement, la version 4.6), soit des mécanismes d'ICP, de signature électronique et de cryptage, peuvent être utilisés.

Certaines applications actuellement en exploitation utilisent des mécanismes de sécurisation spécialisés. L'application Intégration-CLSC fait appel à un tunnel IPSec point à point tandis que SI-PRSA utilise une carte d'intervenant et une carte d'utilisateur couplées à une banque de données anonyme.

Actuellement, la gestion du consentement des usagers à l'utilisation des informations qui les concernent s'effectue à l'aide de formulaires sur support papier.

Par ailleurs, plusieurs projets et concepts comportant des considérations importantes de sécurité sont actuellement en cours d'étude ou de réalisation, dont le projet de la carte accès santé, le projet du Réseau mère-enfant (application des concepts IPP et DPP), le Portail santé du réseau sociosanitaire, le raccordement de groupes de médecine de famille (GMF) et l'accès par les partenaires participant à la dispensation des services à des données classifiées comme sensibles sur le plan de la sécurité. Enfin, des projets de systèmes de gestion des ressources en mode ASP externe au RTSS posent aussi des défis de sécurité importants.

Tendances technologiques

L'évolution en matière de sécurité des systèmes d'information touche aussi bien les pratiques de gestion que les technologies elles-mêmes.

En ce qui a trait aux pratiques de gestion, l'encadrement se formalise généralement sous forme de politiques et de règles de sécurité. Ces politiques et ces règles traitent le plus souvent :

- de responsabilisation des utilisateurs (là où se trouvent les plus grands risques pour la sécurité) ;
- d'imposition de sanctions en cas de manquement à la politique et aux règles ;
- d'intégration des règles aux mécanismes informatiques de sécurité ;
- de classification des informations selon leur sensibilité.

La couverture des aspects de sécurité tend à s'améliorer car les organisations, souvent alertées par la publicisation d'événements tels que la propagation de virus sur le Web, sont maintenant plus vigilantes. Les organisations gouvernementales, plus particulièrement, réalisent une meilleure couverture des aspects de sécurité en appliquant les principes de disponibilité, d'intégrité, de confidentialité, d'authentification et d'irrévocabilité (DICA) préconisés par la directive du SCT

concernant la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale.

Le SCT a également élaboré le modèle général de l'AGSIN⁴⁸ qui propose une vision commune en matière de sécurité au sein de l'appareil gouvernemental québécois, en relation avec des secteurs tels que celui de la santé et des services sociaux. Ce modèle s'appuie sur le concept de domaine de confiance. Les *domaines de confiance* (DC)⁴⁹ sont définis et encadrés en tenant compte des dimensions juridique, humaine, organisationnelle et technologique. Les échanges entre les domaines de confiance se réalisent au moyen d'*interfaces sécuritaires* (IS)⁵⁰ qui sont encadrées par des *ententes* (E)⁵¹ entre les domaines de confiance. Les interfaces sécuritaires sont constituées de règles, de normes, de procédures et de mécanismes de sécurité permettant d'accomplir les différentes fonctions nécessaires à la sécurisation de l'information (sur la base du modèle DICA). Quant aux ententes, elles constituent des cadres de gestion définissant les responsabilités de chaque domaine de confiance.

En pratique, l'accent est mis actuellement sur les aspects d'intégrité et de confidentialité, et ce, aussi bien dans le marché qu'au gouvernement. L'autorisation sous forme de listes de contrôle d'accès et des algorithmes de cryptage sont les mécanismes les plus utilisés. Au regard de l'authentification, l'ICP et les mécanismes de gestion des clés suscitent un fort intérêt. Finalement, la signature électronique et la biométrie retiennent l'attention en ce qui a trait aux questions d'intégrité et d'irrévocabilité.

L'identification consolidée (Single Sign-On) et la gestion des accès en fonction des rôles sont des concepts qui se répandent de plus en plus. Les contrôles d'accès sont effectués grâce à la combinaison des approches serveurs (hosts) et réseau. Aux processus opérationnels courants de gestion de la sécurité sont aussi ajoutés des mécanismes de détection d'intrusions et d'analyse des vulnérabilités. La consolidation et l'analyse des journaux de sécurité, de même que des exercices d'infiltration, sont effectués régulièrement.

Sur le plan organisationnel, un clivage est observé entre les tâches associées à la sécurité et la gestion des technologies. La gestion d'ensemble de la sécurité de l'information, la gestion opérationnelle de la sécurité et la vérification sont réalisées distinctement, et souvent par des responsables qui ne relèvent pas des services de gestion des technologies de l'information.

48. Selon un document de travail du projet d'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN) daté du 16 mai 2001.

49. Voir le lexique pour la définition proposée dans le document de l'AGSIN.

50. Voir le lexique pour la définition proposée dans le document de l'AGSIN.

51. Voir le lexique pour la définition proposée dans le document de l'AGSIN.

La sécurité des systèmes d'information est progressivement reconnue comme une discipline à part entière possédant ses pratiques, ses technologies particulières et ses spécialistes.

Sur le plan technologique, le diagramme 27, tiré d'un document de travail de l'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN), fournit une bonne synthèse des principales tendances technologiques en matière de sécurité. Il présente les grandes fonctions de sécurité, les principaux mécanismes qui permettent de les implanter et les composantes technologiques qui soutiennent ces mécanismes. Le marché des technologies de l'information offre différentes solutions pour la plupart des fonctions, mécanismes et composantes illustrés dans le diagramme. Plusieurs de ces solutions de sécurité sont déjà largement utilisées, comme le protocole SSL, le chiffrement à 128 bits, les VPN, les coupe-feu et les listes d'accès. D'autres, comme le répertoire et l'ICP, sont en évolution rapide et constante, de sorte que les chefs de file à long terme ne sont pas encore connus.

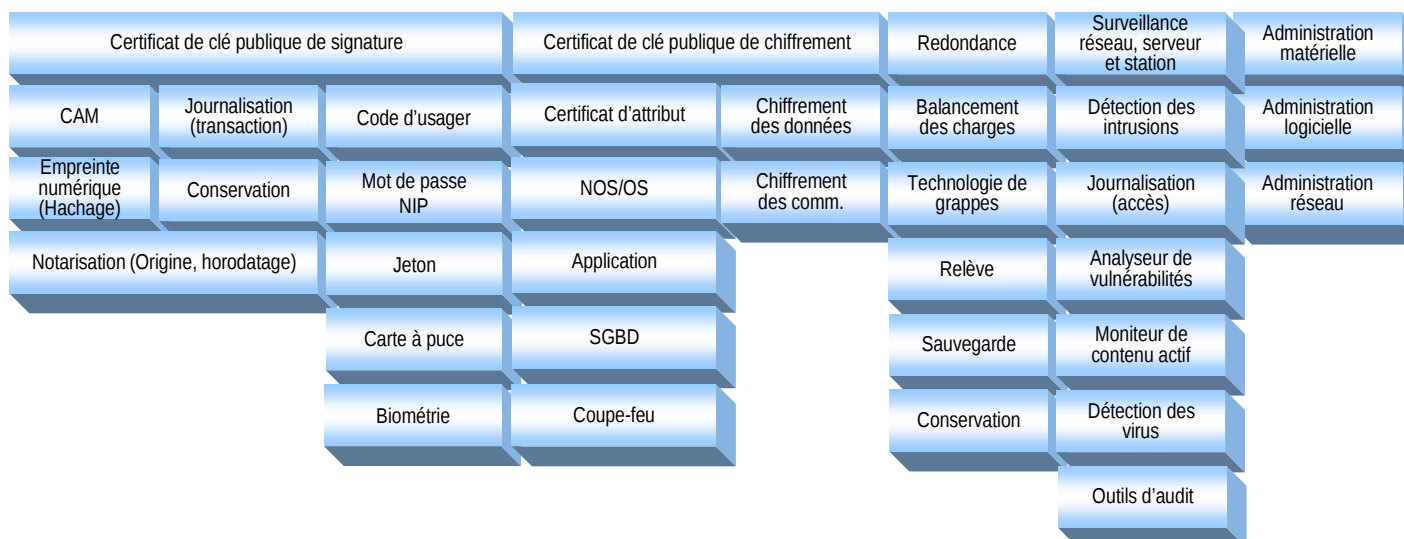
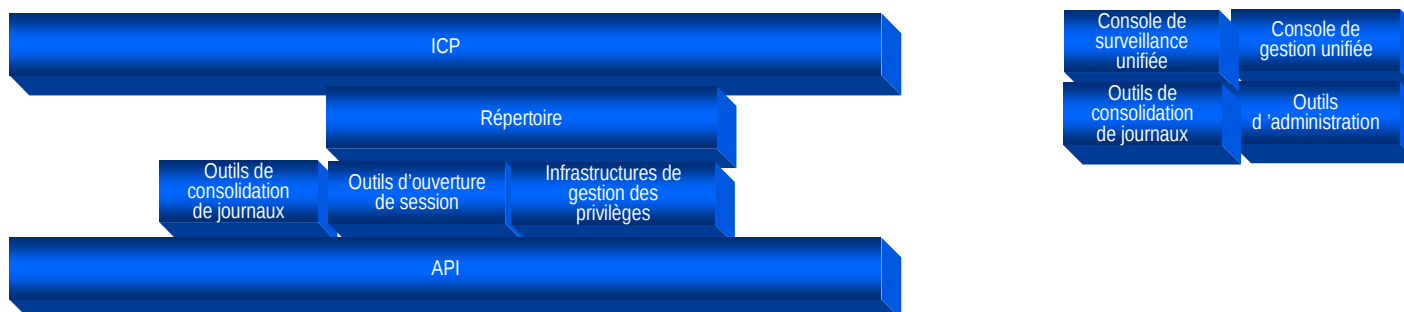
De façon sommaire, les tendances d'évolution en sécurité des systèmes d'information touchent la normalisation, les répertoires d'entreprise, les infrastructures à clé publique (ICP), la biométrie numérique, les techniques d'identification, la sécurisation des accès Web et les réseaux privés virtuels (VPN).

En ce qui a trait à la normalisation se dégagent les observations suivantes :

- les principaux manufacturiers supportent le protocole LDAP qui est une version allégée et compatible à X.500 ;
- la majorité des répertoires (ou annuaires) sont également compatibles aux certificats X.509, et certains supportent plus complètement la norme de répertoire X.500 ;
- le protocole SSL est utilisé par la majorité des sites Web pour sécuriser les communications ;
- une nouvelle version du protocole IPSec est annoncée à court terme ;
- de nombreux algorithmes de chiffrement sont normalisés, tels que DES-CBC, 3-DES, RSA, DSA, RC2, RC5, CAST et AES, et le chiffrement à 128 bits est maintenant le minimum requis⁵² ;
- de nombreux algorithmes standards de hachage pour les empreintes numériques sont offerts tels que MD5, SHA-1, HMAC-MD5 et HMAC-SHA-1.

52. En particulier depuis qu'Electronic Frontier Foundation a produit un appareil qui met moins de 4 heures à décoder les chiffrements à 56 bits.

Pour ce qui est des répertoires d'entreprise, l'illustration fait ressortir le répertoire comme une des principales solutions technologiques qui soutiennent les mécanismes et les fonctions de sécurité logique (identification et authentification, habilitation et contrôle d'accès). En effet, le répertoire est essentiel au fonctionnement des outils de sécurité logique et de l'ICP. Bien qu'il ne soit pas illustré dans le diagramme 27, il est également une composante de base pour la console de gestion unifiée et les outils d'administration. Plusieurs produits sont offerts par des fournisseurs. Le protocole LDAP est généralisé pour l'accès aux répertoires des différents fournisseurs.

Diagramme 27 : Fonctions de sécurité⁵³**Fonctions****Principaux
mécanismes****Principales
composantes et
solutions
technologiques**

53. Diagramme tiré d'un document de travail du projet d'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN) daté du 16 mai 2001.

En ce qui concerne l'ICP, elle constitue une technologie encore nouvelle. Elle est la seule technologie courante qui permet la signature électronique. Des ICP sont utilisées actuellement dans certaines applications gouvernementales. Pour chacune de ces applications, le nombre d'utilisateurs possédant un certificat est limité à quelques centaines.

Des technologies de biométrie numérique peuvent être utilisées en complément des mécanismes d'identification pour assurer l'authenticité de l'utilisateur. Toutefois, elles soulèvent des questions légales, éthiques, économiques et technologiques, de sorte que leur usage généralisé n'est pas prévisible à court terme.

Le jeton électronique et le certificat (utilisé avec une carte à puce ou non) sont des moyens pour renforcer l'identification. Une photographie ou un autre indice biométrique jumelé à une carte à puce permet de rendre l'identification encore plus forte.

Des technologies de sécurisation sont actuellement d'usage courant avec les technologies du Web. Le protocole SSL est très répandu, par exemple pour les sites qui permettent des transactions financières. L'utilisation de SSL est peu onéreuse, mais son usage est généralement limité aux applications disponibles par un fureteur. Les technologies de réseau virtuel privé (VPN) permettent d'éliminer cette contrainte à un coût abordable. Le VPN, souvent basé sur le protocole IPSec et, de plus en plus utilisé en point à point, permet un accès élargi aux applications Web et non Web.

Le SSL et le VPN doivent être associés à un mécanisme d'identification, tel qu'un code d'utilisateur et un mot de passe. Le VPN est aussi utilisé avec un mécanisme d'identification plus fort, tel qu'un jeton électronique ou une carte à puce.

D'autres technologies de sécurisation sont offertes. Par exemple, les SGBD intègrent des mécanismes de sécurisation des données. Des analyseurs/vérificateurs de code peuvent permettre un contrôle des programmes informatiques avant leur implantation. Le balancement de charge entre serveurs, la redondance de composantes, les copies de sécurité, les batteries de secours et les génératrices sont des éléments régulièrement utilisés pour assurer la continuité opérationnelle des systèmes. Les réseaux, quant à eux, font appel aux technologies de coupe-feu pour gérer les accès et prévenir certaines attaques. Des coupe-feu personnels permettent aussi la sécurisation des postes de travail.

Principaux constats

Les éléments de contexte décrits jusqu'à présent permettent de formuler les constats qui suivent relativement aux aspects légaux et administratifs :

- la nécessité de respecter les lois, les règlements et l'éthique impose des mécanismes, des services et des infrastructures de sécurité adéquats qui sont, pour plusieurs, déjà en place ;
- à court terme, l'utilisation de documents sur support électronique se heurte à plusieurs restrictions légales. Le projet de loi concernant la carte accès santé et la loi concernant le cadre juridique des technologies de l'information peuvent apporter des changements importants à cette situation. Par ailleurs, à plus long terme, l'évolution sur les plans international et national est de plus en plus favorable à la reconnaissance légale de documents sur support électronique ;
- des orientations administratives relatives à la sécurité doivent être définies, notamment en ce qui concerne :
 - la gestion du consentement de l'utilisateur aux diverses utilisations des informations personnelles de son dossier,
 - les dossiers de santé électroniques des usagers,
 - les transactions avec signature électronique effectuées aussi bien par les intervenants que par les usagers ;
- bien que plusieurs éléments d'architecture de sécurité soient déjà définis (par exemple, le cadre de gestion et les exigences pour le RTSS), une architecture globale peut être conçue. Cette architecture doit :
 - s'appuyer sur les principes du *Cadre global de gestion sur la sécurité des actifs informationnels du réseau*, et en particulier sur le modèle DICA, I,
 - tenir compte de l'architecture globale de l'information du réseau socio-sanitaire,
 - tenir compte des orientations administratives à définir,
 - être cohérent avec les orientations technologiques du réseau,
 - s'appuyer sur l'Architecture gouvernementale de sécurité (AGSIN),
 - définir les règles de classification de l'information quant à la sensibilité en matière de sécurité,
 - tenir compte des principes, des mesures et des règles de sécurité en relation avec le cycle de vie de l'information (création, emmagasinage, traitement, échange, archivage, disposition),
 - permettre de consolider l'ensemble des mesures et des règles de sécurité sur les plans administratif, organisationnel et technologique.

Pour ce qui est des aspects de nature technologique, les principaux constats sont les suivants :

- une DMZ utilisant des coupe-feu, un serveur relais, des VPN et un répertoire spécifique de sécurité protègent déjà les accès au RTSS ;
- des passerelles d'échange sont en place tant pour les accès Internet que pour les échanges avec la CSST et le RISQ, et d'autres sont prévues avec entre autres le RICIB ou la RETEM ;
- les mécanismes actuels de sécurité sont diversifiés et utilisent différentes technologies pour le cryptage et les répertoires ;
- les risques liés à l'utilisation de systèmes en mode ASP hors RTSS doivent être gérés, ce qui demande une sécurisation des échanges électroniques avec les fournisseurs, aussi bien sur le plan administratif que sur le plan technologique.

3.5.2 *Principes directeurs en matière de sécurité et de passerelles d'échanges électroniques*

La définition des orientations technologiques en matière de sécurité et de passerelles d'échanges électroniques s'appuie sur la présupposition voulant que des actions viennent encadrer davantage la gestion de la sécurité des systèmes et de la protection des renseignements personnels.

Ces actions comprennent d'abord la réalisation d'une architecture globale de sécurité. Cette architecture de sécurité permettra notamment de préciser davantage les composantes technologiques nécessaires pour soutenir les différentes fonctions de gestion de la sécurité. Elle devra s'appuyer sur les principes de l'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN) et définira les interfaces sécuritaires ainsi que les ententes⁵⁴ entre les domaines de confiance. L'architecture de sécurité tiendra également compte des travaux de l'architecture globale de l'information du réseau socio-sanitaire et des orientations retenues pour les projets ayant des conséquences majeures en matière de sécurité, dont le projet de la carte accès santé.

En outre, les éléments suivants devront être prévus dans le cadre global de gestion de la sécurité des actifs informationnels du réseau :

- la définition des domaines de confiance s'appliquant aux organisations du réseau et aux organisations hors réseau ;
- un mécanisme de soutien à l'intégration architecturale de sécurité des projets, en particulier en ce qui a trait à la complémentarité des projets et des concepts

54. Les concepts d'interface sécuritaire et d'entente sont définis dans l'AGSIN.

majeurs tels que l'IPP, le DPP, la carte accès santé et le portail santé du réseau ;

- un processus de certification des applications couvrant l'ensemble des exigences de sécurité qui découlent :
 - du *Cadre global de gestion sur la sécurité des actifs informationnels du réseau*,
 - des *Orientations technologiques du réseau sociosanitaire*,
 - de l'architecture de sécurité du réseau sociosanitaire⁵⁵ ;
 - des *Conditions d'intégration des applications au RTSS*⁵⁶ ;
- un mécanisme pour faire évoluer l'architecture de sécurité et pour en assurer l'actualisation dans les processus de gestion de la sécurité, y compris la certification.

Bien que l'encadrement administratif en matière de sécurité soit sujet à évolution, les constats sur la situation actuelle et les tendances technologiques en matière de sécurité permettent d'énoncer des orientations sur le plan technologique. Ces orientations mettent l'accent d'une part, sur la mise en place de services communs de sécurité et, d'autre part, sur les principes directeurs que devront respecter les interfaces sécuritaires entre les domaines de confiance et les ententes qui les encadrent.

Les fonctions de sécurité à implanter dans les organisations du réseau sociosanitaire se regroupent sous les volets de gestion suivants :

- la gestion des accès, c'est-à-dire l'identification, l'authentification, l'autorisation (ou habilitation) et le contrôle de l'accès;
- la gestion de la disponibilité ;
- la gestion de l'intégrité et de l'irrévocabilité ;
- la gestion de la confidentialité ;
- l'administration et la surveillance des mécanismes de gestion de la sécurité.

Chacune de ces fonctions implique des mécanismes de sécurité particuliers. Le choix de ces mécanismes est fortement lié à trois facteurs, soit la classification des données (en fonction de leur valeur pour le réseau), l'évaluation des risques

55. Cette architecture devra contenir l'ensemble des mesures et des règles de sécurité sur les plans administratif, organisationnel et technologique.

56. Précisant les mesures et les règles de sécurité tant que conditions à respecter et s'intégrant au formulaire d'enregistrement du Bureau d'accueil des applications du Ministère.

associés à la sécurité de ces données et les ressources dont disposent les organisations définissant les domaines de confiance.

Compte tenu des besoins d'interopérabilité, d'économie et de normalisation de la sécurité dans le réseau de la santé et des services sociaux, certaines fonctions doivent être assurées par des mécanismes communs, des normes communes et un cadre de gestion commun.

Pour la **gestion des accès**, la mise en place d'une infrastructure de répertoires soutenant la gestion de la sécurité est retenue et peut être entreprise rapidement afin d'alimenter les travaux relatifs à l'architecture de sécurité du réseau sociosanitaire. De plus, la mise en place à court terme d'une infrastructure de répertoires harmonisés de sécurité permet d'assurer la généralisation de l'usage de **services communs** de sécurité et de constituer une assise permettant de prendre en compte l'évolution future.

L'infrastructure de répertoires de sécurité recommandée se fonde sur l'orientation d'un répertoire intégré alimenté par une fonction de pilotage décentralisée de la sécurité correspondant à la structure organisationnelle définie dans le *Cadre global de gestion sur la sécurité des actifs informationnels du réseau*. L'infrastructure comprend un répertoire d'entreprise ayant un volet intranet et un volet public distincts ainsi que des répertoires communautaires ou de groupe. Plus particulièrement, cette infrastructure de répertoires harmonisés doit permettre :

- de soutenir une structure de rôles qui réponde aux besoins immédiats tout en considérant les besoins prévisibles ;
- de gérer les privilèges d'accès aux applications ;
- de couvrir les fonctions et mécanismes suivants :
 - l'identification et l'authentification des utilisateurs,
 - l'identification et l'authentification des applications participant à des échanges électroniques par réseau étendu de télécommunications,
 - l'autorisation d'accès aux serveurs, aux services communs et aux applications.

Chaque répertoire supporte le protocole LDAP. Les produits et services seront choisis en considération des principes généraux des orientations technologiques.

Pour la **gestion de la disponibilité**, les interfaces sécuritaires mises en place entre les domaines de confiance à l'interne dans le réseau ou avec ses interlocuteurs externes doivent être fonctionnelles et disponibles en tout temps. Aussi, des mesures doivent être prises afin d'assurer la haute disponibilité des différents répertoires, et conséquemment celle des différentes composantes technologiques

qui soutiennent les interfaces sécuritaires, telles que le RTSS et les passerelles de communication. Cela implique également la mise en place d'un plan de relève pour les infrastructures critiques.

Pour la **gestion de l'intégrité et de l'irrévocabilité**, dans la mesure où cette fonction devient nécessaire notamment à cause du nouveau cadre juridique des technologies de l'information, des mécanismes du type ICP seraient alors des services communs de sécurité à définir et à déployer. Différents travaux portent actuellement sur cette question. C'est par exemple le cas avec le projet de la carte accès santé, qui prévoit une carte à microprocesseur intégrant les certificats nécessaires au détenteur de la carte. Ces travaux sont reliés à ceux du Secrétariat du Conseil du trésor à l'égard de l'infrastructure à clés publiques gouvernementale (ICPG). L'intégration de la signature électronique est également possible par l'utilisation de ces mécanismes. Les décisions concernant l'utilisation de ces services devront tenir compte des orientations de l'architecture globale de sécurité du réseau sociosanitaire.

Pour la **gestion de la confidentialité**, le chiffrement des échanges électroniques entre les domaines de confiance peut être nécessaire. Les protocoles recommandés sont alors SSL pour les échanges avec internet et IPSec pour la mise en place de VPN entre les domaines de confiance.

Enfin, pour l'**administration et la surveillance** des mécanismes de gestion de sécurité, différents mécanismes devront être prévus, tels que la journalisation des accès aux services communs de sécurité et la détection d'intrusion dans les infrastructures des interfaces sécuritaires (c'est-à-dire logiciels, matériels et télécommunications). Ces mécanismes pourront profiter également des services communs de gestion des infrastructures de l'environnement intraréseau (définis à la section 2.2.3) pour assurer ces fonctions de gestion.

Principes directeurs à l'égard des interfaces sécuritaires et des ententes

Les interfaces sécuritaires requis dans le réseau sociosanitaire portent sur les échanges internes entre les organisations du réseau sociosanitaire et sur les échanges avec d'autres organisations qui sont à l'extérieur du RTSS.

Échanges internes

Les échanges internes entre les organisations du réseau sociosanitaire utilisent les services de télécommunications et les services communs rendus disponibles par l'**environnement intraréseau** (défini à la section 2.2.3).

De façon générale, les orientations de sécurisation pour les échanges internes sont les suivantes :

- décentraliser la gestion des privilèges d'accès vers les établissements et les organisations du réseau, et assurer l'alimentation dynamique du répertoire d'entreprise géré dans l'environnement intraréseau ;
- permettre la création dynamique de regroupements (ou de domaines de confiance) ciblés en fonction de problématiques ou de secteurs d'activité, grâce à la mise en place d'une architecture de réseau IP VPN sécurisée (voir la section 3.6.3).

L'architecture de sécurité du réseau sociosanitaire permettra de compléter ces orientations pour les échanges internes, en particulier en ce qui a trait aux mécanismes d'authentification, à l'utilisation éventuelle d'une ICP et à l'harmonisation avec les orientations du projet de la carte accès santé.

Échanges externes au RTSS

Les échanges avec des organisations externes au réseau sociosanitaire utilisent les services de télécommunications et les services communs rendus disponibles par *l'environnement public* tel qu'il est défini à la section 2.2.3.

De façon générale, les orientations de sécurisation pour les échanges externes au RTSS sont les suivantes :

- utiliser des passerelles sécurisées pour les communications ;
- utiliser la DMZ du RTSS pour tous les accès aux applications internes du réseau sociosanitaire ;
- recourir à un mécanisme d'identification et d'authentification forte⁵⁷ dans les cas d'accès à des données cliniques ou confidentielles ;
- recourir à un mécanisme de chiffrement pour les utilisateurs accédant au RTSS à partir d'Internet ;
- gérer la sécurité d'accès à l'aide de l'infrastructure de répertoires harmonisés publique et intraréseau ;
- s'assurer que les systèmes hors RTSS utilisés par les organisations du réseau respectent les consignes de sécurité retenues :

57. Manière de s'identifier dans le cadre d'une session d'échange électronique qui est plus forte qu'un code d'utilisateur couplé à un mot de passe (par exemple, avec un jeton électronique ou un certificat).

- la connexion avec l'environnement du fournisseur⁵⁸ doit être sécurisée au moyen d'un mécanisme d'identification fort,
- les informations échangées sont cryptées,
- le réseau du fournisseur est sécurisé selon les conditions imposées par le RTSS et garanties par contrat.

3.5.3 *Perspectives conceptuelles*

Les concepts et les modèles abordés dans la présente section sont complémentaires aux perspectives conceptuelles du modèle technologique de référence présenté au chapitre 2. Ils sont retenus comme orientations en matière de sécurité pour la mise en place de services électroniques communs de sécurité et d'interfaces sécuritaires.

Vue des services communs

La vue des services communs de sécurité présente l'infrastructure de répertoires harmonisés de sécurité, qui est composée de trois niveaux :

- le répertoire d'entreprise, qui comporte une composante de répertoire intranet et une composante de répertoire public ;
- les répertoires communautaires intégrés pour chaque environnement de base ou les répertoires de groupe dans chaque environnement global ;
- les répertoires des mécanismes de contrôle qui sont spécialisés par produit.

Les services communs de sécurité sont basés sur les principes de fonctionnement suivants :

- une gestion des accès par rôle selon un modèle RBAC (Role-Based Access Control) ;
- la mise en place d'un mécanisme de gestion intégrée des informations de sécurité basé sur des répertoires LDAP, avec :
 - une administration décentralisée de l'environnement de base et du répertoire d'entreprise,
 - une automatisation de mise à jour du répertoire d'entreprise, aussi bien pour sa composante de répertoire intranet que pour sa composante de répertoire public ;

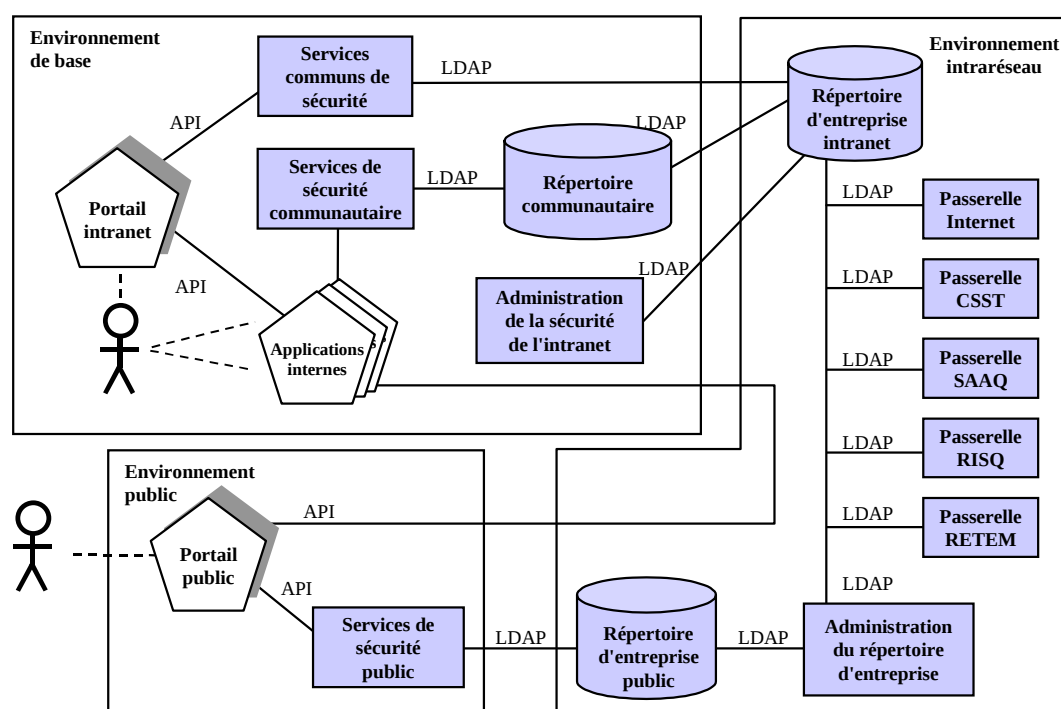
58. Le terme *fournisseur* englobe ici toutes les entités externes au RTSS précisées dans le modèle technologique de référence présenté à la section 2.2.3.

- une infrastructure distribuée de répertoires, dans laquelle :
 - le répertoire d'entreprise est requis pour la gestion intégrée de la sécurité,
 - les répertoires communautaires peuvent être constitués de différentes technologies conformes à LDAP version 3 ou plus.

Le diagramme 28 illustre la structure des répertoires harmonisés soutenant les services communs selon les principes de fonctionnement énoncés précédemment. Cette vue met en lumière :

- les fonctions décentralisées d'administration des environnements de base et les fonctions d'administration du répertoire d'entreprise ;
- l'utilisation des services communs par le portail intranet, un éventuel portail public et les applications au moyen d'API ;
- l'utilisation du répertoire d'entreprise par les passerelles d'échanges électroniques avec le protocole LDAP.

Diagramme 28 : Vue des services communs de sécurité



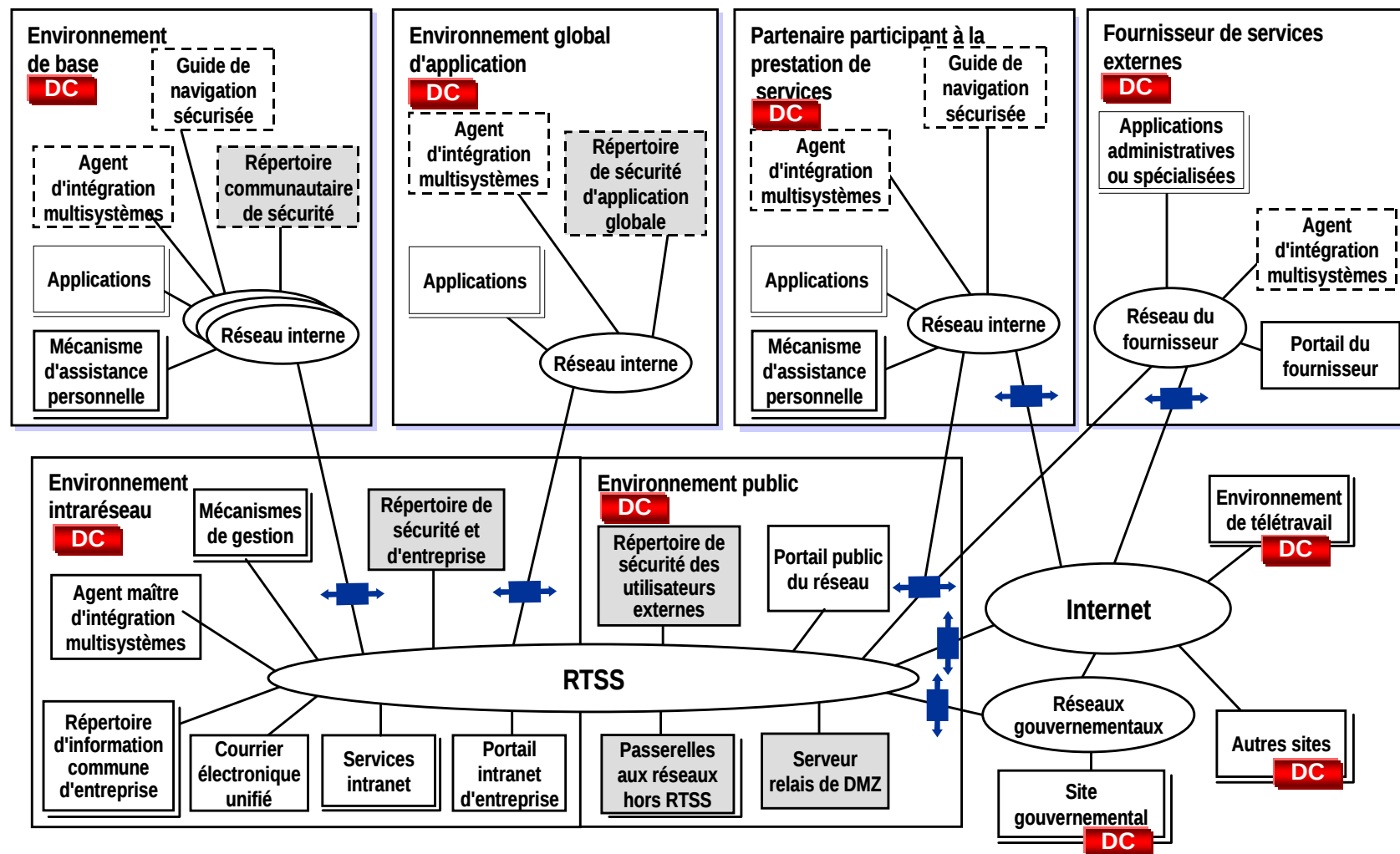
Vue des infrastructures technologiques

La vue des infrastructures technologiques requises pour la sécurité est illustrée par le diagramme 29. Elle est complémentaire à la vue de second niveau des infrastructures technologiques présentée dans le modèle technologique de référence du chapitre 2.

Outre les différents environnements établis comme des domaines de confiance possibles avec l'indication DC, le diagramme précise le positionnement des interfaces sécuritaires entre ces domaines de confiance. Elles sont représentées par des doubles flèches associés aux rectangles sur les liens de télécommunications.

L'architecture de sécurité devra préciser les frontières des domaines de confiance et les mécanismes requis pour soutenir les interfaces sécuritaires entre les domaines.

Diagramme 29 : Vue des infrastructures technologiques de sécurité



3.6 Les orientations en matière de télécommunications

La présente section aborde les orientations spécifiques en matière de télécommunications qui ont été retenues pour le réseau sociosanitaire québécois⁵⁹. Au préalable, les éléments de contexte décrivent les faits saillants de l'état de situation actuelle et les principaux constats qui en résultent ainsi que quelques tendances technologiques. Par la suite, les énoncés de direction et les perspectives conceptuelles définissent les orientations comme telles.

3.6.1 Éléments de contexte

*État de situation actuelle*⁶⁰

Le *Réseau de télécommunications sociosanitaire* (RTSS) est le seul véhicule d'échange d'information autorisé entre les établissements du réseau de la santé et des services sociaux. Il relie les quelque 400 établissements du réseau, répartis sur près de 1 500 sites physiques, les 18 régions régionales, la RAMQ, l'OPHQ, le Ministère et les organismes-conseils relevant du ministre. Il utilise, sur une base de location, les infrastructures de télécommunications du Groupe des télécommunicateurs du Québec (GTQ), un consortium formé par Bell Canada, QuébecTel et Télébec, qui assure l'accès privé au RTSS par les organisations du réseau sociosanitaire. Un technocentre national, situé chez Sogique, et dix-huit technocentres régionaux contribuent à la gestion du RTSS.

Différents niveaux de services sont offerts et soutenus à raison d'un service par site. Ces niveaux de services sont les suivants :

- **Service A :** lien 56 Kbps ou 128 Kbps relais de trame ;
- **Service B :** lien 256 Kbps, 512 Kbps et 1 544 Mbps relais de trame ;
- **Service C :** lien ATM à 1 544 Mbps ;
- **Service D :** lien ATM à 45 Mbps ;
- **Service E :** lien ATM à 155 Mbps ;
- **Service T :** accès commuté pour les télétravailleurs ;
- **Service F :** accès distant commuté ou dédié pour les fournisseurs.

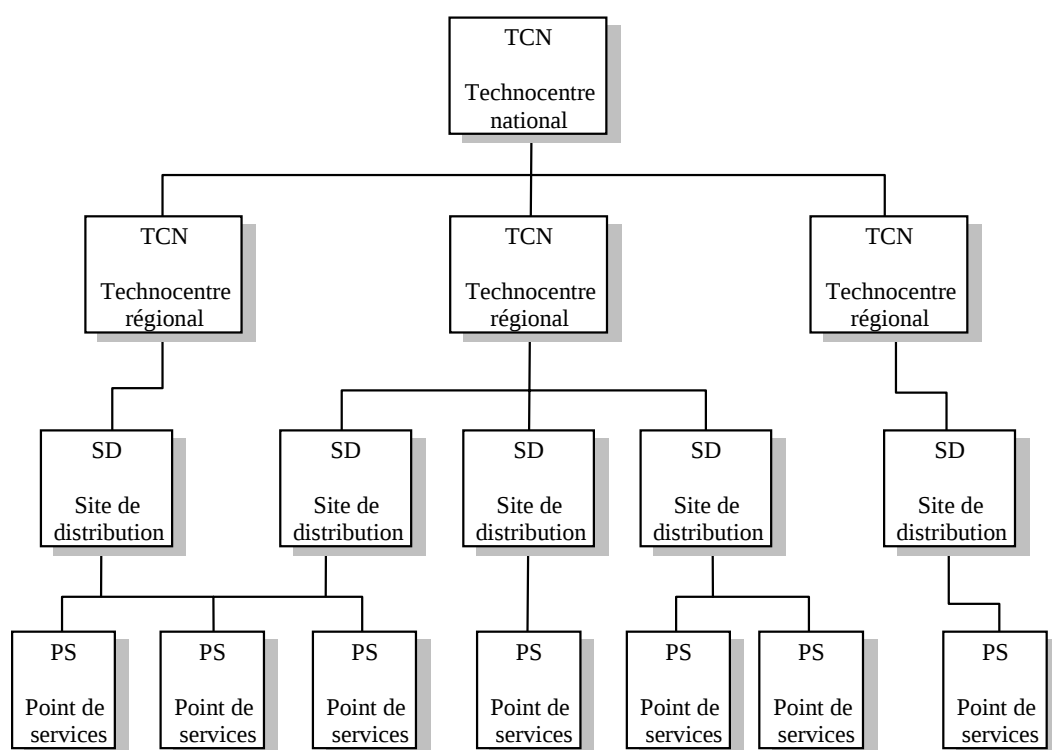
59. Ces orientations portent sur les services du RTSS. Elles ne couvrent pas la téléphonie ni les communications sans fil.

60. Selon le document *Document d'information sur le RTSS*, Bureau d'accueil et Centre de certification, MSSS, version 2.2, 2000 ; et selon le document *Le RTSS un + pour moi et pour la population, Une perspective d'avenir* : MSSS, GTQ, 2001.

Le RTSS comporte deux architectures logiques distinctes qui tiennent compte des caractéristiques transactionnelles des applications.

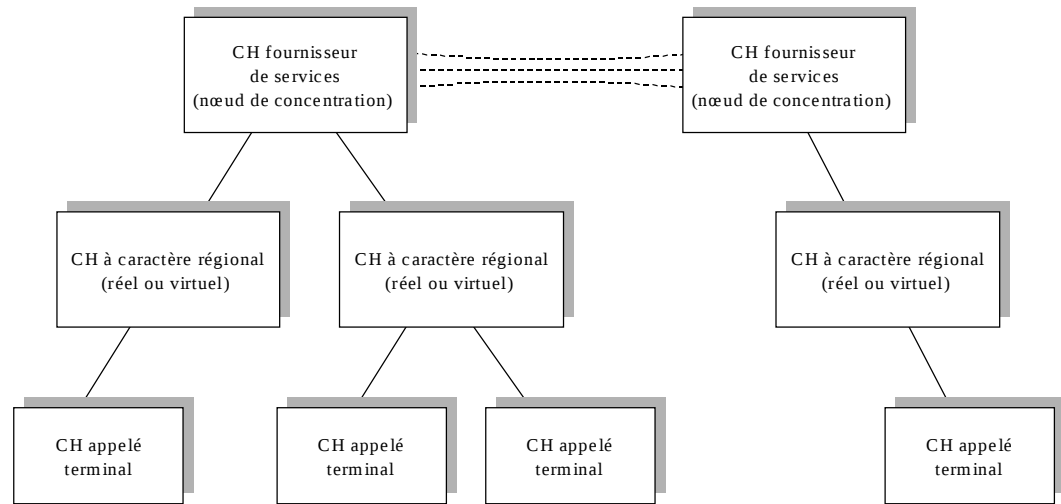
La première est une architecture caractérisée par une structure hiérarchisée des nœuds de communication. Cette architecture permet les échanges de messages diversifiés (des types données, voix et images fixes) pour des applications du domaine clinique et du domaine médico-administratif ainsi que les accès à Internet. Le diagramme 30 présente les principaux nœuds de communication de cette architecture.

Diagramme 30 :
Architecture actuelle pour les domaines clinique et médico-administratif



- Un établissement a généralement un point de distribution et quelques points de services.

La seconde architecture logique est caractérisée par l'utilisation de circuits plus directs entre les sites terminaux d'échange. Cette architecture permet la transmission d'images animées en temps réel demandant une largeur de bande adéquate et continue pour assurer la fluidité des communications. Elle soutient, entre autres, les applications de vidéoconférence pour la télémedecine et le téléenseignement, notamment en point à point avec le standard H.323 et, éventuellement, avec MPEG2. Le diagramme 31 présente les principaux nœuds de communication de cette architecture.

Diagramme 31 : Architecture actuelle pour le domaine de la télésanté

Ces architectures logiques de réseau sont implantées principalement à l'aide de commutateurs et d'aiguilleurs qui gèrent l'acheminement des messages selon le protocole de réseau IP. Le routage est paramétré vers l'architecture appropriée selon le type de communication.

La sécurité sur le RTSS est assurée au niveau physique, au niveau du réseau virtuel privé et au niveau de l'interréseautage. Pour ce qui est des applications, le RTSS permet le transport de messages encryptés, mais ne gère pas la sécurité des applications elles-mêmes.

Au niveau de l'interréseautage, le RTSS comprend une zone démilitarisée (DMZ) pour supporter l'accès Internet sécurisé et les services d'hébergement. Cette zone est caractérisée par :

- l'utilisation de serveurs intermédiaires pour accéder au réseau privé ;
- l'absence de stockage de données sensibles (des types médico-administratives et clinique) ;
- une gestion des accès par des coupe-feu et la détection d'intrusion ;
- un support du chiffrement des communications et de l'authentification forte des utilisateurs ;
- un soutien 24 heures par jour et 7 jours par semaine ;
- un haut niveau de disponibilité.

Le RTSS comporte aussi des passerelles d'échange d'information avec des réseaux externes, dont :

- une passerelle avec la CSST ;
- une passerelle Internet permettant entre autres de gérer le courrier électronique ;
- la passerelle vers les établissements d'enseignement et les organisations reliées au RISQ. Celle-ci est sécurisée avec coupe-feu et détection d'intrusion. Deux liens à 90 Mbps assurent robustesse et communications diversifiées.

De nouvelles passerelles sont prévisibles, notamment avec le RICIB/RETEM.

Au niveau du réseau virtuel privé (à l'intérieur du RTSS), la sécurité est assurée par la diversité physique des routes, la redondance du centre de contrôle, le cloisonnement du réseau et le fractionnement des transmissions.

Enfin, la sécurité physique est assurée par le contrôle des accès aux équipements, la gestion des bâtiments et la gestion des infrastructures.

Tendances technologiques

Plusieurs nouvelles technologies en télécommunications sont maintenant offertes, ou sont sur le point d'arriver sur le marché pour :

- la gestion de la bande passante en fonction d'une catégorisation des besoins de services (*Quality of Service*) ;
- la gestion de sessions de vidéoconférence basées sur IP (*Gatekeeper*) ;
- la diffusion en mode multipoint de session de vidéoconférence ;
- les communications sans fil.

Pour la vidéoconférence, la suite de standards H.3xx⁶¹ distribuée par International Télécommunications Union l'(ITU) est définie pour permettre des échanges d'information basés sur différents protocoles de réseau (par exemple, MTA et Ethernet).

61. Où xx renvoie à la numérotation des différents standards comme H.320 ou H.323.

Principaux constats

Le RTSS est une infrastructure technologique essentielle à la modernisation du système de services. Il apporte une facilité d'échange d'information qui permet d'accroître l'efficacité dans l'organisation des services. Il favorise l'intégration des systèmes, notamment en offrant des services uniformes à l'ensemble des organisations du réseau, voire à l'ensemble du secteur socio-sanitaire. Ses infrastructures peuvent aussi évoluer pour continuer à appuyer efficacement l'organisation des services.

Les besoins d'interconnexion sont en croissance, pour soutenir :

- les interventions au domicile de l'utilisateur ;
- les interventions depuis le domicile du professionnel ;
- les accès pour les partenaires participant à la prestation des services (cliniques médicales, laboratoires, pharmacies, entre autres) ;
- les grappes fonctionnelles multi-organisations (par exemple, les groupes de médecine de famille et les réseaux de télé-services) ;
- les passerelles d'échange avec d'autres réseaux et sites ;
- les interconnexions aux réseaux gouvernementaux comme le RICIB/RETEM ;
- les interconnexions à des réseaux ou à des sites canadiens et internationaux ;
- l'amélioration du réseau supportant les télé-services, aussi bien pour les applications actuelles que pour de nouvelles applications.

Par ailleurs, une consultation menée dans le réseau en janvier 2001 a permis de déterminer un ensemble de besoins. Ainsi, les processus de gestion du RTSS, la sécurisation et la qualité des services peuvent être améliorés pour une performance encore meilleure. Les points susceptibles d'accroître la performance du RTSS sont les suivants :

- en matière de processus de gestion :
 - la réduction de la complexité et des délais pour les changements,
 - la révision des procédures de règlement des problèmes (escalade, délais d'intervention et de réparation),
 - le soutien pour certaines applications (client-serveur, vidéoconférence, télésanté),

- la comptabilisation et le suivi d'indicateurs de gestion (temps-réponse, disponibilité, utilisation),
- la promotion du RTSS et une meilleure information sur ses capacités ;
- en matière de sécurisation :
 - l'amélioration de la sécurité des accès par Internet par une plus grande responsabilisation de l'intervenant et l'utilisation de mécanismes d'identification et d'authentification forte, de chiffrement et de VPN pour les applications non Web,
 - la mise en place de mécanismes particuliers de sécurité pour les grappes fonctionnelles et les groupes d'intérêt ;
- en matière de qualité des services :
 - l'utilisation de dispositifs de gestion de la bande passante,
 - l'amélioration de la capacité et de la performance des liens interpavillonnaires,
 - la robustesse accrue de la solution Internet ;

Des outils communs de gestion additionnels s'imposent également afin d'assurer la gestion préventive des problèmes, de la disponibilité et des performances. Ainsi, les applications de téléservices se distinguent par l'utilisation d'équipements et de logiciels spécialisés, de protocoles particuliers d'échange d'information et de bandes passantes d'une grande capacité sur le réseau de télécommunications. Aussi, la disponibilité et la performance des infrastructures partagées qui soutiennent ces services deviennent critiques dans le cas des applications sensibles au délai, telle que la vidéoconférence et l'imagerie animée en direct.

3.6.2 Principes directeurs en matière de télécommunications

Compte tenu des éléments de contexte décrits précédemment et des défis de sécurité et de performance soulevés par les besoins d'évolution du RTSS, les orientations spécifiques retenues en matière de télécommunications sont les suivantes.

- Reconnaître le RTSS comme unique véhicule de communication autorisé au sein du réseau de la santé et des services sociaux, et ce, afin de garantir le plus haut niveau de sécurité et de performance des échanges.

- Maintenir la distinction entre les deux architectures de réseaux, soit celle des domaines clinique et médico-administratif et celle du domaine de la télésanté, et consolider les services de télécommunications afin d'améliorer l'utilisation des bandes passantes et la disponibilité du RTSS.
- Assouplir la gestion de la sécurité à l'intérieur du RTSS par l'implantation de mécanismes permettant aux établissements de gérer les accès (comme la déhiérarchisation des accès et la mise en place de services de réseau local étendu).
- Soutenir les échanges entre les organisations reliées au RTSS et l'ensemble de leurs interlocuteurs externes, tels que les partenaires participant à la prestation des services (par exemple, les cliniques privées) ou les autres acteurs du secteur de la santé et des services sociaux (par exemple, les chercheurs et les enseignants, les fournisseurs de services d'application ainsi que certains ministères et organismes). La solution de télécommunication sera adaptée aux besoins fonctionnels et de sécurisation des échanges.

Ainsi, des interfaces sécuritaires devront être définies et établies entre le RTSS et les domaines de confiance des interlocuteurs externes. Ces interfaces impliqueront l'utilisation de mécanismes d'identification et d'authentification forte et des garanties de sécurité par entente formelle. Elles impliqueront également une segmentation des accès aux applications du réseau en fonction du profil des utilisateurs définis au répertoire public de sécurité.

Dans les cas d'échanges transactionnels comportant un certain volume, la mise en place de circuits sécurisés avec l'environnement de l'interlocuteur sera privilégiée. Dans les cas d'échanges sporadiques, l'utilisation d'Internet sera permise en autant que les solutions de sécurisation soient celles qui ont été autorisées pour l'accès au RTSS, alors que le choix du fournisseur du lien Internet sera laissé libre.

- Améliorer la robustesse du RTSS et sa continuité opérationnelle par l'implantation des mécanismes requis de redondance d'accès, de redondance des infrastructures de la DMZ et de redondance des passerelles (ROPAS), ainsi que par la mise en place des plans de relève dans tous les technocentres du réseau sociosanitaire (TCN, TCR et TC locaux).
- Exercer une veille technologique en télécommunications afin de prévoir l'évolution du RTSS selon les nouvelles perspectives technologiques qui se dessinent, et ce, avant la fin du contrat avec le fournisseur actuel. Cet exercice permettra procéder aux analyses requises, notamment en ce qui a trait aux télécommunications sans fil et aux technologies de vidéoconférence, dont le standard MPEG2.

Au regard des applications de téléservices, les orientations en matière de télécommunications consistent à :

- à définir et à mettre en place des mécanismes de gestion sur l'architecture de réseau du domaine de la télésanté afin de garantir des services à haut débit et stables pour les applications sensibles au délai, notamment pour la vidéoconférence et l'imagerie animée en direct ;
- à améliorer les réseaux internes par l'utilisation de portiers (*Gatekeeper*) ou d'adaptateurs multipoints (*MCU*) lorsque la situation le justifie ;
- à prendre avantage des services de réseau local étendu prévus dans les orientations en matière de télécommunications afin d'assurer la gestion de l'environnement des applications de téléservices ;
- à privilégier l'utilisation d'Internet pour les communications à l'extérieur du RTSS, sauf lorsque les exigences de qualité nécessitent le recours à une largeur de bande garantie ;
- à considérer l'utilisation de technologies sans fil lorsque celle-ci est pertinente et techniquement faisable.

En ce qui concerne les standards, le standard DICOM est retenu pour les applications d'imagerie médicale, alors que le format MP3 est retenu pour les sons (ce qui inclut la voix). Pour la vidéoconférence, l'utilisation du standard H.323 avec IP est privilégiée. Les autres standards du tableau suivant peuvent être utilisés au besoin, selon les situations et les possibilités des services de télécommunications.

Tableau 7 : Standards particuliers à la vidéoconférence⁶²

	Bande étroite H.320	MTA H.321, H.310	Iso-Ethernet H.322	Ethernet H.323	RTPC H.324
Compression vidéo	H.261	H.261, H.263, MPEG-2	H.261, H.263	H.261, H.263	H.261, H.263
Compression audio	G.711, G.722, G.728	G.711, G.722, G.728	G.711, G.722, G.723, G.728	G.711, G.722, G.723, G.728, G.729	G.723
Multiplexage	H.221	H.221	H.221	H.225	H.223
Signalisation	H.230, H.242	H.230, H.242	H.242	H.230, H.245	H.245
UCM	H.243	H.231, H.243	H.231, H.243	H.323	N/A
Réglage de caméra	H.224, H.281	H.224, H.281	H.224, H.281	H.224, H.281	H.224, H.281
Chiffrement	H.233, H.234	H.233, H.234	H.233, H.234	H.233, H.234	H.233, H.234

3.6.3 *Perspectives conceptuelles*

Les concepts et les modèles abordés dans la présente section sont complémentaires aux perspectives conceptuelles du modèle technologique de référence présenté au chapitre 2. Ils sont retenus comme orientations en matière de télécommunications pour la mise en place d'infrastructures technologiques et de services électroniques communs de soutien aux systèmes d'information.

Vue des services communs

Les services communs de télécommunications s'appuient sur l'architecture de TCP/IP qui définit les protocoles standard de communication régissant les transmissions sur les réseaux logiques du RTSS (médico-administratif et téléservices) ainsi que les transmissions entre le RTSS et d'autres réseaux. Ces services de télécommunications soutiennent l'utilisation des autres services électroniques communs définis dans le modèle technologique de référence, en particulier ceux qui se rapportent à la sécurité, aux échanges évolués et à la gestion des infrastructures partagées.

62. Tableau tiré du document de travail *Constat des technologies pour l'environnement de télémédecine*, Sogique, novembre 2000.

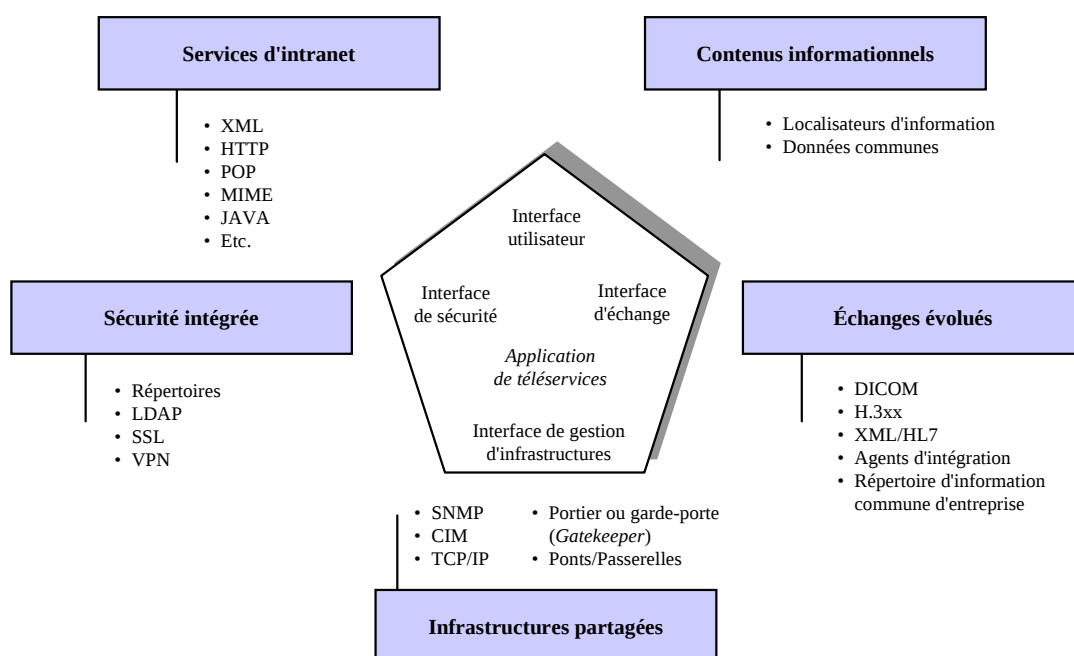
Les services communs de sécurité renvoient entre autres à la gestion des interfaces sécuritaires, y compris des mécanismes tels que les répertoires globaux de sécurité (intranet et public) et les répertoires communautaires. Ces services communs sont définis de façon plus détaillée à la section 3.5.

Les services d'échanges évolués comportent, entre autres, un système basé sur des agents d'intégration qui nécessitent le recours aux services de télécommunications. Ces services communs sont définis de façon plus détaillée à la section 3.1.

Enfin, les services communs de gestion d'infrastructures partagées sont essentiels au soutien de la gestion et de la disponibilité de l'ensemble des infrastructures utilisées dans les échanges du réseau sociosanitaire, dont précisément le RTSS.

Le diagramme 32 rappelle la vue d'ensemble des services communs définie au chapitre 2. Il indique les concepts et les types de standards associés au soutien des télécommunications, notamment en égard à la sécurité, aux échanges évolués et à la gestion des infrastructures partagées.

Diagramme 32 : Vue des services communs pour les télécommunications



Vue des infrastructures technologiques

La vue des infrastructures technologiques de télécommunications est illustrée par le diagramme 33. Elle est complémentaire à la vue de second niveau des infrastructures technologiques présentée dans le modèle technologique de référence du chapitre 2 et elle utilise le même symbolisme de représentation⁶³.

Le diagramme montre les différentes composantes touchées par les orientations en télécommunications (représentées par des rectangles à fond gris et par des traits dédoublés comme le tour de l'ovale du RTSS ainsi que les liens entre le RTSS et les réseaux internes). Les composantes technologiques illustrées dans le diagramme se rapportant aux orientations :

- de réseau local étendu (*Extended LAN*) ;
- d'architecture IP VPN sécurisée ;
- de sécurisation entre le RTSS et Internet ;
- d'amélioration de robustesse par redondance de composantes ;
- de mise en place de mécanismes de gestion des infrastructures partagées.

Chacune de ces orientations est précisée davantage ci-après.

- Réseau local étendu (*Extended LAN*) :

Le lien dédoublé et plus foncé entre les réseaux internes des environnements de base et le RTSS représente la possibilité d'établir un *réseau local étendu* entre les réseaux internes d'environnements de base situés sur des sites distants.

Cette possibilité d'établir une connexion à haute vitesse (à 10 ou 100 Mbps) entre un site de distribution et des points de services se fait généralement à l'intérieur d'une même localité (par exemple, dans la même ville). Ce service, dont l'implantation est prévue à court terme, sera disponible progressivement dans les centres urbains.

63. Le diagramme reproduit un certain nombre de services à des fins indicatives. D'autres services (courrier électronique, services intranet) pourraient également être ajoutés.

- Architecture IP VPN sécurisée :

Cette orientation est une possibilité qui doit encore être approuvée dans le contexte particulier du RTSS. Aussi, les nœuds internes du RTSS (points noirs interconnectés) représentent la possibilité future de *routage sécurisé multidirectionnel* entre les nœuds de commutation du RTSS. Selon cette orientation, les équipements du RTSS devraient être mis à niveau afin d'intégrer des fonctions de sécurité et de routage dynamique entre les principaux nœuds de commutation.

Cette reconfiguration des principaux nœuds du réseau de télécommunication permettrait :

- une amélioration significative des performances du RTSS, car elle réduirait le nombre de nœuds de commutation d'une route de communication ;
- l'établissement de circuit virtuel privé (VPN) pour chaque liaison établie dynamiquement ; les contrôles de sécurité seraient effectués au moyen d'un répertoire de sécurité accessible sous le protocole LDAP.

La mise en place de l'architecture IP VPN sécurisée aurait pour effet de déhiérarchiser le réseau de télécommunications. Ainsi, les circuits pourraient être établis directement entre deux nœuds sans passer par un nœud maître jouant le rôle de chef d'orchestre.

- Sécurisation entre le RTSS et les domaines de confiance externes :

Cette orientation de sécurisation est représentée par les petits rectangles fléchés dans les environnements externes et l'environnement public. À titre d'exemple, à l'aide de son poste de travail et d'un outil d'identification et d'authentification forte, le partenaire participant à la prestation de service qui travaille dans une clinique privée et qui a accès aux applications disponibles du réseau peut se connecter au RTSS en établissant un circuit virtuel privé (VPN) par l'entremise d'Internet ou d'un circuit sécurisé dédié.

Un bastion et un détecteur d'intrusion filtrent les communications vers la DMZ. Le serveur relais de la DMZ authentifie le partenaire et vérifie ses privilèges d'accès à l'aide du répertoire public de sécurité. Des sessions de communication peuvent ensuite être engagées avec les serveurs des établissements. Le retour d'information emprunte le tunnel VPN.

- Amélioration de robustesse par redondance de composantes :

Les liens entre les réseaux internes des environnements et le RTSS sont dédoublés pour représenter les *possibilités de redondance* permettant

éventuellement d'assurer une meilleure continuité opérationnelle. Ces possibilités s'ajoutent à la redondance déjà prévue pour les centres névralgiques du réseau, notamment le serveur relais de DMZ et les infrastructures du TCN.

Les solutions possibles de redondance se situent au regard des liens, de la combinaison liens et protocole IP et de la combinaison route, lien et protocole IP.

La redondance de liens suppose un lien alternatif au lien principal, soit un lien identique sur le même aiguilleur ou un lien différent (du type RNIS, par exemple).

La redondance combinant liens et IP permet de séparer le trafic sur deux liens, ce qui limite la non-disponibilité en cas de perte d'un des liens.

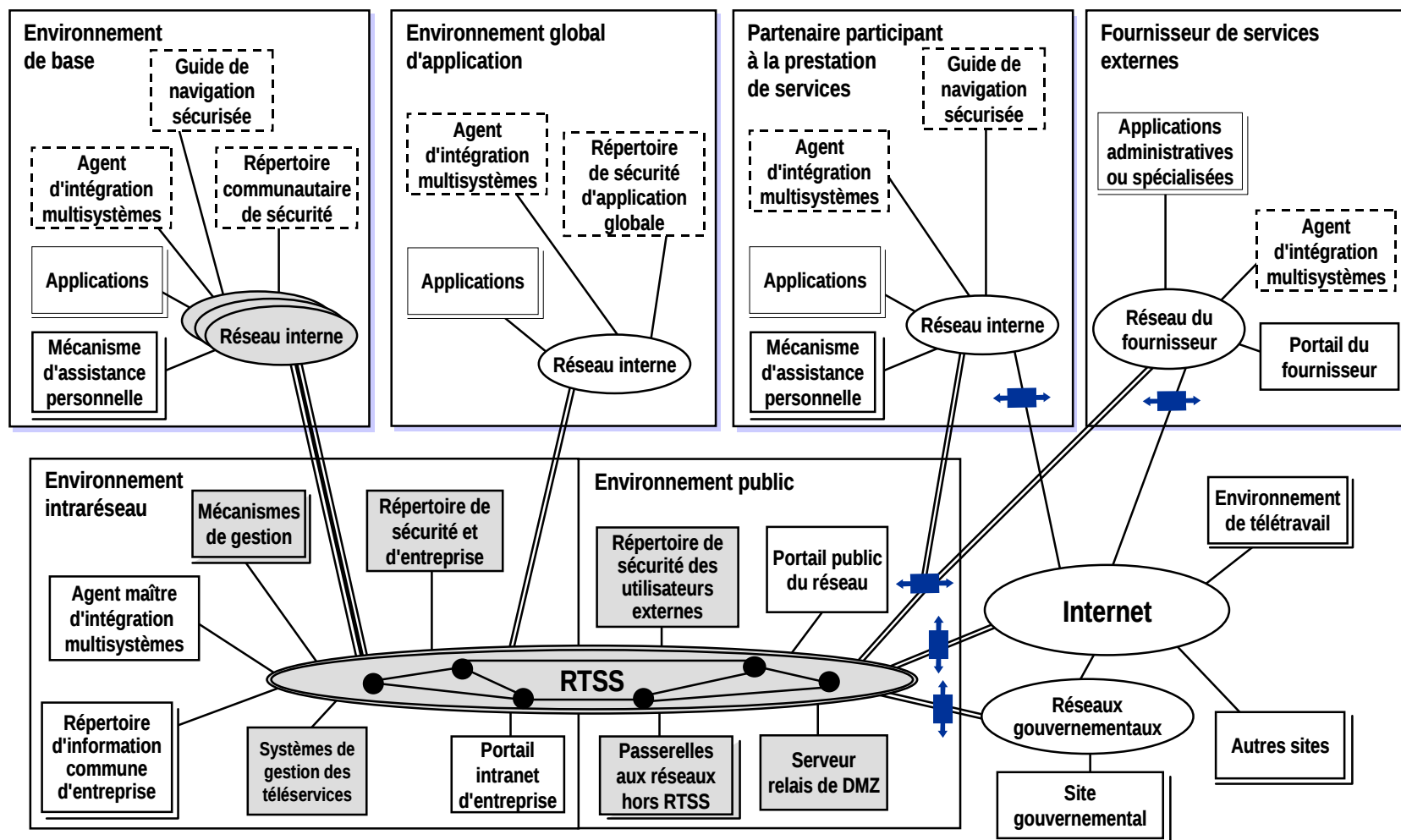
Enfin, la redondance combinée route, liens et IP permet de rediriger automatiquement le trafic en cas de panne de lien ou d'aiguilleur, quitte à ralentir temporairement les performances. C'est la solution la plus sûre.

Les coûts afférents à chacune de ces solutions sont différents, de sorte que chaque situation doit être analysée afin de déterminer la configuration optimale.

- Mise en place de mécanismes de gestion des infrastructures partagées :

Ces mécanismes de gestion représentent différents outils de gestion spécialisés selon les fonctionnalités couvertes, telles que l'administration de la sécurité, la gestion de la disponibilité et de la performance et la distribution de logiciels. Ils renvoient également aux composantes technologiques mises en place pour la gestion des sessions de télé-services. Ils utilisent les informations de base qui sont emmagasinées dans les répertoires communautaires et les répertoires globaux d'entreprise et de sécurité (intranet et public).

Diagramme 33 : Vue des infrastructures technologiques pour les télécommunications



4 LA PLANIFICATION DE LA MISE EN ŒUVRE

Les orientations technologiques présentent des notions et des modèles utiles pour guider la conception et la mise en place d'infrastructures communes sur un horizon d'environ quatre années. Ces notions et ces modèles correspondent aux tendances technologiques présentant le meilleur potentiel d'évolution. Leur mise en œuvre demande que des projets de nature technologique soient planifiés et réalisés.

Par ailleurs, les projets de livraison et d'évolution des systèmes d'information du réseau doivent également se poursuivre. La convergence de ces projets avec les orientations technologiques est voulue le plus tôt possible. Cependant, elle présuppose que les composantes et les infrastructures correspondant aux orientations technologiques soient offertes aux développeurs des systèmes d'information du réseau socio sanitaire.

En conséquence, la transition sera un succès, à condition que les infrastructures technologiques prévues soient mises en place et que les systèmes d'information soient adaptés à leur utilisation.

Outre la mise en place des infrastructures technologiques et des changements aux systèmes, l'évolution se poursuit sur d'autres fronts : les stratégies se précisent ou se transforment, et le marché des technologies voit apparaître de nouveaux concepts et des produits plus évolués. Un processus de gestion des orientations technologiques est donc nécessaire afin de s'assurer que l'alignement sur les stratégies demeure adéquat et que les technologies utilisées continuent de correspondre aux meilleures pratiques.

C'est dans le but d'harmoniser l'évolution des systèmes, les infrastructures et les orientations technologiques que la planification de la mise en œuvre présente :

- des orientations de transition pour les systèmes d'information ;
- un processus de gestion des orientations technologiques ;
- un plan de mise en œuvre pour implanter les infrastructures technologiques et les *services communs*.

Ces différents volets de la planification de la mise en œuvre des orientations technologiques sont abordés successivement dans les sections du présent chapitre.

4.1 Des orientations de transition pour les systèmes d'information

La transition est la période qui marque le passage entre la situation actuelle et une situation où :

- les infrastructures technologiques prévues dans les orientations sont mises en place ;
- les *services communs* sont implantés et opérationnels ;
- plusieurs systèmes d'information majeurs qui sont implantés et opérationnels utilisent les nouvelles infrastructures ;
- chaque nouveau système, ou chaque refonte ou évolution importante d'un système, est conçu et réalisé selon les orientations technologiques.

La stratégie de transition envisagée pour les systèmes d'information du réseau se veut progressive. Les premiers systèmes ou projets touchés sont ceux qui seront désignés comme porteurs. À terme, le cycle de vie des systèmes aura un effet d'entraînement incontournable en faveur des orientations.

4.1.1 Principes d'alignement sur les orientations

Principe 1 : Les nouveaux projets devront se conformer aux orientations technologiques de la façon la plus complète possible.

Les nouveaux projets, particulièrement ceux d'intérêt commun, sont ceux qui sont encore en voie de conception, ce qui inclut les systèmes faisant l'objet d'une refonte, ceux qui nécessitent des changements majeurs et ceux qui en sont encore au stade de l'étude d'opportunité, de la conception administrative (ou analyse préliminaire) ou de l'architecture. Ces systèmes sont tous des projets porteurs et ils devront se conformer aux orientations technologiques de la façon la plus complète possible.

Pour des raisons pratiques, particulièrement dans le cas de progiciels devant être implantés rapidement, des mesures d'exception pourront être adoptées.

Principe 2 : Simultanéité des projets de mise en place d'infrastructures et de développement de systèmes.

La mise en place des infrastructures et des *services communs* prévus dans les orientations technologiques repose sur un échéancier de plusieurs mois. Pendant ce temps, certains projets de livraison de systèmes se poursuivront. Ces projets se dérouleront donc simultanément à des projets de réalisation technologique.

Un projet de livraison de système pourra être révisé pour s'arrimer aux orientations technologiques et devenir un projet porteur si les circonstances s'y prêtent et que cette révision n'entrave pas ses objectifs. Autrement, le projet poursuivra son déroulement en parallèle, selon l'échéancier qui a été planifié.

Principe 3 : Maximisation des bénéfices escomptés pour les projets déjà en cours de réalisation.

L'alignement sur les orientations technologiques pour les systèmes déjà en chantier devra tenir compte des conséquences possibles sur la portée des projets et des bénéfices escomptés d'éventuels changements. Un point d'équilibre devra être trouvé, en fonction :

- de l'état d'avancement du projet ;
- des bénéfices liés à l'utilisation potentielle des infrastructures et des *services communs* amenés par les orientations technologiques ;
- des coûts et des délais de livraison.

Principe 4 : Maximisation des bénéfices escomptés pour les systèmes en place.

Pour les systèmes en place, l'à-propos de certains alignements aura à être analysé cas par cas. Toutefois, la plupart des situations requerront probablement une véritable étude d'opportunité tenant compte à la fois des aspects stratégiques, fonctionnels et technologiques.

4.1.2 Modalités de transition

Selon les principes énoncés précédemment, chaque système ou projet fera éventuellement l'objet d'une évaluation en vue d'un alignement sur les orientations technologiques. Les premiers systèmes visés sont ceux de portée commune utilisant le RTSS. Les paragraphes qui suivent résument les modalités de transition.

Projet livrant après l'implantation des infrastructures communes

Un projet de système en phase d'analyse dont la livraison est prévue après l'implantation des nouvelles infrastructures technologiques communes est un projet porteur qui nécessite :

- un alignement sur les orientations technologiques qui soit le plus complet possible ;

- une synchronisation avec les projets de réalisation technologique qui livreront les infrastructures et les *services communs*.

Un tel projet peut également être utilisé pour la réalisation d'infrastructures et de *services communs*.

Projet livrant avant l'implantation des infrastructures communes

Un projet de système en phase d'analyse dont la livraison est prévue avant l'implantation des nouvelles infrastructures technologiques communes est un projet porteur qui doit s'aligner sur les orientations technologiques applicables et inclure un plan d'évolution pour l'utilisation éventuelle des infrastructures et des *services communs*.

Un tel projet peut également être utilisé pour la réalisation d'infrastructures et de *services communs*.

Projet en phase de réalisation ou système existant

Pour un projet de système en phase de réalisation technique ou pour un système existant, l'alignement doit tenir compte de la portée du système, de la durée de vie utile de la version du système, de l'évolution prévue ainsi que des améliorations fonctionnelles et technologiques à apporter.

En ce qui a trait à la durée de vie utile du système, les investissements pour l'entretien ou la mise à niveau technologique sont à être minimisés dans le cas d'une courte durée (environ un an). Ce type de système ne nécessite donc pas vraiment d'alignement. Par contre, dans le cas d'un système ayant une durée prévue de plus d'un an, les responsables du projet doivent :

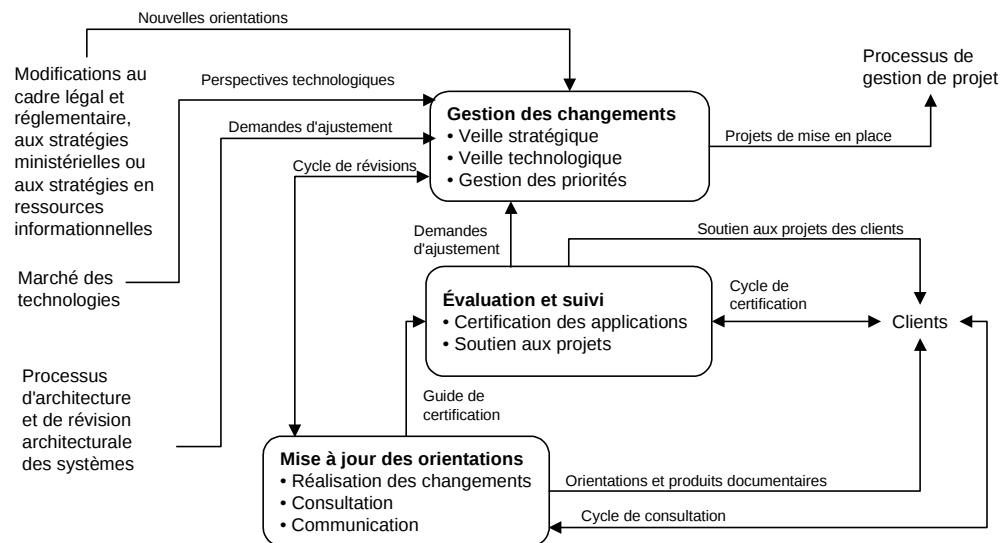
- considérer les améliorations technologiques pouvant apporter rapidement des bénéfices significatifs sans entraîner des coûts de développement élevés (par exemple, l'utilisation du mode Terminal Server) ;
- considérer la vue d'ensemble des systèmes, la portée actuelle du système sous analyse ainsi que l'ampleur des améliorations fonctionnelles et technologiques qui seront nécessaires ;
- planifier les investissements requis pour faire évoluer le système :
 - soit par l'implantation d'une solution transitoire et des changements majeurs au système (ce qui fait apparaître un nouveau projet),
 - soit par la réduction des investissements dans le système actuel et la livraison accélérée d'une nouvelle version davantage conforme à la vue d'ensemble des systèmes, aux besoins fonctionnels et aux orientations technologiques.

4.2 Un modèle de gestion des orientations technologiques

Le modèle de gestion abordé dans la présente section propose un processus qui permet d'appliquer et de faire évoluer les orientations technologiques. Ce processus ne précise toutefois pas les rôles et les responsabilités à l'égard de la gestion des orientations technologiques. Cet exercice est cependant prévu dans le cadre de la mise en œuvre des orientations technologiques.

Le diagramme 34 illustre les activités et les flux d'information du modèle de gestion des orientations technologiques. Ces éléments sont décrits plus en détail dans les sections qui suivent.

Diagramme 34 : Modèle de gestion des orientations technologiques



4.2.1 Description des activités

Le processus de gestion des orientations technologiques comprend des activités de gestion des changements et de mise à jour des orientations ainsi que d'évaluation et de suivi de l'application des orientations.

Gestion des changements

La gestion des changements regroupe les activités requises pour assurer l'évolution des orientations tant en déterminant les ajouts et les mises à jour

nécessaires qu'en établissant la priorité de ces travaux. Ces activités comportent la *veille stratégique*, la *veille technologique* et la *gestion des priorités*.

La *veille stratégique* consiste à suivre les changements qui sont apportés au cadre légal et réglementaire, aux politiques ministérielles et gouvernementales ainsi qu'aux orientations stratégiques en matière de ressources informationnelles afin d'en évaluer les conséquences sur les orientations technologiques du réseau. Ce processus continu permet de déterminer les besoins de changement relativement aux orientations et aux normes.

La *veille technologique* consiste à suivre l'évolution des technologies de l'information et des communications de manière à détecter des occasions d'intérêt pour le réseau. Ce processus est lui aussi continu et il permet notamment d'introduire de nouvelles technologies dans les orientations.

La *gestion des priorités* consiste à réguler l'ensemble des activités d'actualisation et de publication des orientations et des produits documentaires qui leur sont associées, tels que des normes, des guides et les conditions d'intégration au RTSS. Ce processus permet :

- d'attribuer des priorités aux travaux à réaliser ;
- d'engager la production ou l'actualisation des orientations et des produits documentaires ;
- de définir les mandats de réalisation technologique.

Mise à jour des orientations technologiques

La mise à jour des orientations technologiques regroupe les activités requises pour assurer la *réalisation des changements* à apporter aux orientations, les *consultations auprès des clientèles* et la *communication des orientations* et des différents produits documentaires.

La *réalisation des changements* vise à actualiser les orientations et les différents produits documentaires. Les travaux consistent à :

- mener les recherches nécessaires dans la foulée des priorités énoncées par la gestion des changements ;
- produire le matériel de soutien pour répondre aux clients ;
- réviser les orientations et les produits documentaires à la suite des consultations.

Les *consultations auprès des clientèles* visent à informer les organisations et les personnes touchées par les changements et à prendre leur avis en considération

avant de faire connaître les nouvelles orientations et de diffuser la mise à jour des produits documentaires.

La *communication des orientations* et autres produits documentaires, enfin, a pour objectif d'assurer la diffusion auprès des clientèles visées. À cet égard, les travaux consistent à produire le plan et le matériel de communication et à coordonner les activités de communication et de diffusion auprès des clientèles.

Évaluation et suivi de l'application des orientations

L'évaluation et le suivi de l'application des orientations regroupent les activités qui concernent tant la *certification des applications et des technologies* que le *soutien aux projets* dans le but de faciliter l'alignement des systèmes sur les orientations technologiques.

La *certification des applications et des technologies* vise à s'assurer que les conditions d'intégration au RTSS, mises à jour sur la base des orientations technologiques, sont respectées. Cette activité peut entraîner des demandes d'ajustement aux orientations et aux normes.

Le *soutien aux projets* permet d'offrir aux clientèles un accompagnement pendant la conception d'un système afin d'assurer l'alignement *a priori* sur les orientations technologiques. Cette approche contribue à atténuer les conséquences de l'exercice de certification, car elle permet de déterminer, dès la phase de conception, les écarts possibles avec les orientations technologiques. Le fait d'offrir ce soutien n'empêche pas le fait qu'une application doive obtenir la certification requise avant sa mise en production.

4.2.2 Résultats du processus

La réalisation des activités décrites dans le modèle de gestion conduit à des résultats concrets, soit : des orientations technologiques actualisées, des guides proposant les meilleures pratiques, des projets de réalisation technologique, un guide de certification et des attestations de conformité.

Orientations technologiques actualisées

Bien qu'une version actualisée des orientations technologiques soit publiée au début du cycle de gestion, différentes situations conduiront à la production de versions amendées et plus complètes, comme :

- des changements majeurs au cadre législatif et réglementaire ou aux orientations stratégiques du réseau ;
- la réalisation d'analyses complémentaires sur des sujets technologiques particuliers.

Guides proposant les meilleures pratiques

Des guides proposant les meilleures pratiques peuvent être réalisés, par exemple, pour favoriser le partage des connaissances en technologie.

Définition de projets de réalisation technologique

Les orientations technologiques permettent de déterminer les infrastructures et les *services communs* requis pour les systèmes du réseau. Des mandats de réalisation technologique doivent être définis pour mettre en place les infrastructures et les services communs. Ces mandats peuvent faire l'objet de mandats particuliers ou être intégrés dans un projet porteur.

Guides de certification

L'activité d'évaluation et de suivi comprend la certification des applications et des technologies, basée sur les conditions d'intégration des applications au RTSS. Ces conditions d'intégration seront mises à jour afin qu'elles correspondent aux orientations technologiques.

Attestation de conformité

L'attestation de conformité consiste en un document émis par le Bureau d'accueil des applications et fait suite à la certification. Ce document atteste que l'application souscrit et fait aux conditions d'intégration au RTSS.

4.3 Le plan de mise en œuvre

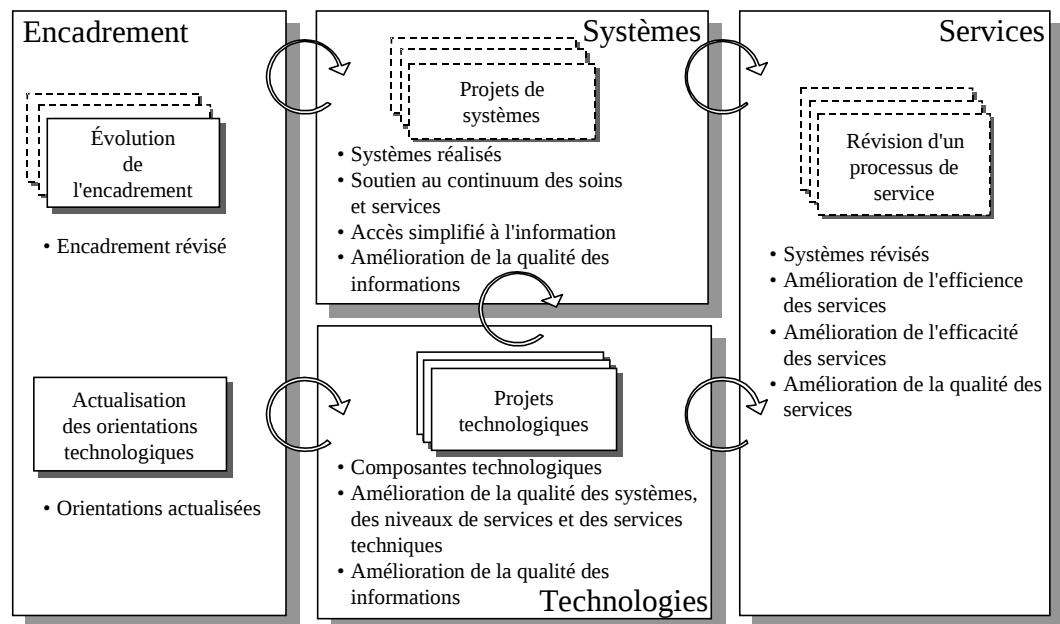
La présente section aborde le plan de réalisation des initiatives ou projets qui découlent des orientations technologiques du réseau. Ce plan de mise en œuvre comprend :

- une chaîne de résultats qui situe les initiatives issues des orientations technologiques dans le contexte plus global de la gestion des ressources informationnelles ;
- les principes sur lesquels s'appuie la planification ;
- l'approche de mise en œuvre des différentes initiatives et projets ;
- le plan d'action qui est défini sous forme de fiches dans lesquelles se retrouvent l'échéancier du projet et l'évaluation des efforts.

4.3.1 Chaîne de résultats⁶⁴

Le diagramme 35 illustre la chaîne sommaire des résultats découlant de l'actualisation des orientations technologiques du réseau. Les détails de ce diagramme sont présentés à l'annexe 2.

Diagramme 35 : Chaîne sommaire des résultats



⁶⁴ . La chaîne de résultats est un concept défini dans la méthode Station DMR Résultats^{MC} du Macroscop^{MC} de DMR conseil.

L'objectif de la chaîne de résultats est de mettre en évidence les initiatives à entreprendre, les résultats intermédiaires et finaux de ces initiatives ainsi que les contributions entre ces initiatives. La chaîne de résultats permet ainsi d'établir un plan de travail cohérent en ordonnant les initiatives en fonction de leurs contributions respectives.

Le diagramme découpe quatre blocs principaux de contributions, soit l'*encadrement*, les *systèmes*, les *technologies* et les *services*. Les blocs sont reliés l'un à l'autre par des flèches circulaires qui indiquent une influence mutuelle. En effet, l'*encadrement* permet d'aligner les *systèmes* et les *technologies* en fonction des stratégies et il est lui-même influencé par les travaux de ces deux blocs. Les *technologies* facilitent l'intégration des *systèmes* et apportent un soutien aux processus de *services*. Elles évoluent selon les besoins des *systèmes* et sont influencées par les besoins des processus de *services*. Enfin, les *systèmes* fournissent un apport informationnel aux processus de *services* et permettent de les faire évoluer. Eux-mêmes sont influencés par les besoins propres aux processus de *services*.

Ces blocs correspondent aux différentes couches d'architecture du modèle de gestion des ressources informationnelles décrit à la section 1.4 du document. En effet, la couche des processus de services est représentée par le bloc des services, alors que les couches de l'information et des applications et données peuvent être associées au bloc des systèmes. Les services électroniques et les infrastructures correspondent au bloc des technologies tandis que les domaines de gestion, enfin, recouvrent tout le bloc d'encadrement.

Cette toile de fond permet de situer les initiatives découlant des orientations technologiques. Ces initiatives sont de deux types. D'une part, elles consistent en des travaux d'encadrement qui doivent être réalisés afin de donner les bons alignements aux systèmes et aux technologies. D'autre part, elles correspondent à un ensemble de projets technologiques. Ces projets visent principalement à mettre en place des infrastructures et des *services communs* ainsi que les mécanismes de gestion les plus appropriés aux technologies.

Le diagramme 35 illustre également les principaux résultats attendus pour chaque bloc. La chaîne détaillée de résultats, qui est présentée en annexe 2, montre quant à elle les résultats intermédiaires et finaux de chaque initiative issue des orientations technologiques. Le tout permet de relier les initiatives technologiques aux résultats globaux visés, soit l'amélioration de l'efficacité, de l'efficacités et de la qualité des services offerts à la population québécoise.

Les paragraphes qui suivent décrivent de façon plus détaillée les initiatives et les projets technologiques de la chaîne de résultats⁶⁵.

65. Le lecteur est invité à consulter l'annexe 2, qui présente les diagrammes détaillés de la chaîne de résultats, pour avoir un aperçu visuel de l'ensemble des initiatives et des projets.

Initiatives du bloc d'encadrement

Les initiatives d'encadrement portent sur les activités de définition et de planification d'ensemble. Elles ont une influence considérable sur les autres volets étant donné qu'elles en définissent les grandes orientations.

L'actualisation des orientations technologiques fait partie du bloc d'encadrement puisque ces orientations définissent les concepts, les modèles et les règles d'architecture technologique que doivent respecter la conception des systèmes d'information et la mise en place des infrastructures. Par ailleurs, les orientations technologiques sont influencées par des initiatives globales d'encadrement, telles :

- le plan stratégique ministériel 2001-2004 pour l'évolution des services du réseau socio sanitaire ;
- le plan d'action en matière de ressources informationnelles 2001-2004 ;
- le cadre de gestion global des actifs informationnels communs du réseau socio sanitaire.

Dans un avenir plus ou moins rapproché, les orientations technologiques seront également influencées par l'architecture globale de l'information.

La chaîne détaillée de résultats (voir l'annexe 2) montre que, pour le bloc d'encadrement, les résultats de l'actualisation des orientations technologiques contribuent à des initiatives externes plus globales, notamment en ce qui a trait à l'évolution des stratégies en ressources informationnelles, du cadre de gestion des ressources informationnelles et des architectures d'ensemble – dont celles qui se rapportent à la sécurité, aux données de référence, aux structures d'échange entre applications et aux banques d'information partagées.

D'autres initiatives d'encadrement résultent directement des orientations technologiques :

- l'évolution des normes et guides technologiques (dont les normes techniques) inclus dans les orientations, les conditions d'intégration au RTSS et d'éventuels guides proposant les meilleures pratiques en technologie ;
- la diffusion des orientations technologiques actualisées ;
- l'analyse des conséquences des orientations sur les projets et les systèmes.

Ces dernières initiatives font partie intégrante du plan de mise en œuvre.

Initiatives du bloc des technologies (services et infrastructures)

Les initiatives ou les projets technologiques sont conséquents aux concepts et aux modèles définis dans les orientations. Ils visent à concevoir et à mettre en place les infrastructures et les *services communs* prévus. Les projets portent sur :

- les *services communs* de sécurité ;
- l'évolution du RTSS ;
- le portail général de services intranet ;
- les services intranet ;
- l'environnement de gestion technique ;
- les fonctions d'échange électronique ;
- la mise en place d'extranets ;
- les banques d'information partagées ;
- les infrastructures de télésanté ;
- le système de diffusion de données communes.

Comme le montre la chaîne de résultats (voir l'annexe 2), les *services communs* de sécurité, l'évolution du RTSS et les fonctions d'échange électronique sont des projets qui seront utiles à plusieurs autres projets. L'ensemble des initiatives de ce bloc est inscrit dans le plan de mise en œuvre des orientations technologiques.

Initiatives du bloc des systèmes

Le bloc des systèmes comprend les initiatives ou les projets de livraison d'applications. Ces projets, quoiqu'ils soient externes à la mise en œuvre des orientations technologiques, doivent utiliser les infrastructures et les *services communs* mis en place par les initiatives du bloc des technologies. Ils sont représentés dans la chaîne de résultats pour attester de la contribution des technologies. Cependant, les projets de livraison d'applications ne font pas partie du plan de mise en œuvre des orientations technologiques. Certains d'entre eux pourront éventuellement être inscrits s'ils sont définis comme des projets porteurs à la mise en œuvre des orientations technologiques.

Initiatives du bloc des services

Les besoins des processus de services aux clientèles du réseau socio sanitaire exercent une influence majeure sur la conception des systèmes et l'usage des technologies. Ces processus de services sont eux-mêmes transformés lorsqu'ils utilisent des systèmes et des technologies comme le dossier de santé électronique

de l'utilisateur, les systèmes de courrier électronique et les infrastructures de télé-santé.

La révision des processus de services fournit donc l'occasion d'intégrer de nouveaux systèmes et moyens technologiques aux méthodes de travail. Comme pour le bloc des systèmes, les révisions de processus de services sont des initiatives externes à la mise en œuvre des orientations technologiques, et elles aussi sont représentées dans la chaîne de résultats afin de montrer que les technologies ont un effet important sur les finalités recherchées en ce qui concerne l'amélioration de l'efficacité, de l'efficacité et de la qualité des services aux usagers du réseau socio-sanitaire.

4.3.2 Principes de planification de la mise en œuvre

Jusqu'à présent, la description de la chaîne de résultats a permis de présenter les initiatives et les projets du plan de mise en œuvre. Une stratégie de mise en œuvre est nécessaire à la planification. Cette stratégie repose sur les principes qui suivent.

Principe 1 : Favoriser la réalisation des objectifs stratégiques.

Le plan de mise en œuvre met l'accent sur les initiatives structurantes qui soutiennent les applications découlant du plan stratégique ministériel et du plan d'action en matière de ressources informationnelles.

Principe 2 : Mettre de l'avant les projets à haute visibilité.

Les projets à haute visibilité qui supportent le déploiement de composantes d'infrastructures ou de services communs, comme le portail intranet du réseau, favorisent la promotion des concepts et des modèles préconisés par les orientations technologiques. Ces projets peuvent donc constituer un levier initial pour la mise en œuvre.

Principe 3 : Ordonner des projets en fonction des résultats.

La chaîne de résultats relève des contributions entre les initiatives. Par exemple, la disponibilité des *services communs* de sécurité et des structures d'échange d'information est de nature à faciliter l'implantation et le développement du portail intranet. L'ordonnement des projets tient donc compte de l'apport des différentes initiatives les unes aux autres, et ce, tant sur le plan fonctionnel que sur le plan technologique.

Principe 4 : Accélérer les projets technologiques les plus importants pour le soutien des projets porteurs.

L'échéancier du plan de mise en œuvre repose sur l'hypothèse d'un rythme d'implantation accéléré dans certains projets technologiques afin de soutenir les projets porteurs le plus tôt possible.

Principe 5 : Synchroniser les livraisons d'infrastructures et de services communs avec les systèmes.

Afin d'assurer la meilleure utilisation ressources, une approche « juste à temps » (*just in time*) est retenue lorsqu'elle est pertinente. Selon ce principe, la réalisation des infrastructures et des *services communs* peut être jumelée à la livraison des applications qui utiliseront en premier ces infrastructures et ces services communs.

Principe 6 : Fournir une première estimation des efforts additionnels requis pour réaliser les initiatives et projets technologiques.

Les estimations des efforts qui devront être investis dans les initiatives et les projets technologiques sont préliminaires. Ainsi, elles n'incluent pas les coûts des ressources que le réseau investit déjà dans l'entretien et l'exploitation d'infrastructures et de *services communs* puisque seuls sont extrapolés les efforts additionnels qui seront requis. De plus, les estimations sont basées sur une définition sommaire des travaux à réaliser. Les phases d'analyse et d'architecture permettront de raffiner les estimations initiales.

4.3.3 Approche de mise en œuvre

Le plan de mise en œuvre couvre une période de quatre ans qui s'étend de 2001 à 2004. Le choix de cette période concorde avec la période couverte par le plan d'action en matière de ressources informationnelles. Compte tenu de cet horizon temporel et des principes de mise en œuvre, les initiatives et les projets technologiques sont regroupés comme suit :

- au sein d'une première livraison de composantes de base, qui est planifiée sur une période d'un an et demi ;
- au sein d'une seconde livraison de composantes à valeur ajoutée se greffant aux composantes de base, qui est prévue au cours de l'année suivant la première livraison ;

- au sein d'une troisième livraison, qui est en fait une phase d'entretien et de gestion continue. Celle-ci débute en même temps que la première livraison (pour les travaux récurrents) et se poursuit jusqu'à la fin de la période de planification.

La troisième livraison permet, entre autres, de tenir compte des ressources additionnelles requises pour la prise en charge des composantes mises en place au moment des deux premières livraisons.

Des fiches de projets concernant ces trois livraisons sont présentées à l'annexe 4 du présent document.

Livraison I : composantes de base

La première livraison permet de réaliser des travaux d'encadrement, et ce, en parallèle avec les projets technologiques. Ces travaux consistent en la mise en place du modèle de gestion des orientations technologiques du réseau et en l'étude d'impact des orientations sur les projets et les systèmes.

Les autres travaux d'encadrement font partie de la phase d'entretien et de gestion continue, étant donné leur caractère récurrent.

Les projets technologiques de cette première livraison visent la mise en place de composantes de base pour les infrastructures et les *services communs* prévus dans les orientations technologiques. Les projets retenus pour cette livraison sont ceux qui répondent le mieux aux principes de mise en œuvre. Ils permettent de concrétiser les concepts généraux d'intégration énoncés dans le plan d'action en matière de ressources informationnelles, ils sont visibles et utiles aux projets porteurs, et leurs résultats serviront à des projets technologiques subséquents. Ces projets portent sur :

- les *services communs* de sécurité ;
- le portail général de services intranet ;
- les fonctions d'échange électronique de données ;
- l'environnement de gestion technique ;
- les mécanismes de gestion des téléservices.

Livraison II : composantes à valeur ajoutée

La deuxième livraison vise les composantes d'infrastructures et de *services communs* complémentaires à la première livraison. Elle comporte des projets technologiques qui consistent :

- à mettre en œuvre les banques d'information partagée et les banques de données de référence pour faire suite au déploiement des fonctions d'échange électronique de données ;
- à compléter les services de sécurité autour des répertoires d'entreprise, communautaires et de groupe ;
- à ajouter des services complémentaires d'intranet et à les intégrer au portail général de services intranet.

Livraison III : continuité et évolution

La troisième et dernière livraison comprend les initiatives et les projets de soutien, d'entretien et d'évolution des infrastructures et des *services communs*. Ces initiatives et projets portent sur :

- l'évolution des produits documentaires associés aux orientations technologiques ;
- les travaux d'architecture d'ensemble ;
- la mise à niveau des serveurs soutenant les *services communs* (en cours de façon continue) ;
- l'évolution du RTSS, dont la mise en place des extranets (projets de passerelles en cours) et le suivi des projets de téléservices (plusieurs projets en cours) ;
- le pilotage des services communs tels que les services intranet, les services de sécurité, les services d'échange électronique de données, les mécanismes de gestion des téléservices et ses infrastructures ainsi que les services de banques d'information partagée.

4.3.4 Plan d'action

Le plan d'action présente, **à titre indicatif seulement**, l'échéancier de la mise en œuvre des orientations technologiques pour les trois livraisons décrites précédemment. Une planification plus détaillée précisera les paramètres du plan de mise en œuvre.

L'échéancier couvre la période allant de 2001 à 2004. Le tableau qui suit montre les échéances prévues pour chaque initiative et chaque projet du plan de mise en œuvre. Ce même échéancier est également présenté à l'annexe 4 sous forme de diagramme de Gantt.

Tableau 8 : Échéancier des initiatives et projets technologiques

		Échéancier	
		Début	Fin
Volet I - Livraison des éléments et des composantes de base			
I.1	Mise en place du modèle de gestion des orientations	2001	2001
I.2	Étude d'impact des orientations sur les projets et les systèmes	2001	2002
I.3	Mise en œuvre des services communs de sécurité	2001	2003
I.4	Mise en œuvre d'un portail général de services intranet (choix des services)	2001	2003
I.5	Mise en œuvre des fonctions d'échange électronique (agent d'intégration)	2001	2003
I.6	Mise en œuvre de l'environnement de gestion technique	2001	2003
I.7	Mise en œuvre des mécanismes de gestion des téléservices	2001	2002
Volet II - Livraison des composantes à valeur ajoutée			
II.1	Mise en œuvre des banques d'information partagée	2002	2004
II.2	Mise en œuvre du système de distribution de données de référence	2002	2004
II.3	Ajout de services communs de sécurité	2003	2004
II.4	Ajout de services communs intranet	2003	2004
Volet III - Continuité et évolution			
III.1	Évolution des normes et des guides technologiques	2001	2005
III.2	Mise en œuvre des extranets (passerelle RTSS - ASP)	en cours	2005
III.3	Expérimentation Web en télésanté	en cours	2005
III.4	Évolution des architectures technologiques d'ensemble	en cours	2005
III.5	Évolution des serveurs partagés offrant des services communs	en cours	2005
III.6	Évolution du RTSS	en cours	2005
III.7	Gestion des services intranet	2002	2005
III.8	Coordination des services communs de sécurité	2002	2005
III.9	Coordination des services d'échange électronique de données	2002	2005
III.10	Coordination des banques d'information partagée	2003	2005
III.11	Coordination de la distribution des données de référence	2003	2005
III.12	Coordination des mécanismes de gestion des téléservices	2003	2005

5 LES CONTRIBUTIONS ET LES CONSÉQUENCES DES ORIENTATIONS TECHNOLOGIQUES ACTUALISÉES

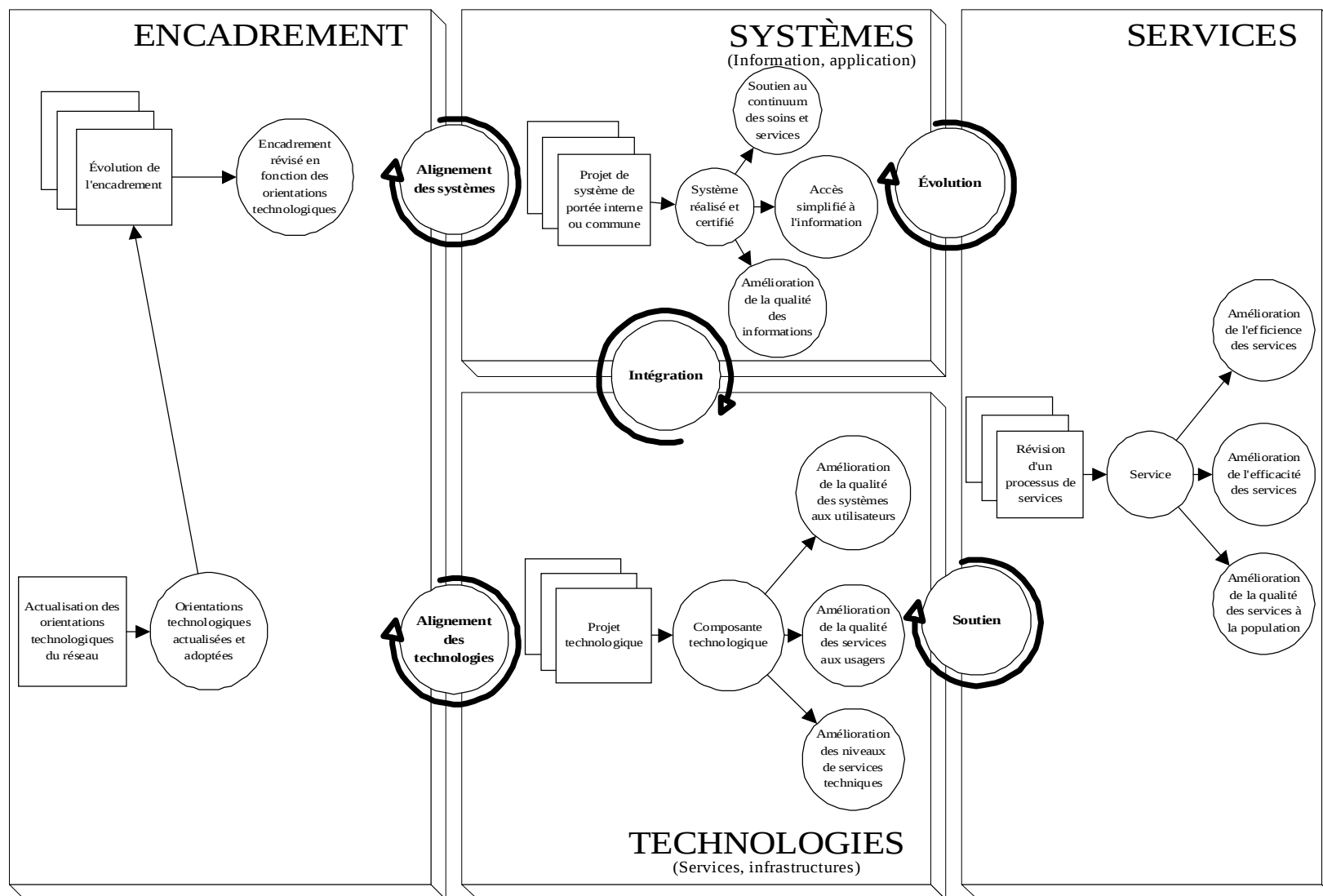
Les contributions des orientations technologiques aux objectifs définis par les orientations stratégiques sont importantes. Le plan de mise en œuvre est ambitieux et les résultats attendus le sont tout autant. Par ailleurs, des investissements et des changements aussi majeurs ne peuvent être réalisés sans avoir de conséquences sur les organisations du réseau, leur personnel, leurs partenaires de la prestation des services et les fournisseurs de produits et services, en particulier ceux du secteur des technologies de l'information. Le présent chapitre traite donc des contributions des orientations technologiques et de leurs principales conséquences.

5.1 Contributions des orientations technologiques

La chaîne de résultats utilisée pour la planification de la mise en œuvre, au chapitre 4, comprend l'ensemble des contributions associées aux orientations technologiques. C'est d'ailleurs là un des premiers buts de la chaîne. Le diagramme 36 montre les principales contributions, qui sont représentées par des cercles. Une vue plus détaillée, qui inclut les contributions intermédiaires pour chaque initiative, apparaît à l'annexe 2.

La cohérence entre le modèle de gestion et la chaîne de résultats permet de tenir compte de l'ensemble des contributions sur chacun des blocs.

Diagramme 36 : Contributions des orientations technologiques



Selon le diagramme 36, sous le volet de l'encadrement, les orientations technologiques, une fois actualisées et adoptées, permettent d'informer les acteurs du secteur socio sanitaire, les autorités gouvernementales et les fournisseurs privés de l'évolution prévue et souhaitée en matière de technologies de l'information et de communication pour le réseau de la santé et des services sociaux.

Elles permettent également d'apporter les ajustements requis à l'encadrement de gestion des ressources informationnelles pour assurer l'alignement des technologies sur les orientations stratégiques.

Sous le volet des systèmes d'information, les orientations technologiques guideront la conception des systèmes au regard de leurs aspects technologiques.

Sous le volet des technologies, les orientations technologiques conduisent à la réalisation de projets visant la mise en place des composantes de services électroniques communs et d'infrastructures technologiques partagées. Ces projets livrent des composantes qui viennent soutenir les systèmes d'information tout en assurant une meilleure utilisation des ressources.

Enfin, les orientations technologiques contribuent à faciliter l'intégration des systèmes et leur interopérabilité en préconisant de nouveaux concepts, de meilleures pratiques et une normalisation ouverte.

Sous le volet des services du réseau socio sanitaire, par l'implantation de systèmes et de technologies adaptés aux besoins, les orientations technologiques contribuent :

- à la performance des infrastructures et des services électroniques en ce qui a trait aux niveaux de services (temps-réponse, disponibilité), à la sécurité et à la protection des renseignements personnels ainsi qu'un soutien aux utilisateurs ;
- à l'amélioration des services d'information aux utilisateurs des systèmes, notamment en soutenant les processus d'échange à l'intérieur de la chaîne de services, en simplifiant l'accès à l'information et en offrant des mécanismes qui favorisent la qualité de l'information ;
- au renouvellement de l'organisation des services aux usagers et de la performance des processus de gestion, y compris la prise en charge des événements récurrents, et ce, de manière à améliorer l'efficacité, l'efficience et la qualité des services rendus aux usagers.

5.2 Conséquences générales des orientations technologiques

Au-delà de leurs contributions, les orientations technologiques ont des conséquences significatives pour la plupart des acteurs du réseau, voire du secteur sociosanitaire dans son ensemble. Ces conséquences touchent principalement les instances décisionnelles du réseau, les organisations du réseau de services ainsi que les fournisseurs de produits et services en technologies de l'information.

5.2.1 Conséquences touchant les instances décisionnelles du réseau

Pour les instances décisionnelles du réseau sociosanitaire et les mandataires jouant un rôle de gestion opérationnelle ou de gestion de projets en matière de ressources informationnelles, la mise en œuvre des orientations technologiques nécessite des décisions d'ordre financier et organisationnel. Elle implique notamment :

- la mise en place d'une organisation de gestion des orientations technologiques ;
- la nécessité de budgétiser et de financer les projets et les activités du plan de mise en œuvre des orientations technologiques ;
- la promotion et le soutien des orientations technologiques du réseau ;
- la coordination des projets relatifs au développement et à la mise en place des systèmes en vue de l'utilisation des composantes technologiques communes ;
- la révision architecturale des systèmes dans le but d'assurer l'alignement sur les orientations technologiques ;
- le suivi des projets de réalisation technologique susceptibles de nécessiter des ajustements ;
- la certification des applications selon les conditions d'intégration aux infrastructures communes du réseau sociosanitaire.

Les mécanismes de gestion définis au chapitre précédent devront être mis en place pour assurer l'application et l'évolution des orientations technologiques du réseau.

5.2.2 Conséquences touchant les organisations du réseau de services

Les organisations du réseau de services représentent les principaux utilisateurs des infrastructures technologiques et des services électroniques. En ce qui concerne ces organisations, les orientations auront pour effet de généraliser l'usage de plates-formes Web. Tout en limitant les besoins d'amélioration aux équipements,

la plate-forme Web permettra un accès élargi à un éventail d'applications et de services électroniques de soutien aux opérations, soit :

- des applications soutenant le continuum des soins et services, telles que l'index patient provincial et le dossier patient partageable ;
- des téléservices en mode Web ;
- des systèmes de gestion d'information sur les ressources et les services ;
- de nouveaux services intranet, tels que la diffusion de nouvelles, les groupes de discussion et le téléchargement de composantes qui s'ajouteront à des services existants améliorés comme le courrier électronique et l'agenda ;
- la possibilité de déployer des systèmes plus simplement et plus rapidement ;
- des services sécurisés d'échanges d'information soutenant le télétravail et les liaisons avec des partenaires.

Les organisations du réseau de services devront également apporter certains ajustements dans leurs processus de gestion des ressources informationnelles, notamment au regard :

- de la participation de coordonnateurs à la gestion décentralisée de la sécurité ;
- de la formation des utilisateurs aux nouvelles technologies ;
- du choix des applications et des technologies, dont la conformité aux orientations technologiques et au processus de certification exigera des gestionnaires une plus grande rigueur ;
- de l'évolution des infrastructures locales, qui devra tenir compte des infrastructures partagées.

5.2.3 Conséquences touchant les fournisseurs de technologies

En ce qui concerne les fournisseurs de produits et de services en matière de technologies de l'information, les orientations technologiques du réseau pourront avoir pour effets :

- de leur permettre d'acquérir une meilleure compréhension des attentes des organisations du réseau socio-sanitaire québécois en ce qui a trait aux technologies ;
- d'accroître leur capacité à prévoir les exigences auxquelles devra répondre leur offre de produits et de services ;

- de donner un avantage compétitif à ceux dont les produits seront attestés par le mécanisme de certification des applications ;
- d'améliorer la qualité de leurs produits et services et de les rendre plus exportables, compte tenu de l'alignement sur les standards de l'industrie préconisé par les orientations ;
- de déceler de nouvelles occasions d'affaires dans l'ensemble du secteur socio-sanitaire québécois.

Compte tenu du potentiel économique que représentent maintenant les technologies du Web, les fournisseurs ont clairement avantage à investir pour orienter leurs produits et leurs services dans ce sens. En rendant leurs produits et services compatibles et intégrables avec les composantes communes du réseau socio-sanitaire, les fournisseurs conservent leurs prérogatives quant au choix des technologies. Dotés des caractéristiques d'ouverture que préconisent les orientations technologiques du réseau, les systèmes mis en œuvre par les fournisseurs seront plus attrayants et répondront assurément mieux aux besoins de leur clientèle, et ce, aussi bien au Québec que partout dans le monde.

6 CONCLUSION

Dans le cadre du processus de consultation, les orientations du réseau sociosanitaire ont été comparées avec celles des autres pays au moyen des travaux de recherche de GartnerGroup. Un constat se dégage nettement : le positionnement en faveur des technologies Internet s'inscrit dans le cadre du mouvement global de décentralisation des infrastructures, mouvement appuyé par la mise en place d'environnements permettant aux organisations d'interfacer entre elles et, dans certains cas, par la mise en place de services partagés.

Le Québec partage avec ces pays la préoccupation de l'instauration d'environnements « intelligents » de prestation des services, dans le but d'améliorer la qualité tout en diminuant les coûts. Les travaux en cours à travers le réseau se situent ainsi à l'avant-garde des réflexions qui se poursuivent au niveau mondial.

C'est pourquoi nous sommes convaincus que ces orientations permettront au ministère de la Santé et des Services sociaux de répondre adéquatement aux orientations gouvernementales relatives à la prestation des services électroniques. Elles permettront aussi au réseau sociosanitaire de bâtir le réseau intégré de services qu'il souhaite offrir à la population québécoise, dans le respect des règles et devoirs qu'il a toujours privilégié à l'égard de la confidentialité de l'information personnelle et privée que la population lui confie.

ANNEXES

ANNEXE 1
SCÉNARIOS D'UTILISATION DES SYSTÈMES
D'INFORMATION

SCÉNARIOS D'UTILISATION DES SYSTÈMES D'INFORMATION

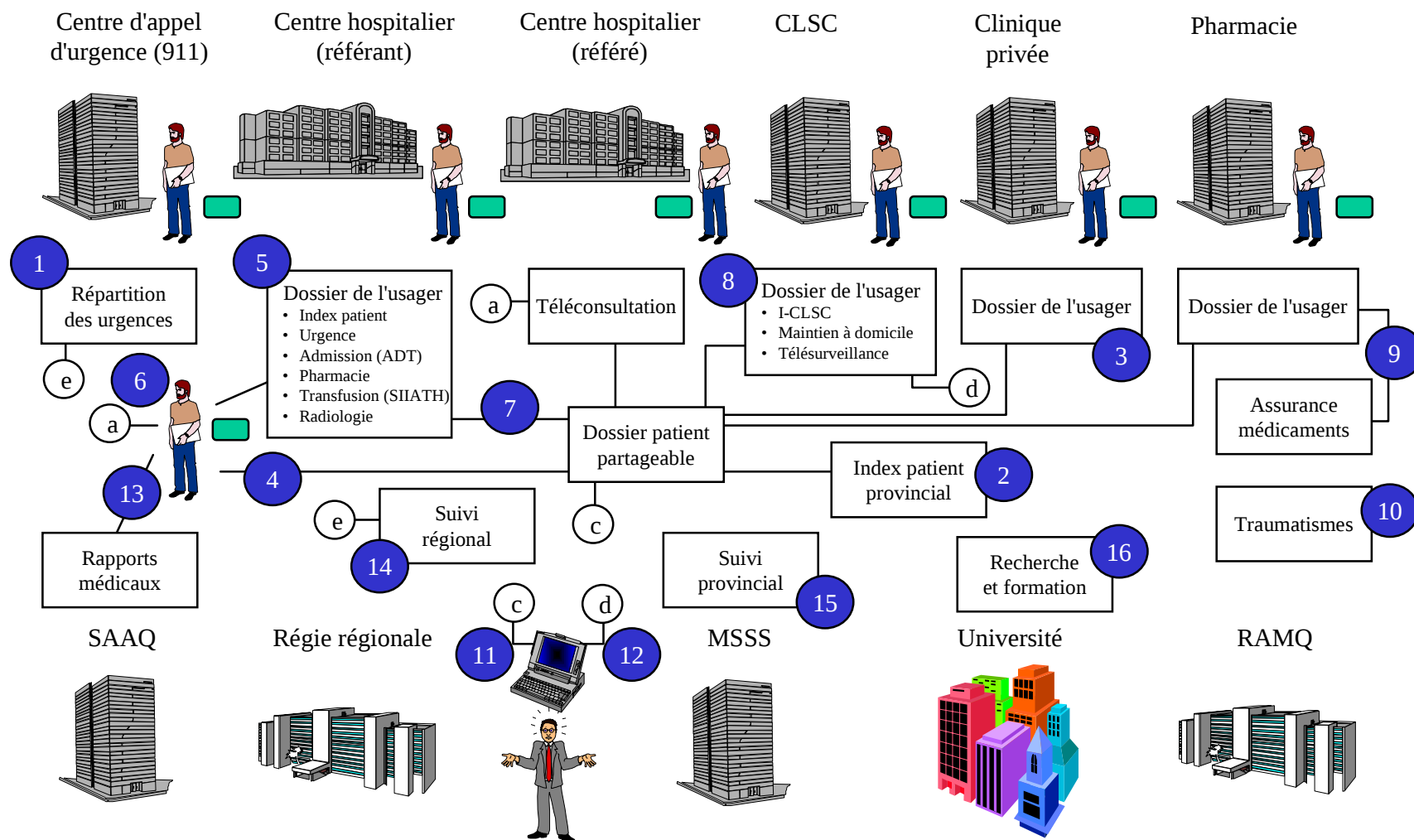
La présente annexe montre deux scénarios types qui illustrent que la complicité entre les établissements et entre les professionnels est nécessaire afin d'assurer la continuité et la complémentarité des interventions. Ces scénarios permettent également d'illustrer les systèmes d'information sous-jacents et les besoins d'échange d'information entre les systèmes. Le premier scénario est un accident de la route alors que le second présente le cas d'une personne en perte d'autonomie.

Le diagramme A1.1 de la page suivante présente le scénario simplifié d'un accident de la route. Les chiffres sur le diagramme reconstituent les principales étapes du scénario.

1. Après la collision, un appel est fait à un centre d'appel d'urgence (911). Une ambulance est envoyée sur place. Par radiocommunication, l'ambulancier demande, au centre de répartition, quelle urgence la plus proche pourra traiter le plus rapidement un blessé grave.
2. Arrivé à l'urgence, le blessé est pris en charge. Pendant qu'on s'occupe de lui, un intervenant consulte l'index patient provincial afin de retrouver les données de son dossier de santé électronique. Son arrivée est aussi consignée au système des urgences.
3. Des informations récentes et pertinentes sur le blessé sont déjà inscrites dans le système de la clinique privée qu'il a consultée au cours des derniers mois.
4. L'intervenant fait appel au dossier patient partageable pour obtenir les données pertinentes sur le blessé. Ces informations sont utilisées pour lui donner les premiers soins.
5. Une transfusion sanguine et une radiographie sont nécessaires. Une vérification est faite dans le fichier d'hémovigilance. La radiographie est portée au dossier de santé électronique de l'usager, où elle pourra être consultée facilement. Le blessé séjourne quelques jours au centre hospitalier. Son dossier d'admission est ouvert et les informations de suivi, incluant notamment les informations sur la médication qui lui est administrée, y sont inscrites.
6. Comme le blessé a subi un traumatisme assez grave, le médecin traitant effectue une téléconsultation auprès d'un spécialiste rattaché à un autre centre hospitalier.

7. Le dossier patient partageable a été mis à jour avec le consentement de l'utilisateur et il permet désormais à un intervenant autorisé de retrouver les informations partageables consignées dans les systèmes du centre hospitalier.
8. Le blessé a quitté le centre hospitalier, mais il a besoin d'une assistance à domicile et, pour les premières semaines, d'une télésurveillance. Les données pertinentes du centre hospitalier ont été transférées au dossier ouvert au CLSC. Tout au long de la période de maintien à domicile, des données de suivi sont inscrites à ce dossier.
9. L'utilisateur s'est rétabli et est redevenu autonome, mais il doit continuer à prendre des médicaments. Il se présente donc à la pharmacie où un nouveau dossier est ouvert. Le pharmacien accède au dossier patient partageable afin de vérifier les contre-indications possibles à l'ordonnance. Son système communique ensuite avec le système d'assurance médicaments pour calculer le coût de cette ordonnance. Le pharmacien inscrit les médicaments prescrits dans le dossier de l'utilisateur.
10. Les données relatives au traumatisme ont été enregistrées pendant que l'utilisateur était encore au centre hospitalier. Ces données sont disponibles aux fins de suivi et de recherche.
11. L'utilisateur peut accéder au dossier patient partageable pour vérifier certaines informations qui le concernent.
12. Pendant une certaine période, l'utilisateur est aussi en communication avec le système de télésurveillance du CLSC.
13. Comme il s'agit d'un accident de la route, des données administratives et cliniques sont transmises à la Société de l'assurance automobile du Québec (SAAQ).
14. Les données nécessaires au suivi de l'utilisateur sur le plan régional, comme l'intervention ambulancière et le cas d'urgence, ont été inscrites au moment opportun dans le fichier de suivi régional.
15. Des données de suivi ont également été transmises au fichier de suivi provincial. Elles ont notamment permis de mettre à jour les indicateurs globaux de gestion des urgences.
16. Les données ont aussi servi à produire un fichier dénominalisé transmis à une université dans le cadre d'une entente de recherche.

Diagramme A1.1 : Exemple de l'accident



Pour compléter le scénario, le diagramme montre, sous la forme d'un petit rectangle ombragé près de chaque intervenant les différents endroits où ce dernier et l'utilisateur doivent s'identifier. Un mécanisme comme la carte d'accès santé est nécessaire pour permettre l'identification non équivoque du professionnel et de l'utilisateur. Ce mécanisme peut également servir à gérer le consentement de l'utilisateur à l'accès aux informations et à singulariser les données électroniques en leur accolant la signature électronique des intervenants.

Ce scénario simplifié d'un accident de la route est indicatif d'une situation où un réseau intégré est mis en œuvre pour soutenir le continuum de soins et services à l'utilisateur. Il montre également que les informations utiles pour donner les services sont indissociables des besoins plus généraux d'information, tant sur le plan de la recherche que sur le plan administratif.

Le scénario d'accident de la route comporte de nombreuses variantes. Par exemple, dans la réalité, d'autres organisations et d'autres intervenants sont appelés à intervenir (laboratoires et centre de physiothérapie, par exemple). Par ailleurs, plusieurs situations exigeant la contribution d'autres organisations ou intervenants peuvent faire l'objet de scénarios similaires :

- un accident cardiovasculaire (urgentologue, cardiologue, etc.) ;
- un enfant battu (centre jeunesse, CLSC, corps policier) ;
- un accident du travail (CSST et autres organismes, selon la nature de l'accident) ;
- la chute d'une personne âgée (coordonnateur régional, personnel du CHSLD et physiothérapeute, entre autres) ;
- une tentative de suicide (CLSC et centre de réadaptation, par exemple).

Les occasions sont donc nombreuses de démontrer la nécessaire relation entre les différents systèmes d'information.

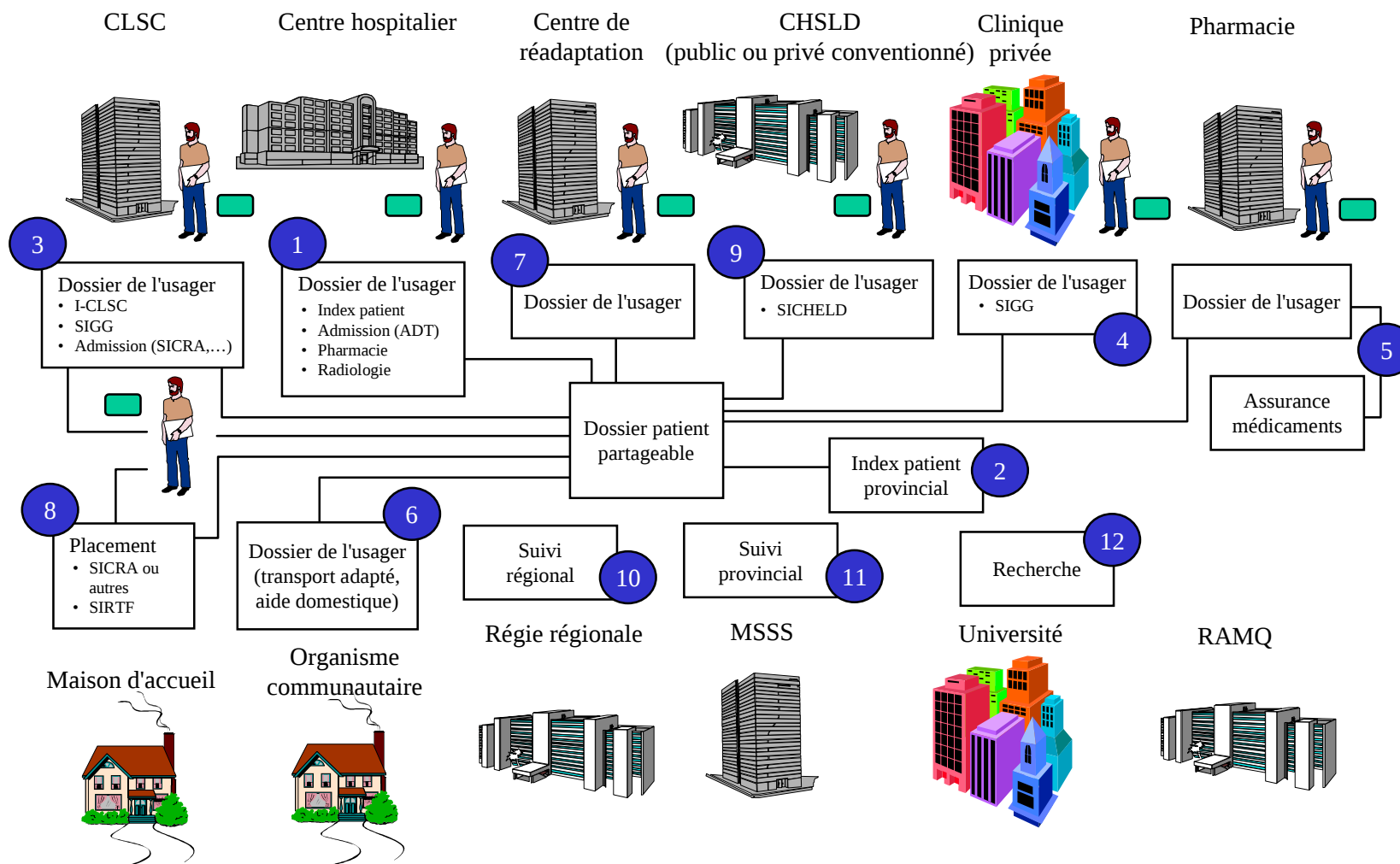
Par ailleurs, l'accident est loin d'être la seule situation qui demande la continuité et la complémentarité des interventions de la part des organisations et des professionnels du secteur socio-sanitaire. À titre indicatif, prenons l'exemple d'une personne en perte d'autonomie, pour lequel un diagramme du même type que celui du scénario d'accident est présenté ci-après (voir le diagramme A1.2). Le déroulement est le suivant.

1. Une personne atteinte de la maladie d'Alzheimer se blesse sérieusement et est amenée au centre hospitalier.
2. Elle est soignée et les informations la concernant sont inscrites à son dossier au centre hospitalier. Ces informations sont maintenant accessibles à partir de l'index patient provincial et du dossier patient partageable.
3. La personne ayant dorénavant besoin d'aide à domicile, elle est dirigée vers le CLSC. Un dossier est ouvert et les données utiles du dossier du centre hospitalier y ont été transférées. Un plan de services est défini et inscrit au dossier du CLSC. La personne est encore relativement autonome. Elle devra cependant être visitée régulièrement. Un coordonnateur est assigné pour exercer le suivi des soins et des services que cette personne recevra.
4. La personne se rend régulièrement à la clinique près de chez elle. Les informations sur son état de santé sont consignées à son dossier.
5. Elle va aussi chez le pharmacien qui tient à jour le dossier de sa médication. À chaque visite, il peut vérifier les contre-indications en accédant au dossier patient partageable et aux données du dossier qu'il tient lui-même sur cette personne. Chaque transaction fait aussi appel au système d'assurance médicaments.
6. Après plusieurs mois, l'état de santé physique et mentale de la personne se détériore. Elle aura dorénavant besoin d'aide à domicile et d'un transport adapté pour se rendre, entre autres, à un centre de réadaptation. Le coordonnateur du CLSC ajuste le plan de services. Un organisme communautaire est sollicité pour l'aide domestique et le transport adapté. Ce dernier a accès au dossier patient partageable, notamment pour l'inscription des services rendus.
7. Le centre de réadaptation a ouvert un dossier en réutilisant certaines données du dossier patient partageable. Les services rendus à chaque visite de la personne sont consignés dans le dossier.
8. À l'occasion d'une visite à domicile, l'intervenant du CLSC, qui continue ses visites régulières, constate que l'état de santé de la personne a empiré. Comme cette personne ne peut plus rester seule, elle devra être placée en maison d'accueil. Le coordonnateur du CLSC met à jour le plan de services. Il inscrit aussi les données nécessaires dans le système des ressources du type familial.
9. Quelques mois plus tard, l'état de santé physique et mentale de la personne est devenu tel qu'elle devra être admise dans un CHSLD. Les évaluations sont faites et une demande de placement s'ensuit. La demande est inscrite dans le système de coordination des admissions. Lorsqu'une place se libère, la personne est effectivement amenée dans un CHSLD. Celui-ci ouvre un dossier en utilisant les informations utiles du dossier patient partageable. Un plan de services est aussi défini et inscrit au dossier.

10. Tout au long du processus, certaines données ont été transmises à des banques de données régionales aux fins du suivi régional. En outre, le placement de la personne dans un CHSLD passe par le système de coordination régionale d'admission.
11. Des données de suivi ont également été transmises au système de suivi provincial. Elles ont notamment permis de mettre à jour les indicateurs globaux de gestion concernant les personnes atteintes de la maladie d'Alzheimer et concernant l'hébergement et les soins de longue durée.
12. Les données ont aussi servi à produire un fichier dénominalisé transmis à une université dans le cadre d'une entente de recherche.

Ce scénario, tout comme celui de l'accident, fait ressortir l'importance du partage de l'information de nature clinique pour assurer des services de qualité aux usagers du système de santé et des services sociaux. Ces scénarios démontrent de façon concrète que des systèmes fiables et partageables d'information clinique et administrative sont effectivement essentiels au continuum des soins et services.

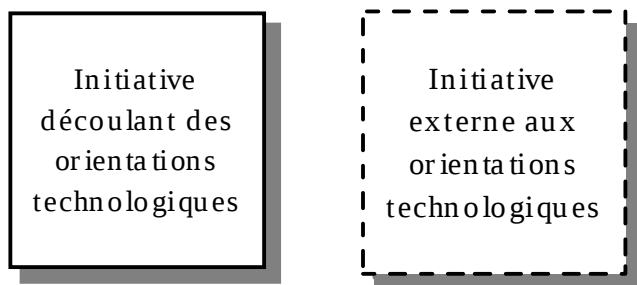
Diagramme A1.2 : Exemple de la personne en perte d'autonomie



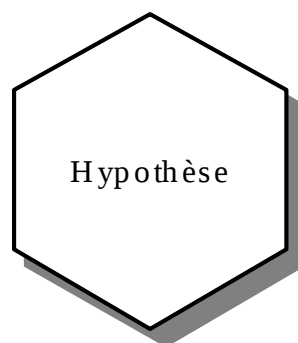
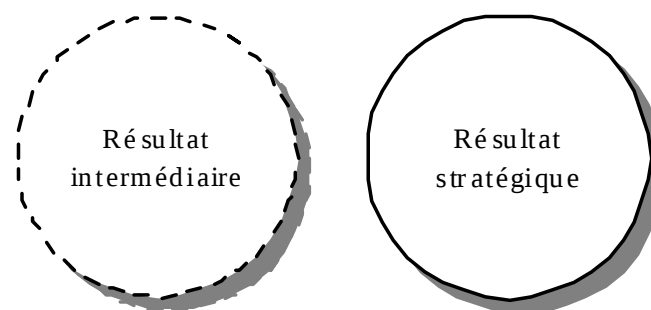
ANNEXE 2 - CHAÎNE DE RÉSULTATS

Formalisme de représentation

Types d'initiatives



Types de résultats



Contribution de base

Contribution complémentaire

Diagramme A2.1 : Vue d'ensemble de premier niveau de la mise en œuvre des orientations technologiques

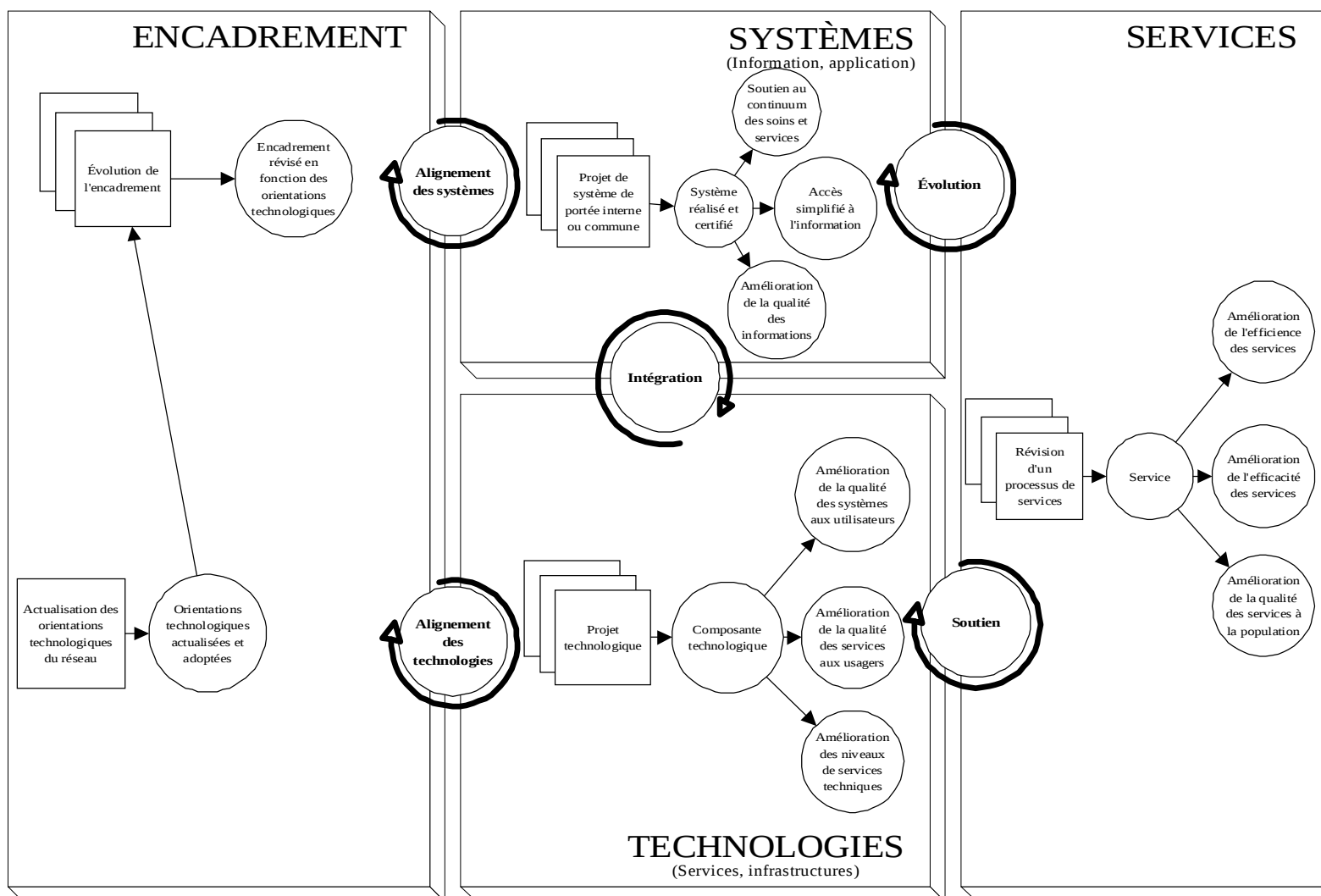


Diagramme A2.2 : Vue d'ensemble de second niveau de la mise en œuvre des orientations technologiques

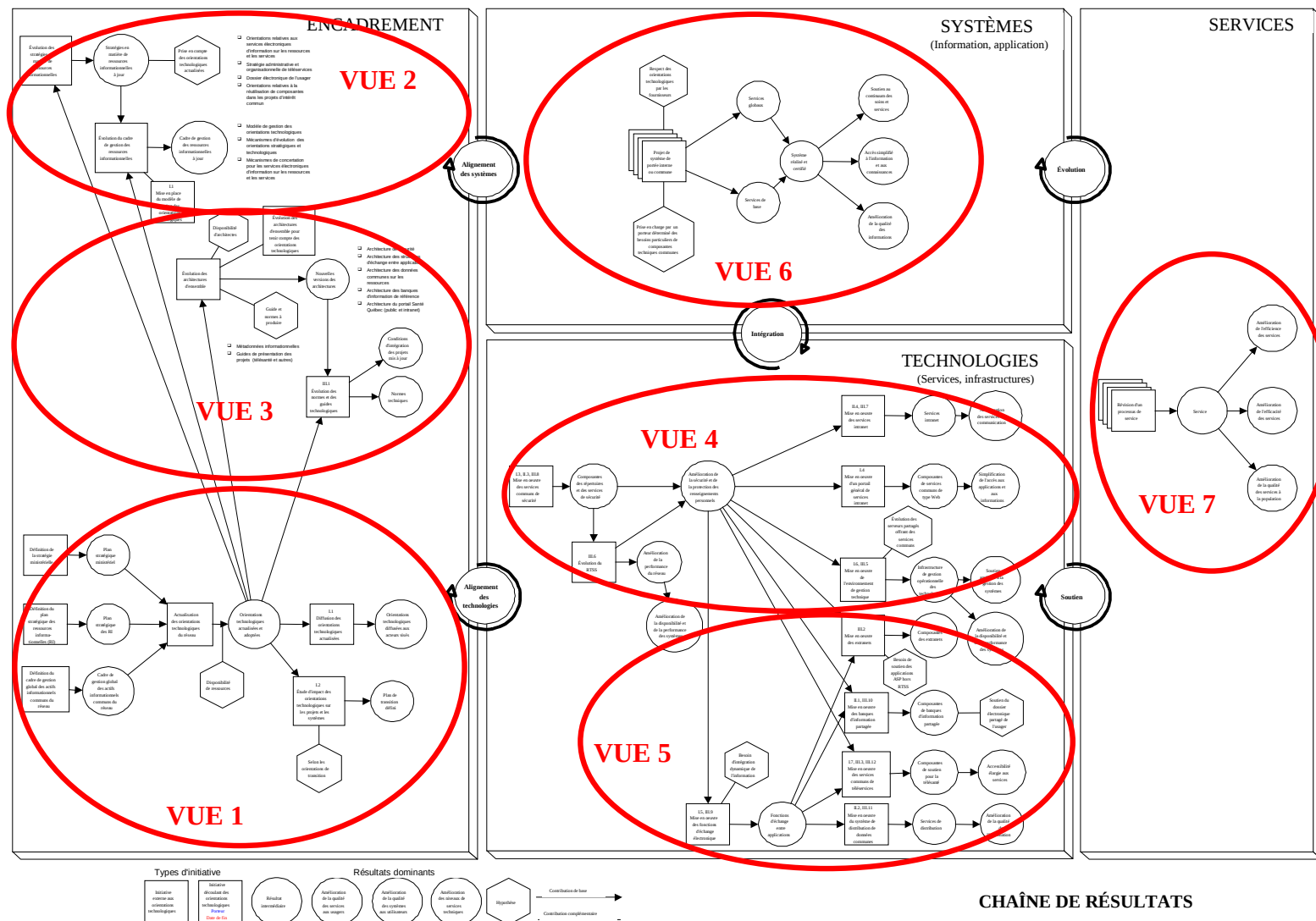


Diagramme A2.3 : Vue 1 de la mise en œuvre des orientations technologiques

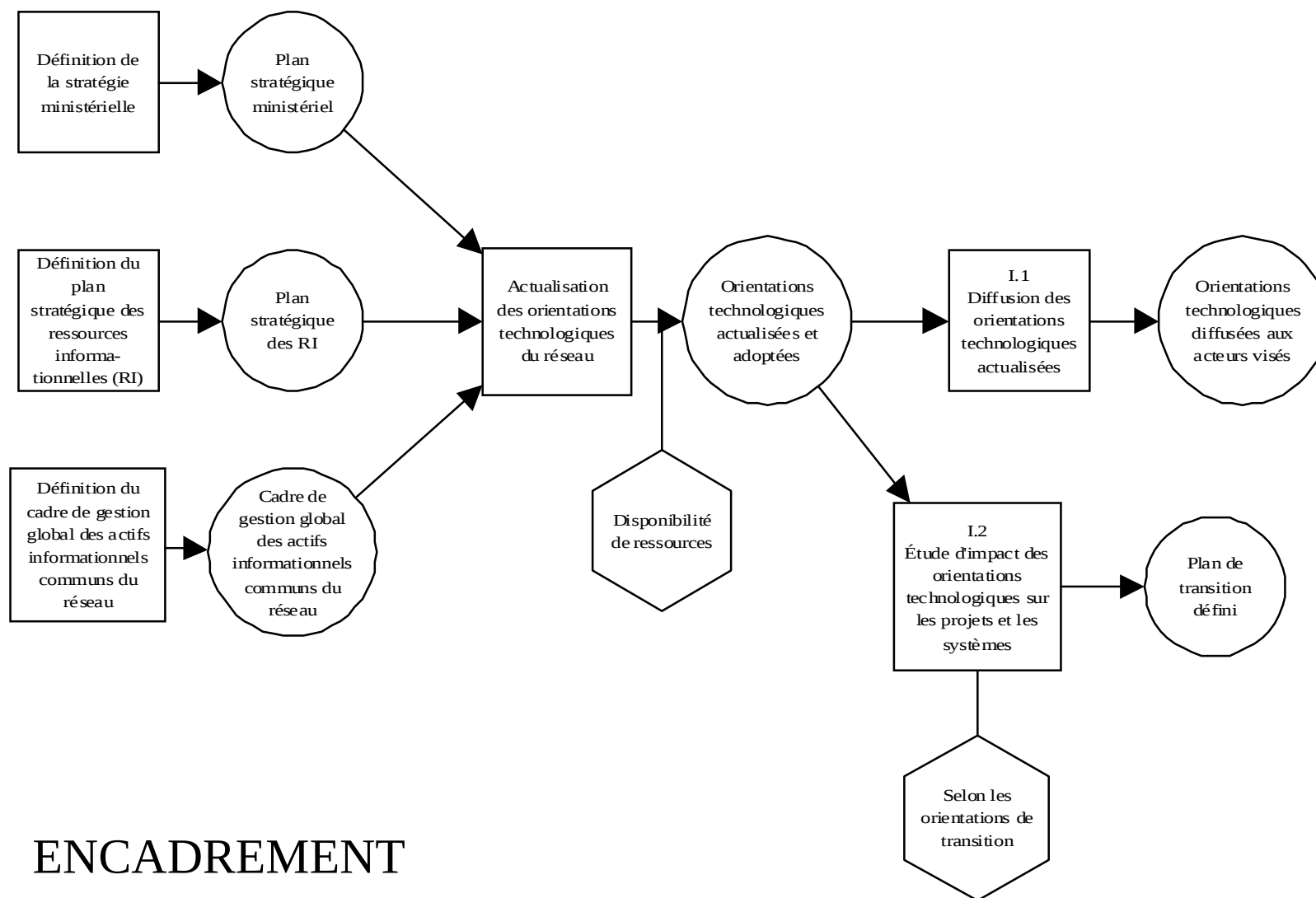
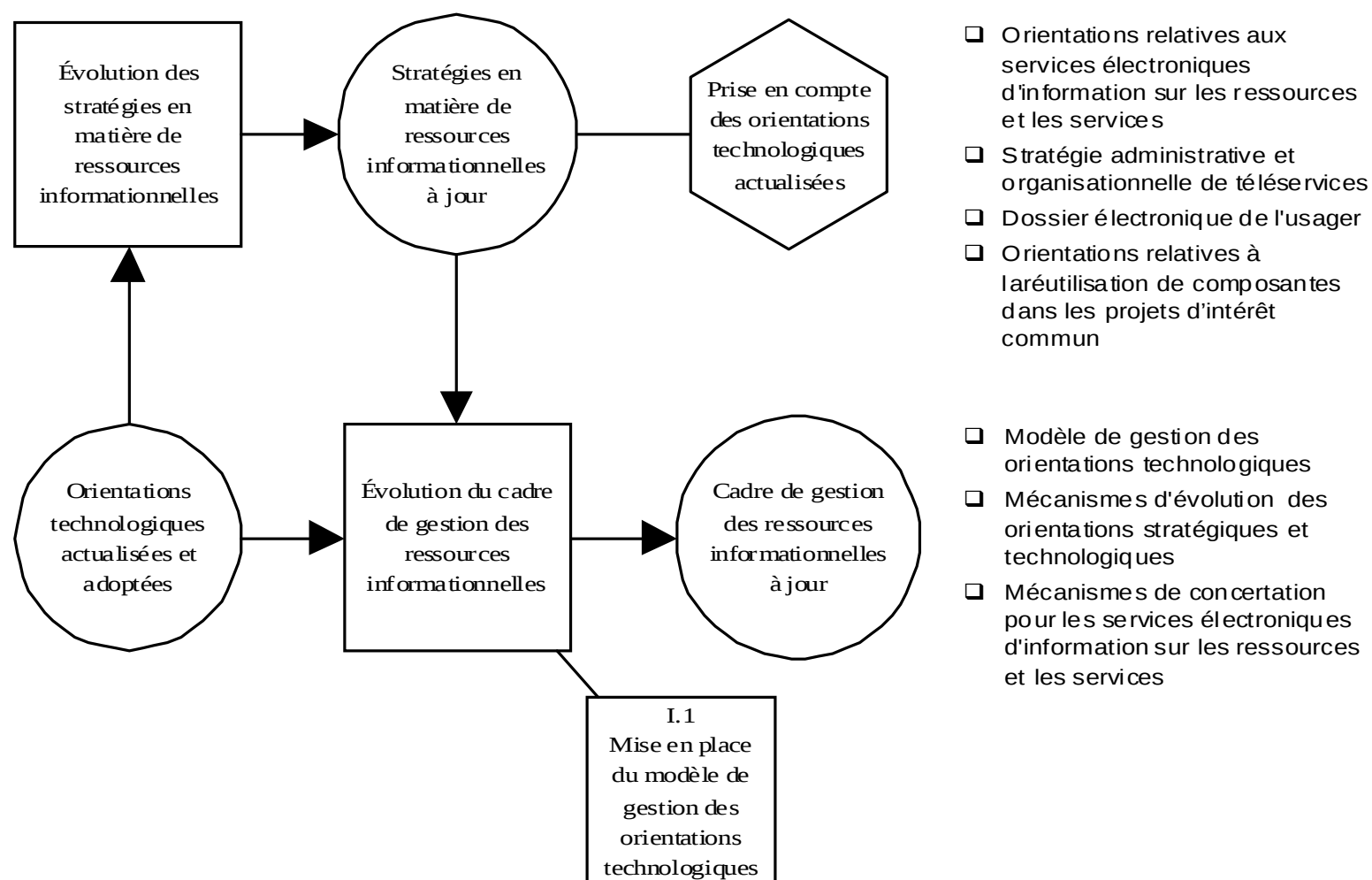


Diagramme A2.4 : Vue 2 de la mise en œuvre des orientations technologiques



ENCADREMENT

Diagramme A2.5 : Vue 3 de la mise en œuvre des orientations technologiques

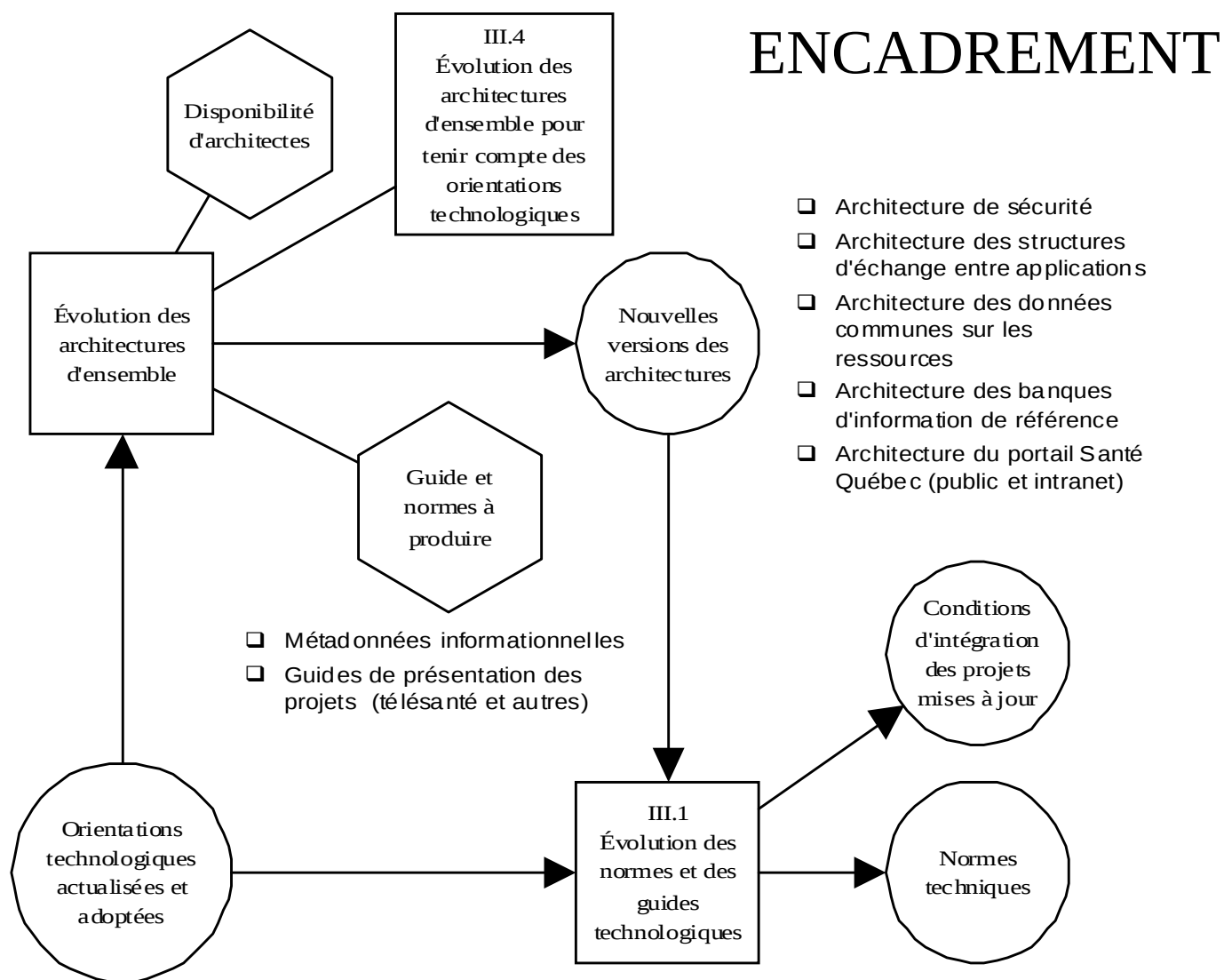


Diagramme A2.6 : Vue 4 de la mise en œuvre des orientations technologiques

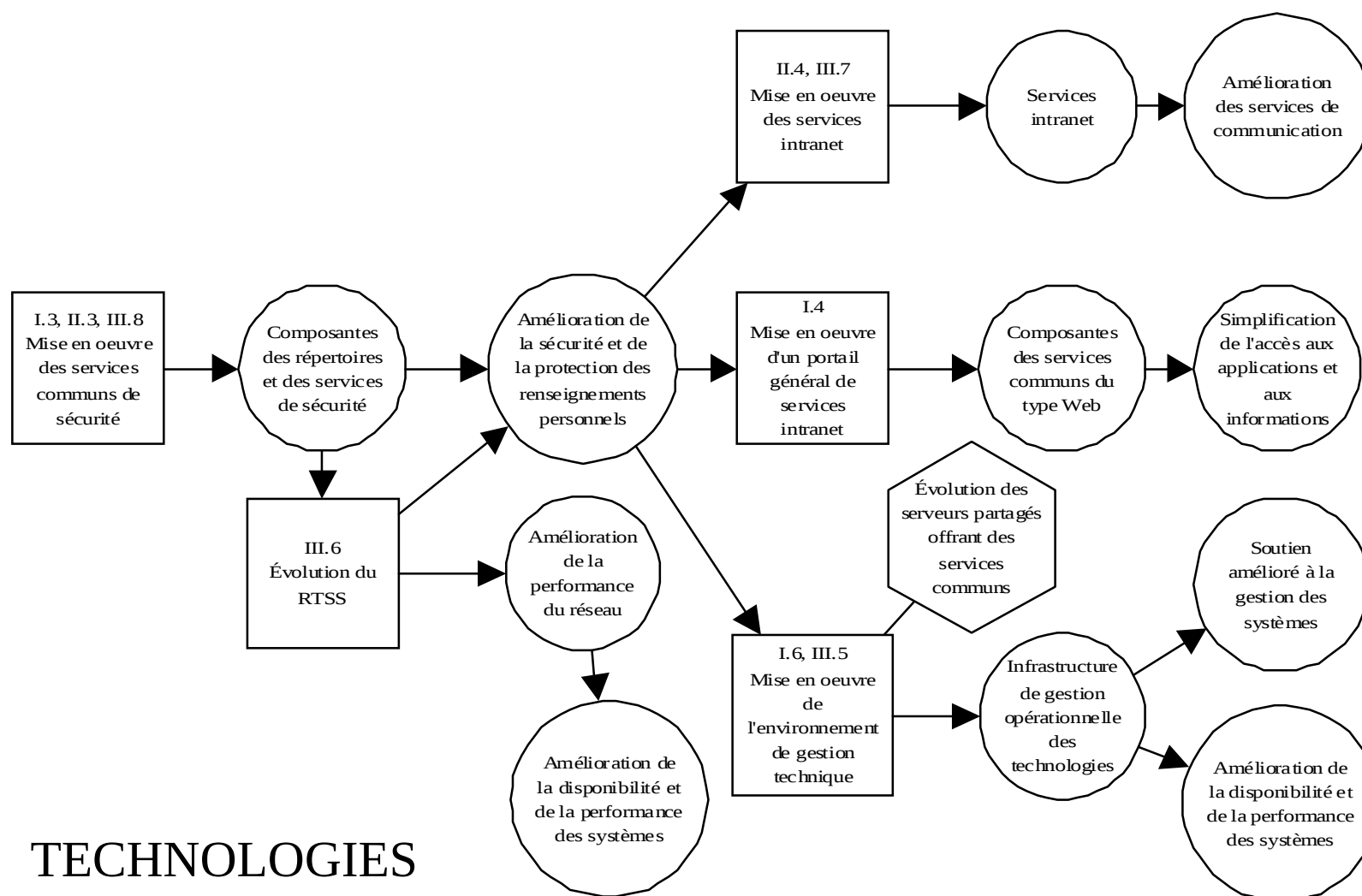


Diagramme A2.7 : Vue 5 de la mise en œuvre des orientations technologiques

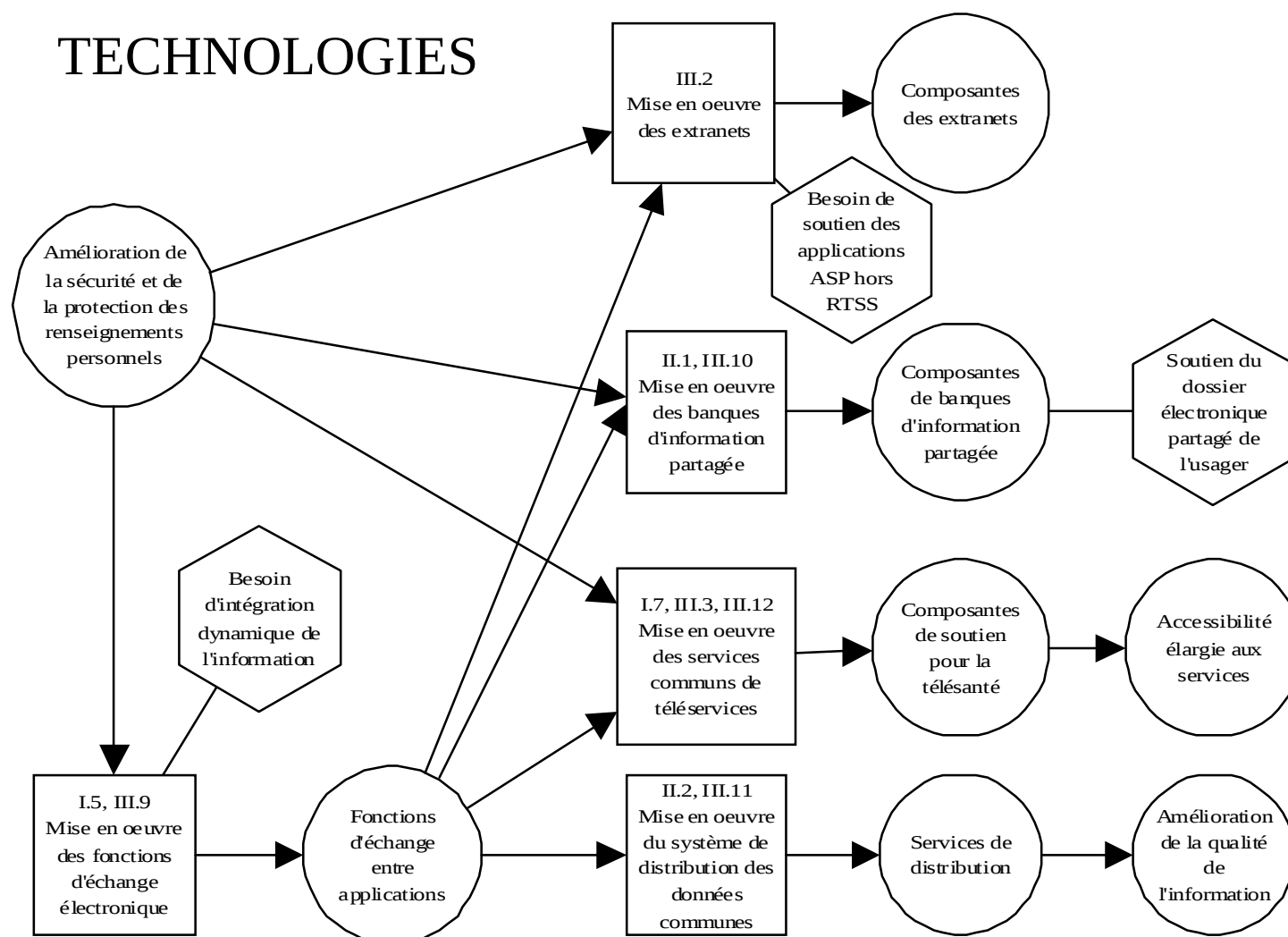


Diagramme A2.8 : Vue 6 de la mise en œuvre des orientations technologiques

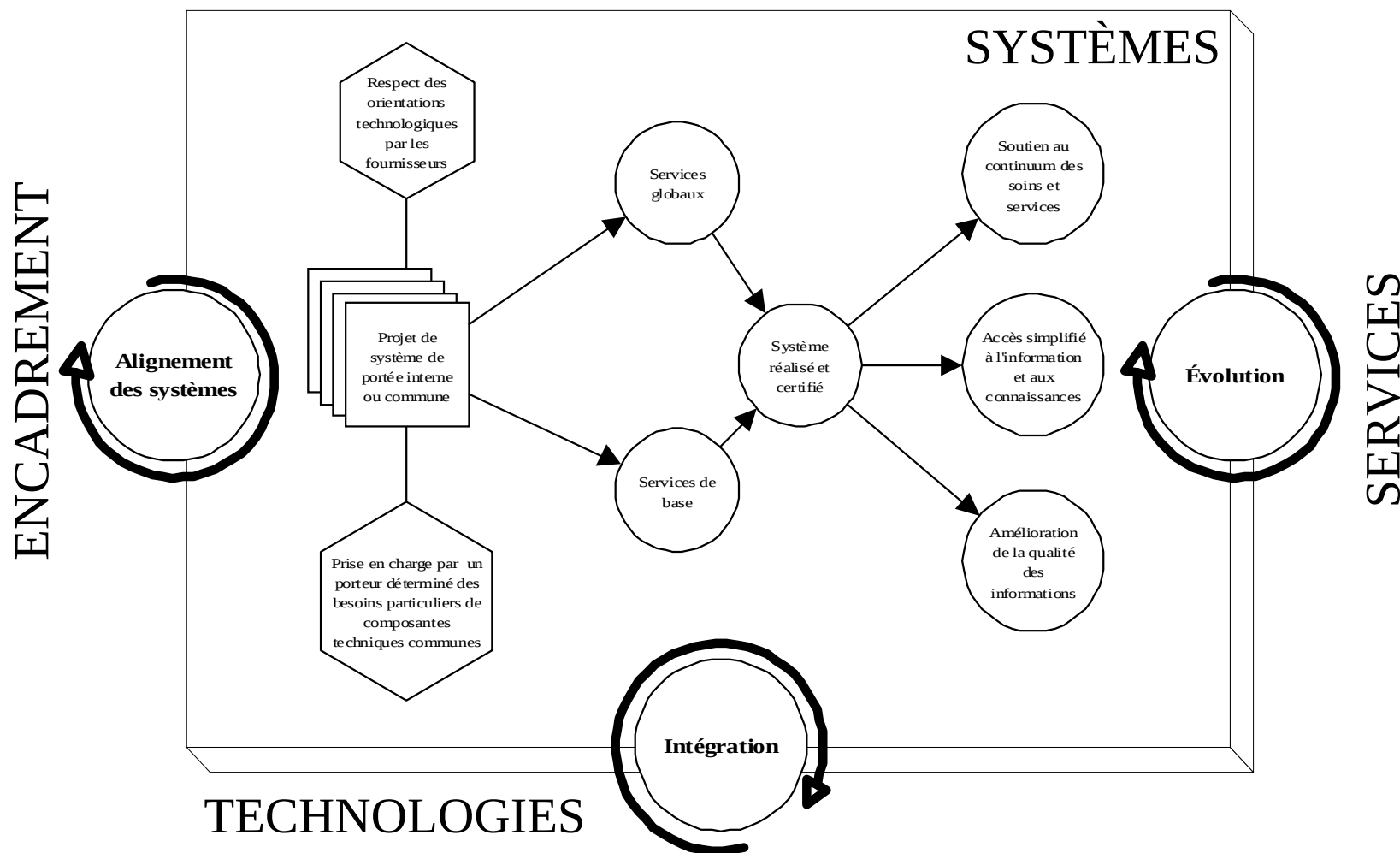
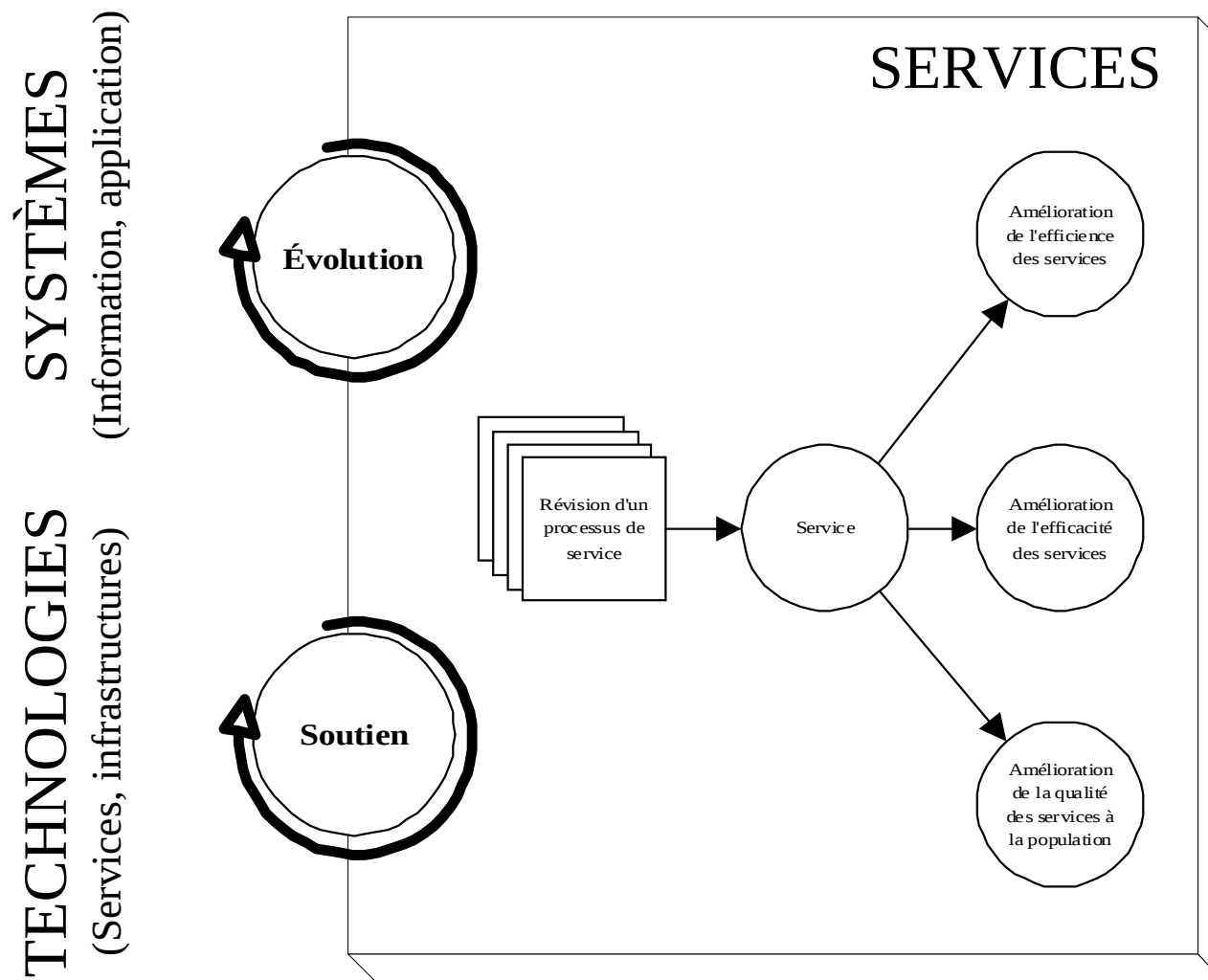


Diagramme A2.9 : Vue 7 de la mise en œuvre des orientations technologiques



ANNEXE 3 ÉCHÉANCIER DE PROJET

Diagramme A3.1 : Échéancier du projet

	2001				2002				2003				2004			
	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
Volet I - Livraison des éléments et des composantes de base																
I.1 Mise en place du modèle de gestion des orientations																
I.2 Étude d'impact des orientations sur les projets et les systèmes																
I.3 Mise en œuvre des services communs de sécurité																
I.4 Mise en œuvre d'un portail général de services intranet (choix des services)																
I.5 Mise en œuvre des fonctions d'échange électronique (agent d'intégration)																
I.6 Mise en œuvre de l'environnement de gestion technique																
I.7 Mise en œuvre des mécanismes de gestion des téléservices																
Volet II - Livraison des composantes à valeur ajoutée																
II.1 Mise en œuvre des banques d'information partagée																
II.2 Mise en œuvre du système de distribution des données de référence																
II.3 Ajout de services communs de sécurité																
II.4 Ajout de services communs intranet																
Volet III - Continuité et évolution																
III.1 Évolution des normes et des guides technologiques																
III.2 Mise en œuvre des extranets (passerelle RTSS - ASP)																
III.3 Expérimentation Web en télésanté																
III.4 Évolution des architectures technologiques d'ensemble																
III.5 Évolution des serveurs partagés offrant des services communs																
III.6 Évolution du RTSS																
III.7 Gestion des services intranet																
III.8 Coordination des services communs de sécurité																
III.9 Coordination des services d'échange électronique de données																
III.10 Coordination des banques d'information partagée																
III.11 Coordination de la distribution des données de référence																
III.12 Coordination des mécanismes de gestion des téléservices																

ANNEXE 4 - FICHES DE PROJET

PROJET I.1

Mise en place du modèle de gestion des orientations	
Description	• Adaptation de la structure organisationnelle, allocation des ressources nécessaires à la gestion des orientations technologiques et organisation des activités de communication.
Préalables	• Approbation des orientations technologiques. • Évolution du cadre de gestion des ressources informationnelles.
Principaux biens livrables	• Structure administrative fonctionnelle avec rôles, responsabilités et procédures. • Plan d'évolution des orientations technologiques. • Plan de communication.

PROJET I.2

Étude d'impact des orientations sur les projets et les systèmes	
Description	• Évaluation des conséquences des nouvelles orientations technologiques sur chaque projet et chaque système en activité. • Proposition d'un plan de transition pour chaque projet ou système.
Préalables	• Approbation des orientations technologiques. • Mise en place du modèle de gestion des orientations.
Principal bien livrable	• Plan de transition détaillé pour chaque système.

PROJET I.3**Mise en œuvre des services communs de sécurité**

Description	• Réalisation de l'architecture de la structure des répertoires ; analyse des différentes solutions et prise en compte de la capacité d'intégration et des conséquences sur l'utilisation de Windows 2000 et de la version 5 de Lotus Notes ainsi que de tout autre environnement qui identifie les utilisateurs (par exemple NOVELL). • Acquisition et implantation des technologies retenues. • Authentification en DMZ et implantation d'une structure LDAP incluant la gestion des rôles. • Gestion des répertoires de sécurité.
Préalable	• Synchronisation avec le projet « Évolution des serveurs partagés offrant des services communs ».
Principal bien livrable	• Infrastructure d'accès sécurisé aux serveurs.

PROJET I.4

Mise en œuvre d'un portail général de services intranet	
Description	• Analyse et élaboration de l'architecture des versions du portail intranet, ce qui inclut les choix de produits pour les serveurs Web et les services communs d'intranet. • Planification et gestion de la migration à la version R5 Web de Lotus Notes. • Arrimage à l'architecture des services (intranet et publics) du portail Santé Québec (projet DGI) lorsque celle-ci sera définie. • Réalisation des versions du portail intranet. • Déploiement de chaque version du portail intranet.
Préalable	• Synchronisation avec le projet « Mise en œuvre des services communs de sécurité ».
Principal bien livrable	• Portail intranet et services communs de l'intranet.

PROJET I.5**Mise en œuvre des fonctions d'échange électronique**

Description	• Adoption d'une approche de développement des architectures (considérer l'utilisation de UML). • Analyse et élaboration de l'architecture des fonctions d'échange électronique de données (ce qui inclut le choix de l'agent maître d'intégration multisystèmes). • Définition des mécanismes particuliers d'échange pour les banques d'information de référence (découpage territorial, établissements, classifications, et autres). • Réalisation et déploiement des fonctions d'échange électronique de données. • Structuration des échanges électroniques d'information (HL7, XML).
Préalable	• Synchronisation avec le projet « Mise en œuvre des services communs de sécurité ».
Principaux biens livrables	• Agent maître d'intégration multisystèmes. • Normes d'échanges multisystèmes (protocoles).

PROJET I.6

Mise en œuvre de l'environnement de gestion technique	
Description	• Révision du cadre de gestion des infrastructures communes du réseau et définition des besoins des TCR et du TCN en ce qui concerne les outils permettant d'assurer une gestion efficace des infrastructures technologiques communes du réseau socio sanitaire. • Mise en oeuvre des solutions de gestion retenues.
Préalable	• Aucun autre projet.
Principal bien livrable	• Processus et outils de gestion des infrastructures technologiques.

PROJET I.7

Mise en œuvre des mécanismes de gestion des téléservices	
Description	• Analyse et élaboration de l'architecture des mécanismes de gestion des téléservices permettant de doter le réseau de services communs pour l'utilisation des téléservices. • Réalisation des mécanismes de gestion des téléservices, y compris l'application de réservation et l'assemblage des composantes d'infrastructures (serveur, portier, ponts et passerelles). • Expérimentation. • Déploiement.
Préalable	• Synchronisation avec le projet d'évolution du RTSS (projet III.6).
Principal bien livrable	• Mécanismes de gestion des téléservices.

PROJET II.1

Mise en œuvre des banques d'information partagée	
Description	• Analyse et élaboration de l'architecture de la solution permettant l'intégration dynamique de l'information à partir d'une banque d'information partagée constituée de données de repérage et de localisation en utilisant un agent d'intégration multisystèmes (messagerie d'application et engin d'interface). • Réalisation d'une preuve de concept et expérimentation dans le cadre d'un projet pilote. • Révision de l'architecture.
Préalables	• Mise en œuvre des fonctions d'échange électronique. • Synchronisation avec le projet « Évolution des architectures d'ensemble ».
Principaux biens livrables	• Répertoire d'informations communes d'entreprise. • Banques d'informations partagées.

PROJET II.2

Mise en œuvre du système de distribution des données de référence	
Description	• Analyse et élaboration de l'architecture de la solution permettant la distribution des données de référence dans les banques d'information de référence des différents environnements. • Réalisation du système de distribution des données de référence. • Expérimentation. • Déploiement.
Préalables	• Mise en œuvre des fonctions d'échange électronique. • Synchronisation avec le projet « Évolution des architectures d'ensemble ».
Principal bien livrable	• Système de distribution des banques d'informations de référence.

PROJET II.3

Ajout de services communs de sécurité	
Description	• Poursuite de la mise en place des services communs de sécurité de la phase I (projet I.3) par le déploiement de fonctions additionnelles pour soutenir les projets porteurs.
Préalable	• Mise en œuvre des services communs de sécurité.
Principal bien livrable	• Services communs complémentaires de sécurité.

PROJET II.4

Ajout de services communs intranet	
Description	• Poursuite de la mise en place des services communs intranet de la livraison I (projet I.4) par le déploiement de nouvelles fonctions.
Préalable	• Mise en œuvre d'un portail général de services intranet.
Principal bien livrable	• Services communs additionnels de l'intranet.

PROJET III.1

Évolution des normes et des guides technologiques	
Description	• Réalisation dans la foulée des nouvelles orientations technologiques, des produits documentaires destinés aux différents acteurs (organisations du réseau, mandataires, fournisseurs privés). • Diffusion des orientations technologiques actualisées et autres produits documentaires.
Préalable	• Mise en place du modèle de gestion des orientations technologiques.
Principal bien livrable	• Diffusion des normes d'échange d'information. • Guides de présentation des projets. • Conditions d'intégration des projets.

PROJET III.2

Mise en œuvre des extranets	
Description	• Répond à des besoins particuliers des organisations du réseau concernant l'utilisation des services externes ou des services offerts en mode ASP par des fournisseurs privés.
Préalable	• Synchronisation avec le projet « Mise en œuvre des services communs de sécurité ».
Principal bien livrable	• Passerelles sécurisées entre le RTSS et les fournisseurs externes de services applicatifs.

PROJET III.3

Expérimentation Web en télésanté	
Description	• Expérimentation des technologies Web dans certains projets pilotes de télésanté afin d'améliorer l'accessibilité et de réduire les coûts. • Définition de normes propres à la télésanté en environnement Web à partir des résultats de l'expérimentation.
Préalable	• Sélection de projets en concertation avec la Table ministérielle en télésanté.
Principal bien livrable	• Rapport de preuve de concept.

PROJET III.4

Évolution des architectures technologiques d'ensemble	
Description	• Élaboration des architectures d'ensemble couvrant les aspects technologiques.
Préalable	• Approbation des orientations technologiques.
Principal bien livrable	• Volet technologique des architectures d'ensemble.

PROJET III.5

Évolution des serveurs partagés offrant des services communs	
Description	• Définition des plans de déploiement des infrastructures technologiques requises par les services communs et intégration de celles-ci dans l'architecture technologique du réseau (pour des considérations de performance, de gestion opérationnelle et de rentabilisation des infrastructures). • Définition et déploiement des serveurs de soutien pour les services communs.
Préalable	• Approbation des orientations technologiques.
Principal bien livrable	• Mise à niveau des serveurs partagés.

PROJET III.6

Évolution du RTSS	
Description	• Gestion des projets visant l'amélioration des performances et de la couverture du RTSS selon les orientations retenues (réseau local étendu, déhiérarchisation, ajout de nouveaux services). • Révision de l'organisation de la gestion des services du RTSS, y compris la veille technologique. • Amélioration de la gestion de la sécurité à l'aide de la structure des répertoires. • Vérification de la robustesse et de la continuité opérationnelle (redondance, plan de relève). • Réponse aux besoins particuliers des projets de téléservices. • Gestion des ententes contractuelles.
Préalable	• Mise en œuvre des services communs de sécurité.
Principaux biens livrables	• Documents d'étude de gestion du réseau. • Organisation de la gestion de réseau. • Mise en place d'infrastructures et d'outils.

PROJET III.7

Gestion des services intranet	
Description	• Maintien et évolution du portail intranet et des services communs de l'intranet.
Préalable	• Mise en œuvre du portail général de services intranet.
Principal bien livrable	• Rapport de gestion.

PROJET III.8

Coordination des services communs de sécurité	
Description	• Coordination des services communs de sécurité.
Préalable	• Mise en œuvre des services communs de sécurité.
Principaux biens livrables	• Approbations. • Rapports de suivi et d'évaluation.

PROJET III.9

Coordination des services d'échange électronique	
Description	• Coordination des fonctions d'échange électronique d'information.
Préalable	• Mise en œuvre des fonctions d'échange électronique.
Principaux biens livrables	• Approbations. • Rapports de suivi et d'évaluation.

PROJET III.10

Coordination des banques d'informations partagées	
Description	• Coordination de l'évolution des banques d'informations partagées.
Préalable	• Mise en œuvre des banques d'informations partagées.
Principaux biens livrables	• Approbations. • Rapports de suivi et d'évaluation.

PROJET III.11

Coordination du système de distribution des informations de référence	
Description	• Coordination de l'évolution du système de distribution des informations de référence.
Préalable	• Mise en œuvre du système de distribution des informations de référence.
Principaux biens livrables	• Approbations. • Rapports de suivi et d'évaluation.

PROJET III.12

Coordination des mécanismes de gestion des téléservices	
Description	• Coordination de l'évolution du système de gestion des téléservices, y compris leurs infrastructures.
Préalable	• Mise en œuvre du système de gestion des téléservices.
Principaux biens livrables	• Inventaire des équipements et des salles de téléservices. • Sessions de téléservices. • Rapports de suivi et d'évaluation.

BIBLIOGRAPHIE

Documents provenant d'organisations du secteur sociosanitaire québécois

« Bilan et perspectives : Projet Infocentres régionaux », Gouvernement du Québec, janvier 1998

« Bureau d'accueil et Centre de certification - Conditions d'intégration des applications », Gouvernement du Québec, novembre 2000

« Bureau d'accueil et Centre de certification : Document d'information sur le RTSS », Gouvernement du Québec, novembre 2000

« Bureau d'accueil et Centre de certification - Formulaire d'enregistrement du détenteur d'applications », Gouvernement du Québec, novembre 2000

« Cadre de référence pour la mise en place des Infocentres régionaux : éléments stratégiques et opérationnels », Gouvernement du Québec, février 1997

« Constat des technologies pour l'environnement de télémédecine », SOGIQUE, novembre 2000

« Salon annuel Informatique-Santé », Discours de M. François Turenne, sous-ministre associé, novembre 2000

« Contenu informationnel minimal commun des entrepôts régionaux de données - Priorités et périodes de conservation proposées », Groupe de travail sur les entrepôts régionaux de données

« Étude des besoins des Régies régionales concernant la mise sur pied des services d'entreposage et d'accès sécuritaire aux données prévus à la RAMQ », Gouvernement du Québec, avril 1998

« Exigences minimales en matière de sécurité pour le raccordement au RTSS : Guide d'information à l'intention des établissements du réseau de la santé et des services sociaux », Gouvernement du Québec, juillet 1999

« Guide d'accompagnement pour l'implantation des entrepôts régionaux de données », Projet des Infocentres régionaux, 4 mai 2000

« Implantation des Infocentres régionaux : Orientations et plan de travail », Gouvernement du Québec, novembre 1998

« Les solutions émergentes, Rapport et recommandations », Commission d'étude sur les services de santé et les services sociaux, Décembre 2000

« Lotus Notes : un investissement et un outil puissant pour le réseau sociosanitaire; perspective , valeur ajoutée et positionnement », SOGIQUE

« Les ressources informationnelles du réseau de la santé et des services sociaux: des orientations à faire évoluer », Gouvernement du Québec, septembre 2000

« Passerelle: RISQ/RTSS », Gouvernement du Québec

« Plan stratégique 2001-2004 du Ministère de la Santé et des Services sociaux », MSSS, avril 2001

« Portrait des banques de données disponibles à la Régie de l'assurance maladie du Québec », RAMQ, 30 novembre 2000

« Proposition conjointe Sogique-RAMQ de la solution administrative et technologique en vue de mettre en place et de fournir aux organisations du secteur sociosanitaire les services afférents à l'index patient provincial », Gouvernement du Québec, SOGIQUE, février 2000

« Proposition pour un modèle de gestion du consentement de l'utilisateur au partage des données de son Dossier Patient Partageable entre les points de service du système sociosanitaire québécois », SOGIQUE, décembre 1999

« Rapport de réflexion sur l'architecture cible », SOGIQUE, avril 1999

« Vision, orientations et stratégies de développement de la télésanté au Québec », Rapport préparé par la Table ministérielle en télésanté, version 2, MSSS, janvier 2001

Documents gouvernementaux (québécois et fédéral canadien)

« Architecture d'entreprise gouvernementale, Contexte, perspectives et architecture de haut niveau », Secrétariat du Conseil du Trésor du Québec version 3.0, décembre 2000

« Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale », Secrétariat du Conseil du Trésor du Québec, novembre 1999

« Architecture gouvernementale de la sécurité de l'information numérique (AGSIN) », Atelier de consultation, Secrétariat du Conseil du Trésor du Québec, avril 2001

« AGSIN - Arrimage en matière de sécurité – ICPG », Secrétariat du Conseil du Trésor du Québec, avril 2001

« AGSIN – Document de travail – BL3 » Secrétariat du Conseil du Trésor du Québec, mai 2001

« Cadre global de gestion sur la sécurité », Gouvernement du Québec, juillet 2000

« Initiative du Carnet de route ... Lancer le processus », Gouvernement fédéral canadien, mars 2000

« Initiatives internationales dans le secteur des dossiers médicaux électroniques : identification formelle et ICP », Gouvernement fédéral canadien, Septembre 1998

« National Health Infostructure, Blueprint and Tactical Plan », Gouvernement fédéral canadien, août/septembre 2000

« Vers les dossiers de santé électroniques », Ottawa, Santé Canada, Bureau de la santé et l'inforoute, janvier 2001

Autres documents de référence

« Clinical Documentation : Cornerstone of Effective Healthcare », Tutorials, GartnerGroup, février 2000

« Debunking CRM Myths in Healthcare », Tutorials, GartnerGroup, mai 2000

« 'Disidentification' in Support of HIPAA Privacy Constraints », Tutorials, GartnerGroup, janvier 2000

« Intelligent Matching: Meeting a Growing Need in IDSs », Tutorials, GartnerGroup, juin 1999

« Introducing the COMPARE Scale for HIPAA », COM-11-2070, GartnerGroup, juin 2000

« PDAs + CSR = Assault on Physicians' Input Bottleneck », Technology, GartnerGroup, juin 2000

« Six Criteria for Evaluating HCO E-Marketplace Solutions », Strategic Planning, GartnerGroup, juillet 2000

« Standards: An Important Key Issue for E-Health », Key Issues, GartnerGroup, décembre 1999

« From Text to Facts: CMV Functions », Tutorials, GartnerGroup, décembre 2000

« Management and Process: Keys to BI Application Success », Tactical Guidelines, GartnerGroup, juillet 2000

« New Options for MCO Strategic Data Management », Strategic Planning, GartnerGroup, juin 1999

« Simulation and Animation Technology for Healthcare », Technology, GartnerGroup, août 2000

- « Statistical Packages: Selection Criteria for Analytic Power », Decision Framework, GartnerGroup, mai 1999
- « Value vs. the Cost of Data », Tactical Guidelines, GartnerGroup, avril 2000
- « Canadian Health Care IT Market: Trends and Directions », Perspective, GartnerGroup, 1999
- « Data Warehouses for Strategic Architecture in Healthcare », Strategic Planning, GartnerGroup, août 1998
- « Gartner's Vision for Healthcare: The Next 10 Years », Strategic Analysis Report, GartnerGroup, janvier 2001
- « Healthcare Information Systems: Perspective », Technology Overview, GartnerGroup, avril 2000
- « Medical Management: Moving Fast », Strategic Analysis Report, GartnerGroup, septembre 1999
- « The Information Expert: New Capabilities for MCOs », Tactical Guidelines, GartnerGroup, septembre 1999
- « How to Choose and Implement Enterprise Master Person Indexes », Strategic Analysis Report, GartnerGroup, août 2000
- « IB Selection Criteria: Technical Adapter Requirements », Technology, GartnerGroup, janvier 2001
- « IB Selection: Healthcare Message Transport Requirements », Technology, GartnerGroup, décembre 2000
- « The Enhancement of Healthcare Through Subportals », Tutorials, GartnerGroup, mai 1999
- « ebXML: Some Hope for Coordinating B2B XML in Healthcare », Tutorials, GartnerGroup, septembre 2000
- « Healthcare's HL7 Messaging Format Sets a Standard », Technology, GartnerGroup, avril 1999
- « HL7 Demonstrates Synergy Between XML and UML », Technology, GartnerGroup, mai 2000
- « HL7 vs. XML Around the World », Select Q&A, GartnerGroup, janvier 2001
- « XML for HCOs: Not Soup Yet », Strategic Planning, GartnerGroup, novembre 1999

- « Integrating the Healthcare Enterprise - IHE Technical Framework Year 3 », HIMSS and RSNA, 2001
- « Assessment of Two Telemedicine Projects: Economic Issues Revisited », Provost L., Fortin J.P., Banville C., Morisset J., Kirouac S., Hubert F., février 1999
- « Common Warehouse Metadata », Technical Overview, Oracle Corporation
- « Cost of Missing, Inaccurate and Inconsistent Customer Data », Tactical Guidelines, GartnerGroup, septembre 2000
- « Data Warehouses for Strategic Architecture in Healthcare », Strategic Planning, GartnerGroup, août 1998
- « HL7 Patient Record Architecture », Liora Alschuler, Christopher Almy
- « Healthcare Data Center Consolidation: The Myths », Key Issue Analysis, GartnerGroup, août 1997
- « Le télédiagnostic en cardiologie pédiatrique et en radiologie : Évaluation de deux projets pilotes (Version abrégée), CEFRIO, mai 1998
- « Message Development Framework », Health Level Seven, Inc., 1999
- « Management and Process: Keys to BI Application Success », Tactical Guidelines, GartnerGroup, juillet 2000
- « MedicalConnection:DicomObjects », <http://www.medicalconnections.co.uk/html/dicomobjects.html>
- « MedWeb : DICOM Cube », MedWeb, 1998
- « MedWeb : Multipublishing DICOM Workstation », MedWeb, 1998
- « HL7 Reference Information Model », Health Level Seven, 2000
- « XML in healthcare », Joachim Dudeck,
- « XML in healthcare computing :the potential », Sean Brennan
- « XML/EDI Explained », Technology, GartnerGroup, juin 1999
- « CRM 'Glossary' for Managed Care Organizations », Tutorials, GartnerGroup, février 2000
- « What Is My Industry Doing With XML? », COM-10-0137, GartnerGroup, janvier 2000

- « Challenges of “Hub and Spoke” Data Warehouse Topology », Strategic Planning, GartnerGroup, mars 1999
- « CRM Analytics and Personalization », Strategic Analysis Report, GartnerGroup, février 2001
- « Data Mining and Advanced Analytics: Extended Coverage », Key Issues, GartnerGroup, novembre 1999
- « Data Mining Applications of the Next Decade », Technology, GartnerGroup, juin 1999
- « Data Mining Projects: Frequently Asked Questions », Select Q&A, GartnerGroup, décembre 1999
- « Data Transformation: Key to Information Sharing », Strategic Analysis Report, GartnerGroup, septembre 1998
- « Data Warehouse Administration », Data Warehouse Network and SAS, 1997
- « Data Warehouse, Data Mining and Business Intelligence: The Hype Stops Here », Strategic Analysis Report, GartnerGroup, octobre 1996
- « Data Warehousing Technical Metadata Management Issues », Tactical Guidelines, GartnerGroup, janvier 2000
- « Impact of an XML repository in development of XML messages », University of Giessen
- « Key Issues: Data Warehouse Operations and Manageability », Key Issues, GartnerGroup, janvier 1999
- « Metadata Management Alternatives for DWs and Data Marts », Decision Framework, GartnerGroup, février 1999
- « CUseeMe Conference Server », Technical Overview, CUseeMe Networks
- « Netmeeting (extraits de NetMeeting resource kit) », Microsoft
- « CWM: A Model-based Architecture For Data Warehouse Interchange », Doug Tolbert
- « Building a guaranteed, quality-of-service (QoS) infrastructure for emerging business applications. », VIPswitch, novembre 1999
- « The Information Security Market Space Invasion Has Begun », GartnerAdvisory, Reserch Note Markets, Dang Van Mien, 17 février 2000

« CUseeMe Web :The Next Revolution of Internet Communications », CUseeMe Networks

« Deploying H.323 Conferencing on Your IP Network », CUseeMe Networks

« Workflow Standards : An Update », GartnerAdvisory, Strategic Analysis Report, Casonato, R., 14 juillet 1999

LEXIQUE

AEG (Architecture d'entreprise gouvernementale)	Projet réalisé par le Secrétariat du Conseil du trésor.
AGSIN (Architecture globale de sécurité de l'informatique numérique)	Projet réalisé par le Secrétariat du Conseil du trésor.
ANSI (American National Standard Institute)	Organisme de normalisation américain qui collabore avec l'ISO.
API (Application Programming Interface)	Interface utilisée par un programme informatique pour obtenir un service d'un autre programme informatique.
ASP (Application Service Provider)	Mode d'exploitation qui consiste à installer les progiciels sur les infrastructures d'un fournisseur (nécessairement à l'extérieur du RTSS) qui vend ces mêmes services à plusieurs organisations afin de rentabiliser ses activités.
Attestation de conformité	Document émis par le Bureau d'accueil des applications du MSSS attestant de la conformité d'une version d'un logiciel aux conditions d'intégration au RTSS.
CAIQ	Commission d'accès à l'information du Québec.
CDA (Clinical Document Architecture)	Standard XML défini par HL7 pour l'échange de documents électroniques de nature clinique et médico-administrative.
Chaîne de résultats	Technique de modélisation définie dans la méthode Station DMR Résultats ^{MC} du Macroscop ^{MC} de DMR conseil. Dans les orientations technologiques, cette technique a servi à l'élaboration du plan de mise en œuvre.
CIM (Common Information Model)	Modèle d'information standard pour la gestion de systèmes et de réseaux. Le modèle CIM est soutenu par le DMTF, un organisme de normalisation réunissant de nombreux fournisseurs de technologies.
CMIP (Common Management Information Protocol)	Protocole de gestion de réseau défini par l'ISO.
CNPRPS	Comité national sur la protection des renseignements personnels et sur la sécurité.
COM/DCOM (Component Object Model/Distributed Component Object Model)	Architectures de Microsoft pour la gestion et l'utilisation d'objets par des programmes informatiques.
CORBA (Common Object Request Broker Architecture)	Architecture définie par l'OMG pour la gestion et l'utilisation d'objets par des programmes informatiques.
CSST	Commission de la santé et de la sécurité du travail.

DEN (Directory Enabled Architecture)	Architecture définie par le DMTF pour une gestion de systèmes et de réseaux basée sur un répertoire.
DMTF (Distributed Management Task Force)	Organisme de normalisation américain réunissant de nombreux fournisseurs de technologies matérielles et logicielles.
DES (Dossier de santé électronique)	Tel que défini par le Bureau de la santé et de l'inforoute du gouvernement canadien, segment d'information sur la santé et le bien-être d'une personne, lequel dossier est accessible à partir d'un système au sein d'un réseau électronique.
ETC	Équivalent temps complet.
Guide de certification	Document émis par le Bureau d'accueil des applications du MSSS, qui concerne la certification et définit notamment les conditions d'intégration au RTSS.
HL7 (Health Level 7)	Organisme de normalisation américain accrédité par l'ANSI, qui définit des standards d'échange pour les données cliniques et administratives. De nombreux pays en font partie.
HTML (HyperText Markup Language)	Langage standard d'affichage Web.
HTTP (HyperText Transfer Protocol)	Langage standard d'échange avec un serveur Web. Il existe aussi une version sécurisée appelée HTTPS, ou HyperText Transfer Protocol Secure.
ICP	Infrastructure à clés publiques.
IEEE (Institute of Electrical and Electronics Engineers)	Organisme de normalisation américain reconnu par l'ISO.
Intervenant	Personne qui participe à la prestation des services aux usagers du réseau de la santé et des services sociaux.
IOM (Institute of Medicine)	Organisme privé américain réunissant un grand nombre d'universités et de centres hospitaliers. L'IOM réalise entre autres des études pour des agences du gouvernement fédéral américain. Dans le cadre des orientations technologiques, les caractéristiques définies par l'IOM servent de référence pour les dossiers de santé électroniques des usagers.
ISO (International Organization for Standardization)	Organisation de normalisation internationale dans différents secteurs d'activité, dont les technologies de l'information et des communications.
Internet Society	Organisme américain de normalisation des technologies d'Internet.

ITIL (Information Technology Infrastructure Library)	Ensemble de normes de processus de gestion des systèmes et des réseaux défini par le British Standard Institute (BSI). Ces normes ont été soumises à l'ISO.
JDBC (Java Database Connectivity)	API pour l'accès à des bases de données en langage JAVA.
LDAP (Lightweight Directory Access Protocol)	Protocole standard d'accès à un répertoire de ressources.
Métadonnées	Description des données des systèmes. On distingue les métadonnées informationnelles des métadonnées techniques. Les premières permettent aux utilisateurs de connaître la définition des données et le contexte de leur saisie. Quant aux métadonnées techniques, elles sont utilisées par les systèmes pour structurer l'information des banques de données.
MIME (Multipurpose Internet Mail Extension)	Extensions normalisées par l'Internet Society pour le courrier électronique.
MJQ	Ministère de la Justice du Québec.
MOM (Message Oriented Middleware)	Nom générique désignant des logiciels d'échange de messages entre des applications.
PDA (Personal Digital Assistant)	Appareil numérique de poche pouvant fonctionner de façon autonome ou avec communication sans fil.
PES	Prestation électronique de services.
POP (Post Office Protocol)	Protocole normalisé par l'Internet Society pour le courrier électronique.
Produit documentaire	Dans le cadre des orientations technologiques, il s'agit d'un document d'orientation, d'architecture, de présentation de normes techniques ou de pratiques en technologie.
Réseau sociosanitaire	L'expression <i>réseau sociosanitaire</i> renvoie aux organisations publiques du secteur de la santé et des services sociaux responsables de la gestion ou de la prestation des soins et des services. Le réseau sociosanitaire inclut les établissements, les régies régionales, l'OPHQ et le MSSS.
Ressources informationnelles	Les ressources informationnelles se définissent comme toutes les ressources qui constituent les systèmes d'information du réseau sociosanitaire, c'est-à-dire les données, les applications (logiciels sur mesure ou commerciaux) ainsi que les technologies (infrastructures logicielles et matérielles).
RETEM	Réseau de télécommunications multimédia en projet à la DGT du SCT, lequel réseau remplacera le RICIB.

RICIB (Réseau intégré de communications informatiques et bureautiques)	Réseau de télécommunications géré par la DGT du SCT, lequel réseau est utilisé par la majorité des ministères et organismes du gouvernement du Québec.
RISQ (Réseau Internet scientifique du Québec)	Réseau de télécommunications du secteur de l'éducation, lequel réseau est utilisé notamment par les institutions d'enseignement et les universités québécoises.
SAAQ	Société de l'assurance automobile du Québec.
SCT	Secrétariat du Conseil du trésor.
Secteur sociosanitaire	L'expression <i>secteur sociosanitaire</i> est utilisée pour désigner l'ensemble des organisations publiques et privées du secteur d'activité ayant trait aux services de santé et aux services sociaux. Le secteur sociosanitaire inclut le réseau sociosanitaire, la RAMQ, les cliniques médicales, les laboratoires, etc.
SGBD	Système de gestion de bases de données.
SMS (System Management Server)	Logiciel de Microsoft pour la gestion de systèmes.
SNMP (Simple Network Management Protocol)	Protocole de gestion de réseau de l'architecture TCP/IP.
SOAP (Simple Object Access Protocol)	Protocole d'échange d'information basé sur XML.
TCP/IP (Transmission Control Protocol/Internet Protocol)	Architecture de réseau normalisée par l'Internet Society.
Téléservices	Les téléservices désignent les services de santé et les services sociaux, l'information sur la santé et le bien-être, les échanges audiovisuels à des fins éducatives, administratives et de recherche, l'échange et le traitement de données psychosociales et clinico-administratives effectués à distance au moyen d'une télécommunication.
UDDI (Universal Description, Discovery and Integration)	Spécification d'enregistrement de services Web pour en faciliter la recherche et l'intégration dans un réseau d'échanges. Les services UDDI utilisent le protocole SOAP.
Usager	Personne qui utilise les services offerts par les établissements du réseau sociosanitaire.
Utilisateur	Personne qui utilise directement un moyen informatique, comme un poste de travail.
W3C (World Wide Web Consortium)	Organisme de normalisation des technologies du Web.
WMI (Windows Management Interface)	Interface standard de Microsoft pour les outils de gestion de système.
XML (Extensible Markup Language)	Langage normalisé par le W3C pour la structuration du contenu de documents en vue de leur échange électronique.

