| Bâtissons.
| Ensemble.
LESISS

MANIFESTE

pour une sécurité des systèmes d'information de santé enfin efficiente

Pour en finir avec une « Sécurité cache-sexe »

MANIFESTE SECURITÉ

PROLÉGOMÈNES - **Le pouvoir de dire non …**

« *Victime d'un pirate informatique, le site internet www.cotes-darmor.gouv.fr est hors-service depuis le 24 juillet 2011* ». Cet exemple éclaire de manière plaisante les déclarations de Patrick Pailloux – Directeur général de l'ANSSI - lors des 6èmes Assises de la sécurité à Monaco, en octobre 2011. Prônant des « règles d'hygiène informatique élémentaire », l'intéressé devait poursuivre son réquisitoire en dénonçant la « sécurité cache-sexe » en vigueur dans bien des secteurs, fustigeant une situation connue de longue date.

A l'heure du e-village mondial, la France n'a pas l'exclusivité – quand elles existent - des politiques de sécurité inadaptées ou défaillantes. Pour autant, à l'aune de l'ampleur des moyens déployés, le bilan crûment évoqué dans la capitale monégasque apparaît bien préoccupant. A croire que ces dernières années, c'est surtout le sable qui a été abondamment arrosé.

Conséquence de ces lacunes ? Aucune entreprise ou institution n'est aujourd'hui à l'abri d'incidents, voire d'accidents ou même de cyber-attaques. Les exemples ne manquent pas à cet égard, d'Areva aux services de Bercy en passant par l'entreprise Sony. Sans oublier le système de pilotage des drones de l'armée américaine infectés. D'évidence, en matière de sécurité les marges d'amélioration sont importantes, et avec l'avènement d'un « Cloud » ubiquitaire mieux vaudrait rapidement prévoir une stratégie adaptée pour juguler les risques et défaillances associés.

A ce sujet, S'il est un domaine technologique où la sécurité et la confidentialité des données – en particulier nominatives - est fondamental, c'est bien celui de la santé. Patients et professionnels (que ces derniers exercent en médecine de ville ou en établissements) sont d'ailleurs arc-boutés sur le sujet. Les uns craignant de voir leur données utilisées à ces fins inappropriées, voire inavouables. Les autres parce qu'ils goûtent modérément la perspective de séjourner, en cas de perte, de vol ou de détournement desdites données qu'ils gèrent pour le compte d'autrui, dans le bureau de quelque procureur en mal de renommée.

S'agissant donc de l'appropriation d'un outil pourtant désormais indispensable pour le pays, l'absence de politique de sécurité adaptée dans le domaine des technologies d'information de santé renforce – légitimement diront certains - auprès des patients et de praticiens leur pouvoir de dire non.

C'est dans ce contexte que le dixième anniversaire de la loi Le 4 mars 2002 sera célébré au printemps prochain. Pour mémoire cette loi, dite de « Démocratie sanitaire » et à l'initiative du ministre Kouchner, ouvrait de nouveaux droits au patient. Entres autre, celui de disposer de ses données de santé, la sécurité et la confidentialité des ces dernières étant garanties par un éventail de dispositions remarquables, tant aux plans réglementaire que technique. 10 ans plus tard, où en sommes-nous aujourd'hui ?

Pour être clair, le bilan ne porte pas exactement à l'euphorie. Les étagères sont remplies d'outils conçus par les technostructures de l'Etat, régalien dans le domaine de la protection des données de nos concitoyens, qu'une approche décrétale et sans véritable lien avec les usages du terrain rend toutefois non utilisées car inutilisables. Moyennant quoi, en matière de politique de sécurité en santé la principale accélération observée jusqu'à une période récente a essentiellement été celle de l'immobilisme.

A qui la faute ? Il ne s'agit naturellement pas de dresser un réquisitoire, puisque la responsabilité de cette situation délétère échoit à tout le monde, et à personne. Il est vrai qu'en matière de sécurité les postes de travail des professionnels abritent un invraisemblable empilement de programmes hétéroclites imposés par les technostructures. Il est tout aussi vrai qu'en médecine de ville ou dans la sphère hospitalière, une joyeuse absence de politique claire de sécurité perdure. **Mais la question pertinente à poser, plutôt que de rechercher de putatifs boucs émissaires, est plutôt celle-ci : comment faire pour sortir le sujet de l'ornière?**

A cet égard, le mythe de l'homme providentiel relevant d'ancestrales chimères, c'est plutôt vers la mutualisation des bonnes volontés expertes qu'il faut à l'évidence se tourner pour trouver les solutions adaptées. C'est donc au carrefour des exigences régaliennes énoncées par l'Etat, des référentiels élaborés par ses opérateurs, et de la concertation avec les utilisateurs et leurs prestataires autour de leurs réels usages et besoins qu'll faut rechercher les solutions. En n'oubliant pas, une fois les choix validés et acceptés, de les assaisonner d'un doigt d'incitations financières, mâtiné d'un zeste de coercitions réglementaires. Le programme "Hôpital numérique" constitue de ce point de vue un levier intéressant qu'il conviendra d'activer au mieux.

S'agissant des ressources financières à la hauteur des enjeux de sécurité, la situation du moment ne se prête guère aux confortables marges de manœuvre budgétaires. Pour autant, une infime partie des améliorations de gestion réalisés grâce aux technologies de l'information sur les 13% des richesses nationales consacrées à la santé et au médico-social peut être raisonnablement envisagée. Pour preuve, la DGOS vient par une simple revue de fonctionnement d'identifier, dans le domaine des seules "inadéquations" hospitalières, un gisement d'économie de 2 milliards d'euro !

En résumé, si en matière de politique de sécurité des technologies d'information de santé la situation est grave, elle n'est pas désespérée. Le présent Manifeste est là pour en témoigner, qui constitue l'amorce de quote-part des industriels spécialisés dans la lutte contre les risques d'erreurs et d'eventuelles fraudes.

Sauf à accepter l'idée du maintien de la France au titre de leader européen du dossier de santé papier, il est urgent d'agir sur le levier des technologies d'information. Afin de donner enfin aux principaux acteurs concernés – professionnels concernés et citoyens – le pouvoir de dire OUI.

MANIFESTE SECURITÉ

COMMENT EST NÉE L'IDÉE D'UN MANIFESTE

A l'issue de la création de la Commission Sécurité de LESISS, l'une des premières initiaitives a été d'organiser une réunion de présentation du projet de Manifeste devant un parterre de personnalités. Cet événement, qui s'était tenu le 29 juin 2010 avait réuni une quarantaine d'invités : RSSI hospitaliers et du Ministère de la santé, industriels, Conseil de l'Ordre, Agences de l'Etat. L'intérêt suscité avait conduit à pousser le projet.

MANIFESTE SECURITÉ

SOMMAIRE

(Ce document peut être téléchargé (http://www.lesiss.org/445_p_26508/2011-10-manifeste-securite.html)

MANIFESTE SECURITÉ

MANIFESTE SECURITÉ

LE MANIFESTE RESUMÉ EN CINQ POINTS

1 Au sein du concert mondial les pays les plus avancés l'ont bien compris : dans un contexte démographique préoccupant amplifié par une crise économique durablement installée, les TIC pour la santé, le médico-social et l'aide à l'autonomie ne peuvent plus être perçues comme un simple artifice technologique ou un poste de coûts. Elles apparaissent au contraire comme un puissant levier pour améliorer les organisations, pour mieux répartir les efforts budgétaires, et surtout pour renouer avec un dispositif sanitaire équitable pour l'ensemble des citoyens ;

2 L'indispensable montée en puissance des TIC suppose leur appropriation par les deux principaux acteurs concernés : professionnels de la santé et patients-citoyens. Or, la réussite de cet écosystème technologique est fortement tributaire de la qualité de l'espace de confiance qui y règne. L'absence de politique de sécurité, ou une politique de sécurité inadaptée conduisent inéluctablement les utilisateurs potentiels à exercer leur droit de retrait. Ce pouvoir de dire non, qui perdure depuis près de vingt ans, fait désormais de la France l'un des leaders mondiaux des dossiers de santé papier ;

3 L'absence ou l'inadéquation d'une politique de sécurité résultent le plus souvent d'un manque de concertation et de coordination entre les différents acteurs concernés : législateur, technostructures de l'Etat, professionnels de la santé, patients. En l'absence de confrontation des demandes et possibilités, l'approche décrétale prend classiquement le dessus qui, non seulement se heurte aux résistances, mais qui dans un domaine aussi rapidement évolutif que celui des technologies de communication, est intrinsèquement condamné à l'obsolescence ;

4 Contrairement à l'idée généralement reçue, en matière de TIC les risques les plus importants sont rarement de nature technique, mais se combinent avec le facteur comportemental. Le domaine de la santé ne fait pas exception à cette règle, qui se traduit par des résistances aux procédures – d'autant plus lorsqu'elles émanent de technostructures ignorant les réalités du terrain. Le refus ou le contournement des règles conduit alors, indépendamment de la qualité des choix technologiques, à des dysfonctionnements aux conséquences parfois tragiques ;

5 Notre pays dispose heureusement d'atouts importants pour mettre un terme à plus de 20 ans de « sécurité cache-sexe ». Le savoir-faire technologique doit toutefois se combiner avec une approche plus concertée de la résolution des obstacles à lever, associé à une approche volontariste dans la mise en œuvre. Les investissements doivent en outre être à la hauteur des enjeux, les moyens à mobiliser étant largement compensés par les gisements d amélioration des organisations que les technologies d'information de santé adaptées peuvent générer.

MANIFESTE SECURITÉ

AVANT PROPOS

LESISS, SA VIE, SON ŒUVRE

La Fédération LESISS (Les Entreprises des Systèmes d'Information Sanitaires et Sociaux) est une jeune organisation créée en 2005 par une vingtaine d'entrepreneurs spécialisés. Elle s'est depuis fortement renforcée puisque plus de 120 entreprises, tant des domaines de la santé, du médico-social que de l'aide à l'autonomie, en assurent aujourd'hui la croissance rapide.

Trois atouts en font un acteur atypique : une expertise multipolaire, une extrême réactivité, et une absence de complexes. En résumé, LESISS est plus une Organisation 2.0 qu'une institution ISO 9000.

LA « COMMISSION SÉCURITÉ DES SYSTEMES D'INFORMATION DE SANTÉ »

Cette Commission (ComSec) a été créée en 2010 pour traiter, sous l'angle de vue de ses membres industriels et en collaboration avec les autres acteurs des domaines de la Santé et du Médico-social qui le souhaitent, le **vecteur déterminant que constitue l'espace de confiance** sans lequel les systèmes d'information de santé ne pourront monter en puissance.

INTERÊT D'UN MANIFESTE SUR LA SECURITÉ

RAPPEL SÉMANTIQUE

Par définition, un manifeste annonce une **prise de position** et un **programme d'action** en vue d'une **avancée significative** dans un domaine. Dans le présent document, c'est de **gouvernance** de la Sécurité des Systèmes d'Information de Santé, des données médicales et socio-médicales dont il est question.

LES FAILLES DE SÉCURITÉ NE SONT PAS TOUJOURS LÀ OU ELLES SONT ATTENDUES

Le maillon le plus faible d'une chaîne de confiance dans le domaine des hautes technologies résulte souvent des facteurs humain et comportemental. Trois exemples choisis parmi les innombrables cas d'école illustrent cette évidence.

MANIFESTE SECURITÉ

Récemment, un virus est venu infecter le dispositif de contrôle à distance, opéré depuis le Nevada et la Virginie, des drones de l'armée américaine sur les théâtres d'opérations militaires. Comment a-t-il pu s'insinuer jusque dans les systèmes ultrasophistiqués de commande de ces appareils ? Pas par Internet, puisque pour d'évidentes raisons de sécurité les appareils ne sont pas directement connectés au réseau mondial. L'enquête en cours s'oriente vers l'introduction d'un logiciel malveillant véhiculé par les disques durs amovibles que les ingénieurs utilisent pour transférer les données entre leurs ordinateurs et le système de pilotage des drones. A cause de cette faille humaine des insurgés irakiens avaient déjà réussi en 2009, avec une technologie bon marché, à détourner le flux vidéo non crypté des caméras embarquées de ces appareils de combat télécommandés.

Appliqué au domaine de la santé, ces failles comportementales peuvent avoir des conséquences dramatiques. Elles pourront se traduire dans un service hospitalier par le blocage, avec un simple chariot pour la maintenir ouverte, de la porte sécurisée d'un local strictement réglementé alors qu'elle est équipée d'un système de contrôle d'accès ultraperformant.

Dans le même ordre d'idées, en novembre 2008 le vol de l'ordinateur chez un médecin de l'Oise, élu de la majorité, a été perpétré ; l'appareil dérobé contenait onze années d'activité et plus de 10,000 dossiers patients. Le praticien réalisait bien des sauvegardes régulières, mais ces dernières l'étaient sur un disque externe qui se trouvait près de l'appareil, qui avait naturellement été emporté par les cambrioleurs !

Dans ces deux derniers exemples Il ne s'agit naturellement pas de jeter la pierre à quiconque, pas plus que de chercher à dresser une liste de boucs émissaires. C'est plutôt le décalage entre les pratiques du terrain dans un contexte souvent anxiogène et la finalité des dispositifs déployés qui sont à incriminer. Décalage qui illustre l'absolue nécessité d'une politique de sécurité adaptée.

Dans ce contexte l'attention de la Commission Sécurité de LESISS ne se limitera naturellement pas aux lacunes ou aux dysfonctionnements des protections techniques, ou aux seuls constats d'irrespect des règles. Elle travaillera en effet à la source des problèmes, notamment autour de **deux leviers essentiels : d'une part sur les considérations éloignées des pratiques attendues par les praticiens et les patients, d'autre part sur le manque de réalisme de certaines préconisations**, graves de conséquences par leur inadéquation avec une pratique de santé efficiente et sûre.

PLAN D'ACTION

Par des réflexions inscrites dans une démarche déterminée et responsable, l'objectif visé par la Commission Sécurité LESISS sera d'apporter une contribution significative sur le sujet sensible de la protection des systèmes d'information de santé ; en versant dans le domaine public les résultats de ces travaux collaboratifs et bénévoles, et en tenant compte des besoins et attentes des différents acteurs et utilisateurs des SIS, mais également de leurs devoirs et responsabilités.

REVUE GÉNÉRALE DE SITUATION

LES ATOUTS

En premier lieu, les opérateurs concernés de l'Etat ont récemment témoigné, dans une logique de plus grande concrétude, d'une volonté d'organiser et de règlementer les SIH et la SSI santé. L'Etat et de ses services sont bien sûr légitimes dans leurs exigences de haute qualité (décret confidentialité, décret hébergeurs, mise en place d'un référentiel d'homologation pour les messageries sécurisées, loi HPST, RGS, création de l'ANSSI…). Pour autant, ces différentes instances devront, dans la concertation et la prise en compte de l'expertise des acteurs concernés de la société civile, contourner un obstacle bien identifié : la tentation de sacrifier à une profession de foi, alimentée par les technostructures, au détriment de la prise en compte des pratiques et usages exprimés par les acteurs de terrain.

A ce sujet, de récentes initiatives sont toutefois encourageantes :

- L'un des trois pré-requis que la DGOS a retenu**s** dans les critères d'éligibilité des incitations liées au programme « Hôpital numérique » concerne les obligations fermes en matière de SSIS. A ce sujet des indicateurs clairs s'articulent désormais autour d'un réel pragmatisme (simplicité, exposition à la critique des puristes de la SSI, auditabilité dans la gestion des identités, reprise et continuité des services, PSSI et processus de protection de la confidentialité des données des patients) ;

- Même s'il faudra veiller à en assurer la cohérence d'ensemble, la Maîtrise d'ouvrage des projets sera assurée par deux opérateurs publics clairement identifiés : la DSSIS pour le pilotage et la coordination, et l'ASIP pour le volet opérationnel. Ces deux instances viennent d'ailleurs de se voir confier, par le Secrétariat général des Ministères sociaux, l'élaboration d'une PGSSIS ;

- La consultation publique au sujet des indicateurs élaborés dans le cadre d'Hôpital numérique s'inscrit dans la volonté de tenir compte des éventuelles suggestions des acteurs ; de même nul doute que s'agissant de la PGSSIS la concertation régulière qui permettra de recueillir les expertises, notamment des industriels spécialisés, trouvera un écho très favorable ;

- la sonnette d'alarme tirée par l'ANSSI, qui préconise dans un communiqué du 8 octobre dernier « *la nécessaire application de règles d'hygiène informatique élémentaire* » et un retour à des pratiques simples mais trop souvent oubliées, entre autres par manque de formalisme ;

- La poursuite de l'amélioration du dispositif d'agrément des hébergeurs de données de santé à caractère personnel, dont le référentiel et la méthodologie, élaborés en concertation avec les industriels spécialisés évolue positivement au fil de l'eau ;

- La mise en place de la BNI des projets e-Santé qui marque une volonté de changement dans la lisibilité.

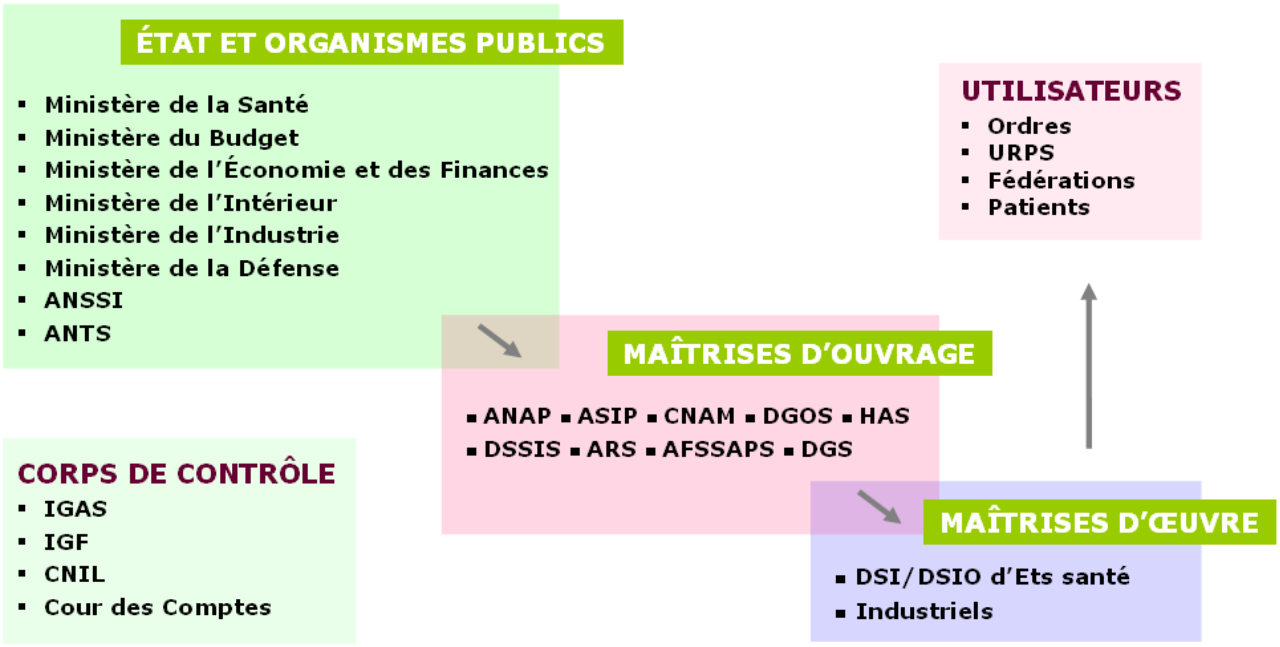
LES OBSTACLES

Cette dynamique positive ne doit pas faire oublier le lourd passif d'un écosystème institutionnel manquant de coordination et de clarté, peu adapté aux exigences de sécurité et/ou d'ergonomie sur l'ensemble de l'activité des soins médicaux (établissements hospitaliers publics et privés, médecine de Ville, secteur médico-social, contraintes spécifiques liées à la mobilité des acteurs …).

Sauf à maintenir la France sur les plus hautes marches du podium européen en matière de dossiers médicaux papier, la garantie d'un niveau approprié de sécurité, de confidentialité et d'accessibilité des données du citoyen ne pourra faire l'impasse de la prise en compte des besoins exprimés par les utilisateurs de terrain, notamment en matière d'utilisabilité.

UN JEU D'ACTEURS COMPLEXE AMPLIFIÉ PAR UNE ABSENCE DE COHÉRENCE

Sans naturellement prétendre à l'exhaustivité, la complexité du jeu d'acteurs - chacun étant focalisé sur ses propres intérêts - peut très synthétiquement être représentée comme suit :



En dépit des efforts consentis et comme l'ont détaillé d'innombrables études et rapports des corps de contrôle de l'Etat, **cet écosystème complexe des SIS a jusqu'à présent brillé par son inefficacité en raison de la faiblesse de trois piliers fondamentaux**, émoussant les réalisations effectives supposées atteindre les objectifs assignés par l'Etat et les autorités déontologiques :

- des **maîtrises d'ouvrage inappropriées**, aux imbrications complexes et ambigües, couvrant un champ incomplet et dont les réflexes pour traiter les sujets se conjuguent le plus souvent par la voie décrétale ;

- la **coordination des acteurs**, pénalisée par un empilement de technostructures souvent concurrentes entre elles, souffrant d'un changement de cartographie permanente et d'une absence de commandement unifié ;

- une **difficulté pour respecter des règles édictées** – quand ce n'est pas un refus délibéré –par l'Autorité Publique, quand elles existent (par exemple le RGS, qui s'applique en théorie à la sphère publique, et le Décret Confidentialité concernant les données des patients).

Dans ce contexte délétère, d'impressionnants budgets publics ont de longue date été engloutis dans des projets semi-finis, le plus souvent captés par un nombre proportionnellement réduit d'industriels généralistes. La connaissance parcellaire qu'ont ces derniers de l'écosystème sectoriel complexe de la Santé les conduit trop souvent - délibérément ou par défaut de compréhension des jeux d'acteurs - à complexifier davantage encore lesdits projets. En les conduisant *de facto* à l'échec avec la régularité d'un métronome.

A contrario les entreprises spécialisées et imprégnées du tissu sectoriel, sont souvent des TPE et PME innovantes. Ne disposant toutefois pas d'un volant financier suffisant, elles subissent de plein fouet les déséquilibres consécutifs, et se voient privées des opportunités pour mettre en œuvre leurs capacités d'innovation.

Cette configuration défavorable est en outre renforcée par des réticences fortes des utilisateurs potentiels, souvent rédhibitoires, pour lesquels la complexité réelle ou perçue des outils et de l'architecture déficiente des postes de travail constitue un puissant repoussoir. Sortir de ce cercle particulièrement vicieux suppose donc d'œuvrer de concert dans une recherche de pragmatisme.

DES ATTENTES BIEN IDENTIFIEES

Si l'enseignement des 15 années écoulées n'a d'évidence pas été encore officiellement tiré, les demandes des différents acteurs impliqués dans l'appropriation d'un SIS qu'un espace de confiance doit sécuriser sont heureusement bien identifiées :

- **Les Professionnels de la Santé et du Médico-social** attendent des solutions ergonomiques, performantes et financièrement supportables afin d'atténuer les nouvelles contraintes, inéluctables, liées à la mise en œuvre d'un environnement réglementaire en matière de sécurité fiable ;

- **Les patients,** qui ont une assez bonne perception de leurs attentes en matière de gestion de données de Santé - disponibilité si besoin, intégrité, traçabilité, propriété – sont pour autant en règle générale loin des considérations liées aux outils techniques. C'est donc le rôle des industriels, en collaboration avec les professionnels de santé, de trouver les solutions appropriées pour répondre à ces légitimes attentes ;

MANIFESTE SECURITÉ

- **L'État et ses Organismes affiliés** ont investi afin de poursuivre, pour l'heure sans résultats probants, la mise en œuvre d'une sécurité fiable des SIS. Même si du point de vue des industriels les choix envisagés ne sont pas toujours frappés du sceau de la pertinence, pour autant ils prennent acte de la volonté récemment affichée de renforcer cette construction dans la concertation ;

- **Les industriels** souhaitent l'avènement des conditions essentielles de montée en charge du marché des SIS : des référentiels stables, notamment en termes d'interopérabilité et de sécurité, des procédures de certification cohérentes, associés à des financements appropriés ;

- **Les organismes payeurs** attendent de ces systèmes qu'ils permettent une meilleure maîtrise des dépenses de Santé et un accroissement de l'accessibilité et de la qualité des soins (coordination des acteurs, lutte contre la fraude, performance globale…).

LES ENJEUX

- Assurer la sécurité des patients : accessibilité et qualité des soins, confidentialité des données ;

- Permettre aux professionnels de santé l'exercice de leur métier dans les meilleures conditions, entre autres s'agissant de protection en matière de responsabilité juridique ;

- Garantir l'interopérabilité, le respect des normes ainsi que le choix de standards internationalement reconnus et utilisés avec succès dans d'autres domaines d'activités sensibles (par exemple banque, assurance, aéronautique…) ; à ce sujet la nécessaire harmonisation ne pourra faire l'économie d'une mise à niveau de solutions propriétaires qui ne satisferaient pas ces exigences basiques ;

- Assurer aux industriels et investisseurs ainsi qu'aux donneurs d'ordre l'optimisation du retour sur leurs investissements ;

- Renforcer l'application des dispositifs légaux en adaptant la réglementation avec le pragmatisme et la concertation avec les acteurs concernés (en particulier les utilisateurs attendus) et en élaguant en tant que de besoin les clauses obsolètes ou inapplicables.

LES RISQUES

- Le sous-investissement, la poursuite de grands projets portés par des acteurs déconnectés des réalités du terrain ;

- Le rejet par les utilisateurs pour cause d'inadéquation entre les contraintes métiers particulières et les outils et modalités d'emploi imposés ;

- Les conflits d'intérêts et les rivalités entre organismes entravent la pérennité des investissements consentis et sont préjudiciables à l'intérêt général.

MANIFESTE SECURITÉ

LE BESOIN D'UNE POLITIQUE DE SECURITÉ FORMALISÉE

OBJECTIF D'UNE POLITIQUE DE SECURITÉ

Pour mémoire, **ce sujet ne peut plus relever d'un simple processus facultatif** puisqu'au final, en raison de la montée en puissance des outils de communication il a un impact direct et croissant sur la sécurité du patient. S'il en existe de nombreuses définitions, un moyen simple pour décrire l'importance d'une politique de sécurité consiste à l'aborder sous l'angle de son objectif prioritaire, lequel consiste à établir le cadre d'intervention, les principes directeurs et les règles pour parvenir à sa mise en œuvre. En d'autre terme, **une politique de sécurité doit donc être clairement formalisée !**

UN INSTRUMENT PRÉCIEUX

Vu sous cet angle, une politique de sécurité formalisée constitue un instrument précieux pour la réalisation des objectifs de sécurité. C'est un moyen simple d'établir une **trajectoire précise d'actions concertées entre tous les acteurs**. Or il n'en est pour l'heure pas ainsi dans l'écosystème de la santé et du médico-social en raison de considérations sectorielles « expertes », aussi nombreuses que divergentes. Ces atermoiements n'ont fait qu'intellectualiser, ces quinze dernières années, les tentatives infructueuses de construction d'une politique de sécurité. Au contraire cette politique doit être claire, naturelle, et perçue comme indispensable aux vues d'une gouvernance efficiente au service des citoyens.

Chaque Direction de système d'information de santé doit donc (ou devra donc très vite) disposer de sa Politique de Sécurité des systèmes d'information santé, ou PSSIS. **C'est un objectif prioritaire que doivent se fixer les intéressés**, à l'exemple de la dynamique institutionnelle récemment engagée autour d'une Politique *Générale* de Sécurité des Systèmes d'Information Santé, ou PGSSIS.

CONDITIONS DE L'APPLICATION RÉUSSIE D'UNE POLITIQUE DE SÉCURITÉ

Fidèles à leurs pratiques ces quinze dernières années dans le domaine des SIS, l'Etat et ses service ont eu dans le domaine de la sécurité une approche décrétale qui a classiquement conduit à un concert d'échecs répétés. L'exemple du décret « Confidentialité » publié le 15 mai 2007 en est une illustration particulièrement démonstrative. Inappliqué car – de l'aveu même en 2009 du Président de l'une des principales Agences concernées de l'Etat – inapplicable, **cet exemple illustre les limites d'un carcan réglementaire obsolète et inadapté**.

Tant qu'elle sera élaborée en chambre, sans prendre en amont l'avis des entreprises spécialisées et de leurs utilisateurs – surtout dans un domaine aussi complexe que celui de la santé, la réglementation ne peut en effet qu'accélérer l'immobilisme. Symétriquement**, une PGSSIS convenablement formalisée ne conduira à une amélioration de la qualité des systèmes d'information au service du citoyen que dès lors qu'elle sera soumise à des mécanismes négociés d'incitation, mais également de coercition.**

UN CHANGEMENT POSITIF DE PARADIGME INITIÉ PAR LE MINISTERE DE LA SANTÉ

Dans ce contexte délétère, la Commission Sécurité de LESISS salue la dynamique suscitée par le Ministre de la santé et portée par la DGOS, qui dans l'élaboration de ses indicateurs du programme « Hôpital numérique » a introduit les conditions de formalisation d'une PSSIS pour les établissements éligibles.

La démarche, même si elle devra naturellement être affinée au fil de l'eau dans la concertation, est d'autant plus pertinente que cette action de sécurisation des systèmes d'information de santé est menée de manière pragmatique. Cet effort courageux de simplicité prenant en compte des objectifs, modestes mais qui s'imposent, est d'autant plus pertinent dans un contexte où nombre de situations existantes dans les écosystèmes concernés doivent (ou devront) être entièrement repensées.

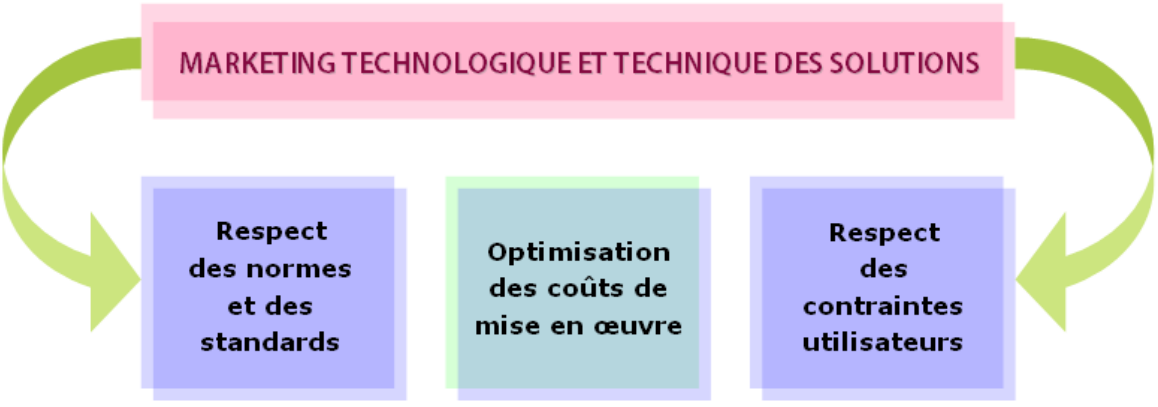
Cette nouvelle dynamique est donc un exemple intéressant du but que doit s'assigner une PGSSIS, empreinte tant de pragmatisme que de règles claires, où l'exigence et la simplicité se combinent dans la recherche d'une gouvernance enfin efficiente. Tout aussi intéressante sera la manière dont les PSSIS dans les établissements éligibles à « Hôpital numérique » seront déclinées, formalisées … et appliquées.

PROBLÉMATIQUE D'APPROPRIATION ET CONTRIBUTIONS

UN JEU D'ACTEURS D'UNE COMPLEXITÉ INEGALÉE

Bien que n'ayant pas vocation à se substituer aux autres acteurs, mais en raison de sa spécialisation et de son expertise panoramique, la Commission Sécurité de LESISS dispose des compétences industrielles et de la compréhension de la complexité des jeux d'acteurs. Elle affirme sa détermination à **soutenir, dans son champ de compétence et à la mesure de ses moyens, les trois piliers défaillants des SSIS** précédemment évoqués : la maîtrise d'ouvrage, la coordination des acteurs, et le respect des règles de sécurité.

Cette association de compétences et d'expertises pointues s'exprime dans les travaux collégiaux et procure une visibilité sur les plans technique et fonctionnel, ainsi que sur le volet marketing. Ces atouts permettent d'anticiper la mise en œuvre effective des meilleures solutions en garantissant l'optimisation des coûts.



MANIFESTE SECURITÉ

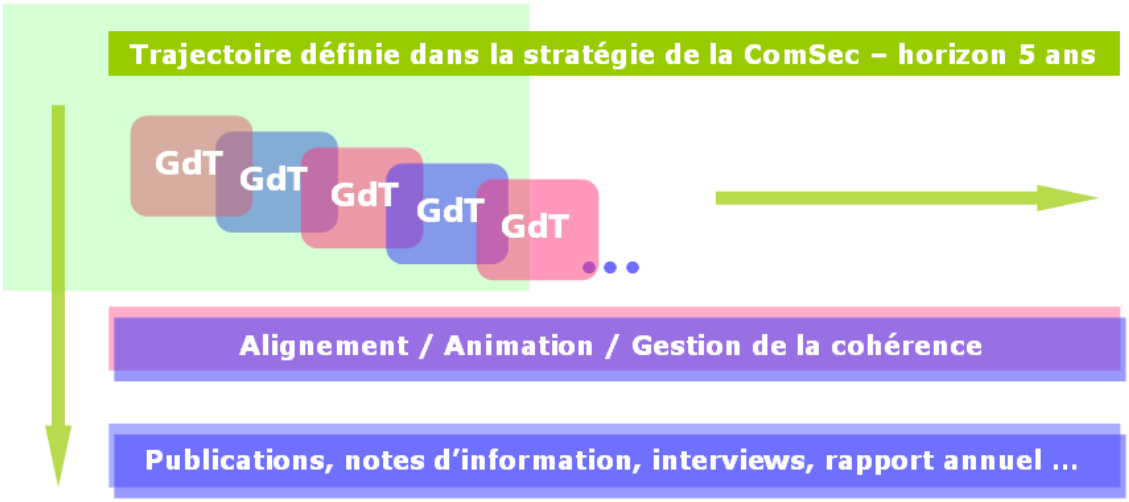
CONTRIBUTION DE LA COMSEC

La Commission Sécurité de LESISS va renforcer ses travaux, en coordination avec les diverses entités publiques et les représentations de professionnels de santé et de patients concernées, entre autres autour de cette vision Marketing.

TRAJECTOIRE ET DOSSIERS PRIORITAIRES DE LA COMMISSION

Les dossiers constitués par la Commission Sécurité vont être instruits par le prisme de groupes de travail thématiques (GDT). Cette forme d'organisation permet en effet de démultiplier les ressources et de mieux bénéficier des expertises. Avant la fin de l'année 2011 la Commission Sécurité aura ainsi avancé sur les sujets suivants :

- ***DC:*** *Etat des lieux et alignement du « décret Confidentialité »* avec le nouveau paradigme porté par la DGOS ;
- ***PGSSI / PSSI :*** *Référentiels de PGSSI (nationale) et PSSI* en adéquation à l'ensemble des acteurs, entre autre ceux de la médecine de Ville (prescripteurs, auxiliaires médicaux pharmacies d'officine) ;
- ***HDS / SPT :*** *Hébergement de données de Santé et sécurité du poste de travail,* en concertation avec la FNTC (Fédération Nationale des Tiers de Confiance) et l'AFHADS (Association Française des Hébergeurs de Données de Santé ;
- ***IA :*** *Indicateurs d'avancement* en concertation avec l'observatoire de la DGOS.



Les orientations de l'ASIP du 06/10/11 précisent : « *Ces travaux définiront des exigences de sécurité par paliers permettant d'inscrire les réalités opérationnelles dans un niveau de maturité et une trajectoire en conformité avec la cible de sécurité définie.* »

Dans le cas des SI de Santé la diversité des acteurs, l'inertie liée aux décisions inappropriées dans le passé, la gestion de l'investissement public et l'innovation proposée par les offres industrielles complexifient la définition de cette trajectoire.

CONTRIBUTION DE LA COMSEC

Ces groupes de travail thématiques étudieront les axes de progrès et émettront des propositions concrètes qui clarifieront l'opérabilité des jalons de cette trajectoire. Ces progrès seront régulièrement mesurés et communiqués.

DES POLITIQUES DE SECURITÉ APPLIQUÉES CAR APPLICABLES

LA NÉCESSITÉ D'UNE CONFIANCE PARTAGÉE

Il ne peut y avoir d'actions génératrices de confiance sans confiance en ces actions. L'assurance d'une politique partagée est donc indispensable, clairement acceptée par toutes les parties concernées. Elle constitue un véritable contrat réciproque dans un respect sans faille des engagements et en toute transparence, de règles appliquées – et donc applicables.

Dans tous les pays avancés le système de Santé – la France ne fait pas exception à cette règle - représente un tel enjeu stratégique qu'on ne peut le faire reposer sur un espace de confiance branlant. Un cadre de sécurité robuste et clairement défini est donc nécessaire, associé à un partage des responsabilités dont la PSSIS interne et la PGSSIS représentent, chacune dans son champ d'application, un élément fondamental.

Rappelons que la confiance ne se décrète pas, elle se mérite et elle s'instaure par l'exemplarité partagée dans le respect des règles établies.

CONTRIBUTION DE LA COMSEC

La Commission Sécurité de LESISS veillera à recommander la logique d'exemplarité partagée comme levier de confiance pour la promotion de la sécurité en santé, et sera un témoin vigilant des engagements des parties prenantes. La Charte BP6 (Bonnes Pratiques en Systèmes d'Information de Santé), prochainement publiée pourra de ce point de vue constituer un puissant levier.

LES SOURCES D'INSECURITÉ

Comme l'illustrent les exemples précédemment évoqués, c'est le plus souvent le facteur humain qui détermine la gravité des risques face aux menaces, et conduit aux erreurs et aux négligences tant au plan de la conception que de l'exploitation des traitements de l'information. Étonnamment, cette évidence est rarement appréhendée à sa juste mesure.

La réduction des risques passe donc par une prise en compte des facteurs humain et comportemental à tous les niveaux des solutions techniques : leurs usages, la portée de leur efficacité, leur utilisabilité, la qualité des documentations, etc.

CONTRIBUTION DE LA COMSEC

La Commission Sécurité de LESISS traitera soigneusement ce volet comportemental facteur de risques, en associant les acteurs concernés qui le souhaiteront.

L'ÉQUILIBRE ENTRE LES OBLIGATIONS ET L'ASSISTANCE

La PGSSIS rappelle les obligations de sécurité et garantit, aux établissements de santé et aux acteurs de la médecine de ville et des réseaux, la fourniture de canevas de bonnes pratiques en vue de protéger efficacement les données des patients dans leurs systèmes d'information de Santé.

En matière de sécurité, une politique réussie s'articule autour de responsabilités partagées. Ces canevas, dont l'ASIP Santé vient de voir confier la mission de les produire, se présenteront sous la forme de référentiels et autres documentations.

Ce *droit* des responsables de SIS et des prestataires à bénéficier de ces référentiels doit symétriquement s'accompagner de *devoirs*, entre autres concernant la production de résultats d'analyses de risques.

CONTRIBUTION DE LA COMSEC

La Commission Sécurité de LESISS veillera, en coordination avec les services concernés de l'Etat (en particulier ASIP, DGOS et DSSIS) ainsi qu'avec les autres acteurs concernés qui le souhaiteront, à la promotion des politiques de sécurité santé, dans le respect des référentiels de la politique générale de sécurité.

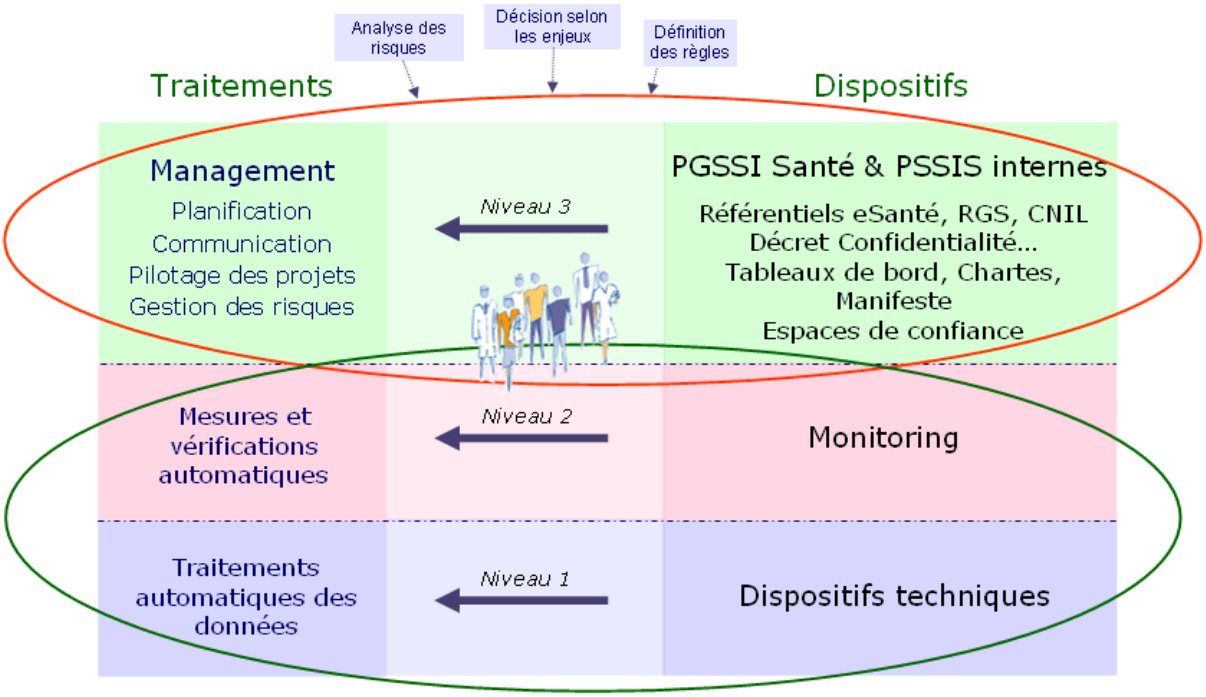
LES 3 NIVEAUX DU DISPOSITIF DE POLITIQUE DE SECURITÉ

Toute organisation doit s'assigner une Politique de Sécurité interne, avec ses principes directeurs et ses règles à respecter pour atteindre les objectifs de sécurité qu'elle s'est définie et fixée.

La PSSI interne est un dispositif qui ne peut intrinsèquement être automatisé. Pour autant, ce dispositif stratégique constitue le socle dynamique de l'arsenal de sécurité nécessaire à la gestion des risques.

Pour illustrer la différentiation de niveaux dans les types de dispositifs SSIS, le schéma ci-après distingue les solutions techniques de sécurité (*niveaux 1 et 2* entourés en vert), des outils servant au management de la politique sécurité (*niveau 3* entouré en rouge).

Les méthodes EBIOS 2010 et MEHARI 2010, par exemple, ainsi que leurs logiciels, se positionnent à ce niveau 3 du schéma. Ces outils reposent sur des textes déclaratifs, et laissent une large place au traitement humain des données.



CONTRIBUTION DE LA COMSEC

La Commission Sécurité LESISS veillera à ce que les dispositifs techniques de sécurité Santé (niveaux 1 et 2 du schéma ci-dessus) soient appliqués de la manière la plus rationnelle possible et à leurs justes niveaux, en tenant compte des exigences des politiques internes des établissements traitées au niveau 3.

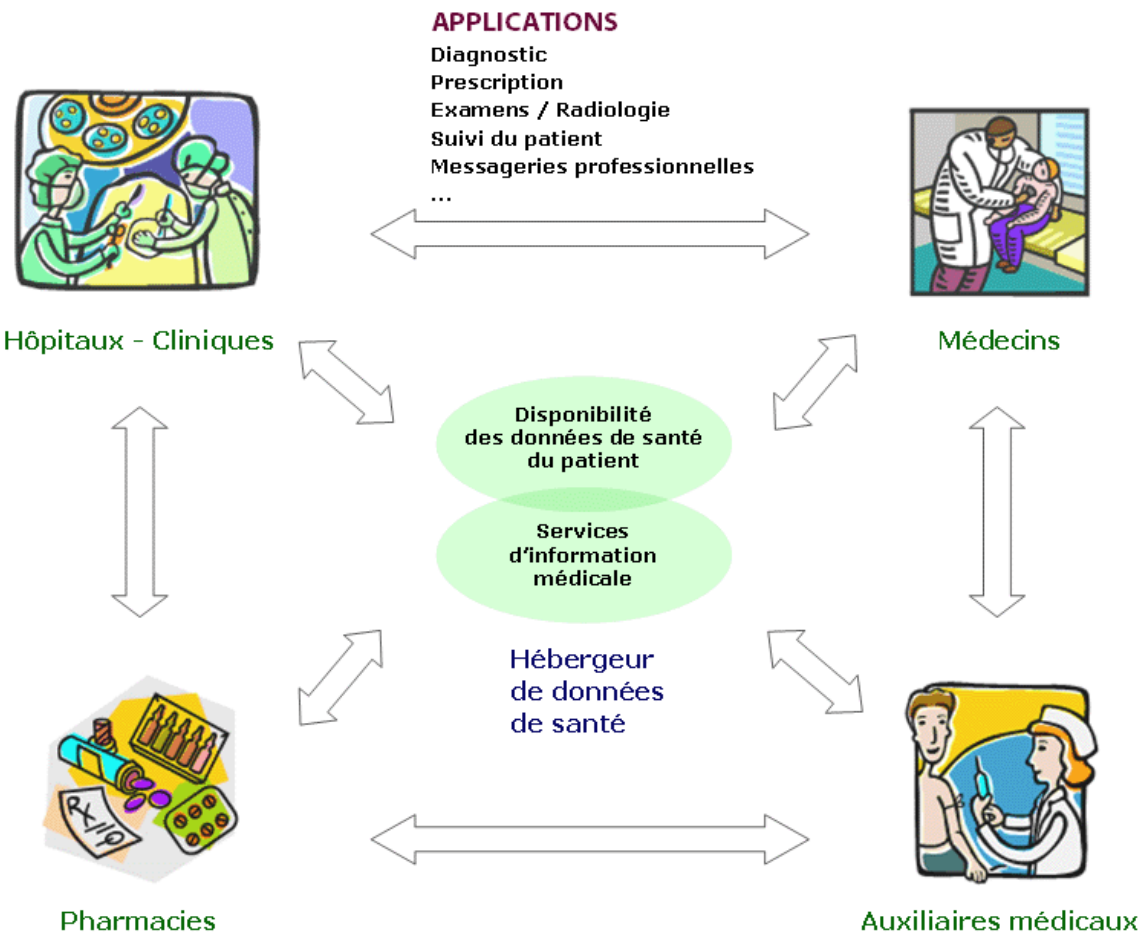
PRISE EN COMPTE DE L'ENSEMBLE DES ACTEURS DANS LES PROCESSUS SANTÉ

Le schéma ci-après met en évidence des environnements dont les objectifs et contraintes peuvent varier : médecine de Ville vs/ sphère hospitalière, secteur privé vs/ secteur public …

Force de propositions, le Groupe de Travail PGSSI / PSSI sera amené à préconiser et à mettre en exergue les principes directeurs et les règles qui lui paraîtront manquer dans la panoplie des bonnes pratiques en Santé.

Ces recommandations pourront par exemple porter sur le formalisme approprié et les mises à jour de certaines documentations, sur leur intelligibilité, ainsi que sur la prise en compte d'usages métier afin d'écarter le manque de réalisme de certaines demandes, ou au contraire leur absence, en proposant en tant que de besoin des éléments de mesure plus simples, etc.

MANIFESTE SECURITÉ



CONTRIBUTION DE LA COMSEC

La Commission Sécurité LESISS contribuera, par la mutualisation des compétences et du savoir-faire de ses adhérents actuels et à venir, pour qu'à l'horizon 2013 toutes les entités santé aient à disposition leurs PSSIS propres, à l'échelle de leurs moyens et des enjeux de leurs activités.

LES INDUSTRIELS, DIRECTEMENT CONCERNÉS

Les cordonniers étant traditionnellement les plus mal chaussés, la Commission Sécurité de LESISS œuvrera en interne afin de promouvoir les bonnes pratiques de sécurité auprès de ses adhérents.

CONTRIBUTION DE LA COMSEC

La Commission Sécurité de LESISS organisera, avec son expertise interne ou en recourant en tant que de besoin à des ressources externes, des sessions d'information et de formation concernant la PSSIS, auprès de ses adhérents concernés au bénéfice de leurs utilisateurs.

LA COUVERTURE DES GARANTIES, SUJET TROP SOUVENT ÉLUDÉ

Parmi les types de risques graves liés aux systèmes d'information, les menaces de cyber-attaques interpellent en général modérément les acteurs de l'écosystème de la Santé. D'autres secteurs d'activité économique, comme les assureurs, en ont pris acte de longue date. Les procès en responsabilité intentés par des patients, par exemple, constituent un risque à ne pas négliger, qu'une couverture assurantielle palliera d'autant mieux qu'une PSSIS adaptée aura été mise en œuvre.

CONTRIBUTION DE LA COMSEC

La Commission Sécurité de LESISS n'ignore pas les impacts financiers et médiatiques que peuvent engendrer des problèmes de disponibilité, d'intégrité et de confidentialité des données des patients. Elle veillera à ce qu'ils soient considérés dans les analyses et pris en compte dans les décisions relatives aux actions de sécurité.

RISQUES MAJEURS LIES A L'INAPPLICATION D'UNE POLITIQUE DE SECURITÉ

Les difficultés et les risques inhérents à la complexité des SIS ne peuvent pas être correctement gérés lorsque les objectifs de sécurité ne sont pas clairement en place dans les esprits. L'inapplication d'une politique de sécurité, quand bien même cette dernière existe, augmente sensiblement ces risques et conduit à des prises de décision inappropriées, voire irrationnelles. La panique qui vient ensuite précède généralement l'apathie, laquelle constitue les prémisses du désastre.

CONTRIBUTION DE LA COMSEC

La Commission Sécurité de LESISS, consciente des conséquences d'une poursuite des rejets des technologies de communications liée à une politique de sécurité inexistante ou inappropriée, mobilisera les forces vives de ses membres au service des meilleures pratiques. A cet égard et pour renforcer cette dynamique, les contributions de nouveaux adhérents seront naturellement prises en compte.

REJOINDRE LESISS ET PARTICIPER AUX TRAVAUX D'EXPERTS

Comme les quinze années écoulées l'ont clairement montré, en matière de technologies d'information de santé et pour le médico-social les acteurs économiques – les industriels concernés s'agissant de ce secteur– ont le choix entre trois postures :

- Attendre de l'Etat que ses technostructures communiquent une feuille de route ;
- Tenter seuls d'orienter les décisions vers un nécessaire pragmatisme ;
- Rejoindre l'Organisation qui affiche expertise et détermination et bénéficier du levier d'action.

Ceux qui ont mesuré les limites des deux premières options et souhaitent gérer leur avenir avec un acteur sans complexe et doté d'une forte capacité de conviction sont invités à rejoindre très vite LESISS !

BUREAU DE LA COMMISSION SÉCURITÉ LESISS

Jérôme Duvernois – Président – jduvernois@le6.org
Yannick Motel – Délégué Général - ymotel@le6.org
Christophe Cianchi – Président de la Commission Sécurité ccianchi@le6.org
Patrick Mensac – Vice-Président de la Commission Sécurité pmensac@le6.org

REMERCIEMENTS

Les auteurs du présent Manifeste tiennent plus particulièrement à remercier, pour leur apport essentiel aux premiers travaux de la Commission, Mesdames et Messieurs :

Sophie Carli Bacher – Mc Kesson
Lisbeth Hajji – Koïra
Isabelle Perre – Cerner
Tudy Bernier – Orange HealthCare
Nicolas Carpentier – Enovacom
Olivier Cazals – Ilex
Frédéris Connes – HSC
Samuel Desnos - Avencis
Dominique Gougerot – Berger Levrault
Yannick Kereun – Softway Medical
Elie Le Guilcher – Evolucare
Norbert Lipszic –DBMotion
Georges Munoz – CertEurope
Jean-Michel Nowak – SE Conseil
Luc de Rancourt – Koïra

MANIFESTE SECURITÉ

LISTE DES ADHÉRENTS LESISS

4 AXES
ACTIBASE
ADE Conseil Santé
ADS CONSEIL
AGFA Healthcare
ALCATEL LUCENT
ALERE France
ALLODOC
ANTESYS
APIGEM
ARCAN SYSTEMS
ARISEM
AVENCIS
AXIGATE
AXILOG
BE-Itech
BERGER-LEVRAULT
BLUELINEA
Business Card Associates
BUSINESS OBJECTS
C2i nnovativ' Systems
CALYSTENE
CAPSULE TECHNOLOGIES
CBA
CERNER
CERTEUROPE
CGTR
CISCO Europe
COMPUTER ENGENEERING
CORWIN
COSILOG
COVALIA
CRIP (Groupe Séphira)
CS3i
DB MOTION
DELL France
DL Santé
EELEO EMC
E-NOVATION
ENOVACOM
FAP Informatique
FSI
GLOBAL IMAGING ONLINE
H2AD
Habitat & Santé
HOPI
HSC
ILEX
IMPROVE Santé
INFINE Conseils
INTELLIGENCIA
INTELLEC
INTERSYSTEMS
JIC
KAYENTIS
KEOSYS
KEYNECTIS
KI-LAB
KLEE Group
KOÏRA
LENREK Informatique
LOGEMED
LOGICMAX
MC KESSON France
MEDECOM
MEDSYS
MEDASYS
MEDIANE
MEDISCS
MEDISSIMO
MEDITRANS
MICRO 6
MICROPOLE UNIVERS
MOBILE DISTILLERY
NUANCE HEALTHCARE
MERIQUE ASSISTANCE
ODSIS
OLEA MEDICAL
ORANGE BUSINESS SERVICES
ORION HEALTH
OSIRES
PANASONIC
PCI RPH
PENARANDA
PMSIpilot
PROKOV Editions
RESEARCH IN MOTION France
RESSOURCES Informatique
SAFICARD
SAGEM Sécurité
SANEXIS
SANTEOS
SE Conseil
SFR
SIEMENS Health Services
SIGEMS
SNAL
SNEPA
SOFTWAY Médical
SPH
SQLI
SYSTANCIA
TAM Télésanté
TECHNOSENS
TELEVITALE
TIC UNIVERSEL
TLM France
TRACEMED
UBIQUIET
UBISTORAGE
UNIMED
VIDAL
WARESYS
XIRING

GLOSSAIRE

AFSSAPS	Agence Française de Sécurité Sanitaire des Produits de Santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANAP	Agence Nationale D'appui à La Performance des établissements de santé et médico-sociaux
ANTS	Association Nationale des Techniques Sanitaires
ARS	Agence Régionale de Santé
ASIP	Agence des Systèmes d'Information Partagés de santé
BNI	Base Nationale d'Informations « e-santé »
CNAM	Caisse Nationale d'Assurance Maladie des travailleurs salariés
CNIL	Commission Nationale de l'Informatique et des Libertés
DC	Décret « Confidentialité » 2007-960 du 15 mai 2007
DGS	Direction Générale de la Santé
DGOS	Direction Générale de l'Offre de Soins
DSSIS	Délégation à la Stratégie des Systèmes d'Information de Santé
EBIOS 2010	Expression des Besoins et Identification des Objectifs de Sécurité. Méthode d'analyse des risques de l'ANSSI, version 2010
GDT	Groupe De Travail thématique de la Commission Sécurité de LESISS
HAS	Haute Autorité de Santé
HDS	Hébergeur agréé de Données de Santé à caractère personnel
HPST	Loi « Hôpital Patient Santé Territoire »
IA	Indicateurs d'Avancement
IGAS	Inspection Générale des Affaires Sociales
IGF	Inspection Générale des Finances
MEHARI 2010	Méthode d'évaluation et de management des risques liés à l'information du CLUSIF (Club de la Sécurité de l'Information Français), version 2010
PGSSIS	Politique Générale de Sécurité des Systèmes d'Information de Santé
PSSIS	Politique de Sécurité des Systèmes d'Information de Santé
RGS	Référentiel Général de Sécurité
SPT	Sécurité du Poste de Travail
SIS	Systèmes d'Information de Santé
SSIS	Sécurité des Systèmes d'information de Santé
URPS	Unions Régionales des Professionnels de Santé

NOTES