Principes d’architecture

Développement d’une Preuve de Concept

Auteur(s) et contributeur(s)

Nom & Coordonnées	Qualité & Rôle	Société
Gérald ATTARD	Consultant en Architecture logicielle	Xxxxxxxxxx

Historique des modifications et des révisions

N° version	Date	Description et circonstance de la modification	Auteur
1.0	13/01/2023	Création du document	Gérald ATTARD

Validation

N° version	Nom & Qualité	Date & Signature	Commentaires & Réserves
1.0	Kara Trace CIO, Ursa Major Health		
	Anika Hansen, PDG, Jupiter Scheduling Inc.		
	Chris Pike Architecte d'entreprise principal, Schedule Shed		

Tableau des abréviations

Abr.	Sémantique

Table des matières

I. Introduction

Les principes édictés dans ce document définissent les caractéristiques générales de la plateforme commune créée par et pour le Consortium MedHead.

Ces caractéristiques couvrent quatre domaines complémentaires et définissent les bases sur lesquelles la nouvelle solution applicative devra se fonder pour se construire de façon robuste et progressive, à savoir les domaines :

- métiers ;
- applicatifs ;
- données ;
- technologiques.

En outre, les principes énoncés ici se basent sur le précédent document, anciennement labellisé *architecture-principles.* Néanmoins, bien que ces nouveaux principes édictés soient fondés sur de plus anciens, ils ne suivront pas la même numérotation. Aussi, pour assurer une certaine transition, les principes existants seront précédés du sigle (-), alors que les nouveaux seront désignés avec (+). De plus, les anciens principes contiendront la mention « *Anciennement labellisé :* » pour indiquer l'ancienne numérotation associée.

II. Principes métiers

II.A. (-) Principe A1 : Primauté des principes

II.A.1. Déclaration :

Les principes énoncés ici s'appliquent à tous les membres du Consortium, que nous appellerons collectivement l'entreprise.

II.A.2. Raisonnement :

La seule façon de fournir aux décideurs un niveau cohérent et mesurable d'informations de qualité est que toutes les organisations respectent ces principes.

II.A.3. Implications :

Sans ce principe, des exclusions, du favoritisme et des incohérences mineraient rapidement la gestion et la pertinence des décisions concernant l'architecture.

Les initiatives ne débuteront pas tant que leur conformité aux principes n'aura pas été examinée. Un conflit avec un principe sera résolu en modifiant le cadre de l'initiative.

II.B.(-) Principe A2 : Maximiser les avantages pour l’entreprise

II.B.1. Déclaration :

Les décisions d'architecture et de conception général sont prises pour fournir un avantage maximum à l'entreprise dans son ensemble, dans le cadre des efforts entrepris pour améliorer les soins dispensés aux patients touchés par ces décisions.

II.B.2. Raisonnement :

Ce principe incarne « l’engagement sans faille à servir autrui ». Les décisions prises selon la perspective de l'entreprise ont une plus grande valeur à long terme que les décisions prises dans une perspective organisationnelle particulière. Un retour surinvestissement maximal nécessite des décisions architecturales et de conception pour respecter les moteurs et les priorités à l'échelle de l'entreprise. Les intérêts d’aucun groupe minoritaire ne porteront atteinte aux intérêts de l’entreprise. Cependant, ce principe n'empêchera aucun groupe minoritaire de faire son travail.

II.C.(-) Principe A3 : Conformité aux lois et aux règlements

II.C.1. Déclaration :

Le système d’information, les processus métier et les livrables doivent être conformes à toutes les lois, politiques et réglementations pertinentes.

II.C.2. Raisonnement :

La politique de l'entreprise exige le respect des lois, politiques et réglementations. Cela n'exclut pas les améliorations des processus métier qui conduisent à des changements de politiques et de réglementations.

II.C.3. Implications :

L'entreprise doit être attentive à se conformer aux lois, réglementations et politiques externes concernant la collecte, la conservation et la gestion des données, formation et accès aux réglementations. L'efficacité, le besoin et le bon sens ne sont pas les seuls moteurs. Les changements au niveau des lois et des réglementations peuvent entraîner des changements dans nos processus ou applications.

II.D.(-) Principe A4 : Adhésion au serment d’Hippocrate

II.D.1. Déclaration :

En tant qu'entreprise à visé médical dont le but est d’améliorer les soins dispensés aux patients, toutes les décisions organisationnelles doivent adhérer au serment d’Hippocrate (« d’abord ne pas nuire, ensuite soigner ») en ce qui concerne les soins prodigués par tous les membres du Consortium et leur personnel interne.

II.D.2. Raisonnement :

La politique d'entreprise consiste à respecter les principes de soins aux patients et à reconnaître que les décisions organisationnelles peuvent avoir un impact sur leur vie.

II.D.3. Implications :

À tous les niveaux, l'entreprise doit être attentive à prendre des décisions visant à apporter de la valeur (économique et thérapeutique) au patient ainsi qu'aux organisations membres. Des conséquences financières et liées à la réputation peuvent s’en suivre directement si le patient subit un préjudice, intentionnellement ou par négligence.

II.E.(-) Principe A5 : Normes ouvertes pour garantir des normes élevées

Anciennement labellisé : ***Principe C3***

II.E.1. Déclaration :

L'application de normes ouvertes et de meilleures pratiques convenues peut soutenir l'organisation en lui apportant les connaissances et l'expertise du secteur.

II.E.2. Raisonnement :

Les principes décrits ici s'appuient sur les meilleures pratiques du secteur qui ont évolué par des normes, des méthodes éprouvées et des directives. L'utilisation des normes associées peut permettre de mieux tirer parti des avantages découlant des principes avec lesquels nous nous alignons.

II.E.3. Implications :

Nous encouragerons et soutiendrons, au moins, les normes ouvertes et les meilleures pratiques architecturales listées ci-dessous. Toutes les conceptions et architectures doivent être conçues, le cas échéant, pour prendre en charge des extensions. Il est conseillé de documenter la manière dont les extensions prennent en charge ces normes ou sont conçues pour être étendues à cette fin, selon les thématiques ci-dessous :

- L’architectures pilotées par les événements :
  - Source des événements.
- Les Architectures microservices :
  - Spécification OpenAPI des contrats de service ;
  - Maillages de services :
    - Observabilité des services,
    - Surveillance des services,
    - Découverte des services,
    - Visibilité de l'intégration des services.
  - Déploiement via une infrastructure conteneurisée, immuable et reproductible ?
- La conception pilotée par le domaine.
- Le développement centré sur le comportement :
  - pour garantir l'exactitude des résultats attendus centrés sur le patient ;
  - pour soutenir un développement aligné avec un langage omniprésent.
- La tolérance aux pannes.
- L’intégration d'OpenID Connect avec les fournisseurs d'identité des patients gérés par l'État.
- Le choix de la technologie devrait favoriser les langages JVM en raison des directives du Consortium.
- La documentation devrait favoriser Javadoc ou NDoc pour le code source et les milestones ou ASCIIdoc pour la documentation au niveau du projet.

Comme cela définit un état cible, il est acceptable de faire des compromis, mais ces derniers doivent être documentés et justifiés.

II.F. (-) Principe A6 : Favoriser une culture de “learning” avec des preuves de concept, des prototypes et des Spike

Anciennement labellisé : ***Principe C4***

II.F.1. Déclaration :

L'entreprise encourage les implémentations centrées sur l'apprentissage qui réduisent les risques, valident les hypothèses et investissent dans l'apprentissage nécessaire pour faire évoluer la plateforme de manière responsable.

II.F.2. Raisonnement :

Le Consortium encourage collectivement l'utilisation de validations de principes, de Spike et de prototypes, ainsi que d'autres moyens d'enquête pour atteindre un état d’échec sans danger dans les zones où les informations disponibles sont insuffisantes pour comprendre le risque lié à la prise de décisions de conception ou de mise en œuvre spécifiques au niveau de la production.

Le coût de l'investissement dans les efforts d'apprentissage pour réduire les risques est encouragé dans toute l'entreprise afin de protéger les intérêts des patients, des partenaires et de l'entreprise elle-même.

II.F.3. Implications :

Les partenaires du Consortium conviennent collectivement de stimuler une culture de prise de décision fondée sur des preuves et centrée sur l'apprentissage.

Ce faisant, les exceptions et considérations suivantes devraient s'appliquer :

1. Fournir une hypothèse pour chaque apprentissage
    - Toutes les implémentations liées à l'apprentissage doivent être accompagnées d'une hypothèse définissant l'apprentissage souhaité et permettant de mesurer si ce résultat d'apprentissage a été atteint.
2. Isoler les preuve de concept des données et des systèmes de production
    - Des mesures doivent être prises pour atténuer ou éliminer le risque d’impact sur les patients lorsqu'il existe un risque de nuire au patient ou à l'entreprise. Par exemple, l'apprentissage peut être mené de manière isolée dans un environnement artificiel afin d'éviter l’impact sur les systèmes de production.
    - Utiliser des données factices ou anonymisées.
    - Les données des patients utilisées pour les activités d’apprentissage à haut risque doivent être protégées, afin d’éviter un impact sur la sécurité des données ou les soins aux patients. Les PoC devrait utiliser des données anonymisées ou factices lorsque cela est possible.

3. Assouplir la conformité, mais tenir compte des conséquences
    - Les normes de gouvernance et les niveaux de conformité peuvent être assouplis lorsque des mesures sont prises pour protéger les systèmes de production et les données des patients. Les PoC isolées des données réelles des patients et des systèmes de production ne sont pas régies par des normes externes ou une quelconque gouvernance d'entreprise en matière de séparabilité.
    - Lorsque les normes et la gouvernance ne sont pas pleinement respectées, les responsables de la mise en œuvre et les concepteurs devraient réfléchir à la manière dont ces prototypes ou ces mises en œuvre centrés sur l'apprentissage peuvent fournir des leçons dans les mises en œuvre finales en production.
    - Il est fortement déconseillé de produire directement des prototypes. Il convient plutôt de veiller à ce que les conceptions tiennent compte des effets secondaires de la production qui peuvent invalider tout apprentissage. Par exemple, l'omission de problèmes de sécurité ou la mauvaise estimation du volume de données attendu peut entraîner des problèmes de performances qui invalident les apprentissages tirés d’un tel prototype non évolutif.
    - Les tests de performance des prototypes et des implémentations centrées sur l'apprentissage devraient valider les algorithmes clés faisant partie de cette échelle d'apprentissage.
4. Les principes de base de l'ingénierie, de la livraison et des tests ne doivent pas être assouplis pour l'architecture de la PoC.
    - La validation de principe doit viser spécifiquement à respecter les principes suivants :
        - Principe B1 : Continuité des activités des systèmes critiques pour les patients
        - Principe B2 : Clarté grâce à une séparation fine des préoccupations
        - Principe B3 : Intégration et livraison continues
        - Principe B4 : Tests automatisés précoces, complets et appropriés
5. Plans de test comme outils de communication des exigences
    - Les livrables avec des plans de test autodocumentés sont préférables aux plans de test documentés en externe.
    - La preuve de concept doit comporter des plans de test décrivant comment le produit doit se comporter.
    - Les plans de test doivent utiliser des scénarios BDD (behaviour-driven development - voir A5) pour décrire les critères d'acceptation métier qui sont dans la portée.
    - Les plans de test doivent utiliser le langage commun de l'entreprise et être compréhensibles par les partenaires techniques et non techniques.

6. Tester les rapports d'exécution pour documenter le comportement pris en charge
    - Pour prendre en charge la visibilité des comportements attendus, l'apprentissage continu et la transparence concernant l'état du logiciel :
        - Les PoC devraient avoir des pipelines CI qui exécutent des tests et produisent des rapports d'exécution des tests
        - Les environnements CI doivent permettre aux propriétaires des logiciels d'inspecter les exécutions passées et les dégradations de la build qui peuvent affecter les l'hypothèse, en ligne avec le principe B3.

II.G.(+) Principe A7 : Gérer l'information est l'affaire de tous

II.G.1. Déclaration :

Toutes les entités composant le Consortium participent aux décisions de gestion de l'information nécessaires pour atteindre les objectifs d’amélioration des soins médicaux.

II.G.2. Raisonnement :

Les utilisateurs de l'information sont les principales parties prenantes, ou clients, dans l'application de la technologie pour répondre à un besoin médical.

Afin de s'assurer que la gestion de l'information est alignée sur la politique du Consortium, toutes les entité de MedHead doivent être impliquées dans tous les aspects de l'environnement de l'information.

Les spécialistes médicaux du Consortium et le personnel technique responsable du développement et de la maintenance de l'environnement informatique doivent se réunir en équipe pour définir conjointement les buts et les objectifs de l'informatique.

II.G.3. Conséquences :

Pour fonctionner en équipe, chaque partie prenante, ou client, devra accepter la responsabilité du développement de l'environnement de l'information.

Un engagement de ressources sera nécessaire pour mettre en œuvre ce principe.

II.H.(+) Principe A8 : Application à usage commun

II.H.1. Déclaration :

Le développement de la plateforme commune, utilisée et développée par et pour le Consortium, est préférable au développement d'applications similaires ou en double qui ne sont fournies qu'à une seule entreprise particulière, exception faite en cas de décision spécifique du Consortium pour répondre à un besoin avéré.

II.H.2. Raisonnement :

La capacité de duplication est coûteuse et prolifère des données contradictoires.

II.H.3. Conséquences :

Les entreprises consituant le Consortium, prises indépendamment, ne devront pas dépendre d'une capacité qui ne sert pas l'ensemble du Consortium. Elles devront donc se doter de la capacité de remplacer leur système prioritaire par un système à l'échelle du Consortium ; cela nécessitera l'établissement et le respect de politiques exigeantes et strictes.

Indépendamment du Consortium, les entreprises ne seront pas autorisées à développer des capacités pour leur propre usage qui sont similaires et/ou dupliquées des capacités des outils à l'échelle de Consortium. De cette manière, les dépenses de ressources rares pour développer essentiellement la même capacité de manière légèrement différente seront réduites et réparties dans les secteurs présentant à la fois de la valeur-ajoutée et un besoin avéré.

Les données et les informations utilisées pour soutenir la prise de décision d’une seule entreprise seront normalisées dans une bien plus grande mesure qu'auparavant, puisqu’a partir de l’application de ce principe, ces données et informations serviront la prise de décision à l’échelle du Consortium.

En effet, les capacités organisationnelles plus petites qui produisaient des données différentes, et qui n'étaient pas partagées entre d'autres organisations, seront remplacées par des capacités à l'échelle du Consortium. L'impulsion pour l'ajout à l'ensemble des capacités à l'échelle du Consortium peut bien provenir d'une entreprise qui aura su démontrer, de manière convaincante, la valeur des données et/ou des informations précédemment produites par sa capacité organisationnelle. Néanmoins, une fois que de telles données et/ou informations auront été qualifiée de Valeur, la capacité résultante fera partie du système à l'échelle du consortium, et ces données et/ou informations produites seront partagées au sein de l’ensemble du Consortium.

II.I. (+) Principe A9 : Responsabilité technologique

II.I.1. Déclaration :

Le Consortium est responsable de l'organisation technologique, de la possession et de la mise en œuvre des processus et de l'infrastructure médicale nécessaires, permettant aux solutions médicales de répondre aux exigences définies pour les soins d'un patient, en matière de fonctionnalité, de niveaux de service, de coût et de délai de mise en oeuvre.

II.I.2. Raisonnement :

Le Consortium s'impose d'aligner efficacement les attentes des patients avec les capacités et les coûts afin que les soins prodigués soient les plus efficaces possibles : des solutions efficientes et efficaces ont des coûts raisonnables et des avantages évidents.

II.I.3. Conséquences :

Un processus spécifique à chaque soin prodigué doit être créé pour spécifier à la fois ses processus de réalisation et son contexte d'utilisation.

Ainsi, chaque fonction technologique nécessaire à un soin doit définir des processus pour gérer les attentes du patient.

En outre, des modèles de données, d'applications et de technologies doivent être créés pour permettre des solutions médicales intégrées de qualité, afin de maximiser les résultats médicaux.

II.J. (+) Principe A10 : Protection de la propriété intellectuelle

II.J.1. Déclaration :

La propriété intellectuelle (PI) du Consortium doit être protégée. Cette protection doit se refléter dans l'architecture technologique, la mise en œuvre et les processus de gouvernance. Néanmoins, ce principe ne saurait prévaloir sur le **Principe A4 : Adhésion au serment d'hippocrate**.

II.J.2. Raisonnement :

Une grande partie de la propriété intellectuelle du consortium est hébergée dans son domaine technologique.

II.J.3. Conséquences :

Bien que la protection des actifs de propriété intellectuelle soit l'affaire de tous, une grande partie de la protection réelle est mise en œuvre dans le domaine technologique - même la confiance dans les processus non technologiques peut être gérée par des processus technologiques (e-mail, notes de service, documentation opératoire, etc.)

Une politique de sécurité, régissant les acteurs humains et technologiques, sera nécessaire pour améliorer considérablement la protection de la propriété intellectuelle. Cette démarche se veut, à la fois, d'éviter les compromis et de réduire les responsabilités des collaborateurs médicaux.

III. Principes d’application

III.A. (-) Principe B1 : Personnalisation de l'ADM TOGAF

Anciennement labellisé : ***Principe C1***

III.A.1. Déclaration :

L'architecture métier sera façonnée par la personnalisation et l'amélioration continue d'un cadre d'architecture adapté à partir de l'ADM de TOGAF 9.2.

III.A.2. Raisonnement :

Afin de fournir un langage et une lisibilité communs pour l'architecture, il est nécessaire de partir d'une base bien définie et offrant plusieurs options. Le TOGAF d'OpenGroup fournit un cadre centré sur la gestion des exigences.

Ce TOGAF comprend la gouvernance et les conseils qui soutiennent la spécialisation d'un cadre et d'une méthodologie permettant de déterminer quels niveaux de rigueur sont requis pour les fonctionnalités liées à la sécurité des patients, à la confidentialité des données, à la sécurité globale des informations et au respect de l’exactitude des informations.

III.A.3. Implications :

L'ADM de TOGAF comprend la gouvernance et les protections nécessaires pour garantir une architecture capable de répondre aux exigences éthiques, métier et d’état concernant les logiciels centrés sur le patient.

L'architecte logiciel du Consortium devra collaborer avec les parties prenantes médicales, métier et techniques pour convenir d'un cadre architectural, qui pourra être modifié selon les projets et les différents contextes métier.

III.B. (-) Principe B2 : Référentiel d'architecture centralisé et organisé comme source de référence

Anciennement labellisé : ***Principe C2***

III.B.1. Déclaration :

Toutes les informations pertinentes sur le plan architectural devraient être disponibles dans un répertoire d'architecture central géré en permanence par la fonction d'architecture métier, qui en sera responsable.

III.B.2. Raisonnement :

Lorsque les artéfacts d'architecture sont dispersés sur plusieurs systèmes, il devient difficile, au fil du temps, pour tous les partenaires d'avoir une vision claire et à jour de l'état de l'architecture.

III.B.3. Implications :

Un répertoire centralisé simplifie le problème de la consolidation et de la conservation de tous les artéfacts, décisions et contenus actuels relatifs à l’architecture dans un paysage d'exigences métier et techniques en constante évolution.

III.C. (+) Principe B3 : Indépendance technologique

III.C.1. Déclaration :

Les applications informatiques sont indépendantes des choix technologiques spécifiques et peuvent donc fonctionner sur une variété de plates-formes informatiques.

III.C.2. Raisonnement :

L'indépendance des applications informatiques, par rapport à la technologie sous-jacente, permet à celles-ci d'être développées, mises à niveau et exploitées de la manière la plus rentable et la plus opportune. Dans le cas contraire, une technologie, sujette à une obsolescence continue et à sa dépendance vis-à-vis de fournisseurs extérieurs, deviendra un moteur d’investissement, en lieu et place des soins prodigués à un patient, tel qu’énoncé au sein du **principe A9 : Responsabilité technologique**.

Sachant que chaque décision médicale, prise en fonction d’un résultat informatique, rend le patient dépendant de cette technologie. Ainsi, l'intention de ce principe est de garantir que le logiciel d'application ne dépend aucunement du matériel et des logiciels de systèmes d'exploitation spécifiques.

III.C.3. Conséquences :

Ce principe nécessitera des normes qui prennent en charge la portabilité.

Pour les applications commerciales sur étagère (COTS) et gouvernementales sur étagère (GOTS), les choix actuels peuvent être limités, car bon nombre de ces applications dépendent de la technologie et de la plate-forme.

Des interfaces de sous-système devront être développées pour permettre aux applications héritées d'interagir avec les applications et les environnements d'exploitation développés dans le cadre de la plateforme commune à l'ensemble du Consortium.

Le middleware devra être adapté et utilisé pour découpler les applications des solutions logicielles spécifiques.

À titre d'exemple, ce principe pourrait conduire à l'utilisation du langage Java®, et de futurs protocoles de type Java® accordant une grande priorité à l'indépendance de la plate-forme.

III.D. (+) Principe B4 : Facilité d'utilisation

III.D.1. Déclaration :

Les applications informatiques devont être faciles à utiliser.

La technologie sous-jacente est transparente pour les utilisateurs, afin qu'ils puissent se concentrer sur les tâches médicales à accomplir.

III.D.2. Raisonnement :

Plus un personnel médical doit comprendre la technologie sous-jacente, moins il est productif ; la facilité d'utilisation est une incitation positive à l'utilisation d'applications informatiques. Il encourage ces mêmes personnels médicaux à travailler dans un environnement d'information intégré au lieu de développer des systèmes isolés pour accomplir leur(s) tâche médicale en dehors de l'environnement d'information intégré du concortium.

Ainsi, les connaissances informatiques requises pour faire fonctionner un système médicale ne devront pas être un frein et/ou un obstacle direct ou indirect aux soins prodigués au patient.

La formation informatique devra être réduite au minimum et le risque d'utiliser un système de manière inappropriée devra être faible. L'utilisation d'une application informatique doit être la plus intuitive possible pour n'importe quel personnle médical.

III.D.3. Conséquences :

Les applications devront avoir une « *apparence et une convivialité* » communes et répondre à des exigences ergonomiques strictes, issues d'une charte graphique adaptée.

Par conséquent, la norme d'apparence commune doit être conçue et des critères de test d'utilisabilité doivent être développés en vue d'homogénéiser tous les services offerts par la plateforme du Consortium.

Les lignes directrices pour les interfaces utilisateur ne doivent pas être limitées par des hypothèses étroites sur le niveau de formation du personnel médical, tel que la langue, la formation aux systèmes médical ou la capacité physique...

Des facteurs tels que la linguistique, les infirmités physiques du personnel médical (acuité visuelle, capacité à utiliser le clavier et/ou la souris) et la maîtrise de l'utilisation de la technologie ont de vastes ramifications pour déterminer la facilité d'utilisation d'une application.

IV. Principes technologiques

IV.A. (-) Principe C1 : Continuité des activités des systèmes critiques pour les patients

Anciennement labellisé : ***Principe B1***

IV.A.1. Déclaration :

Les opérations essentielles à la santé des patients, ainsi que les autres pratiques de soin, doivent être assurées malgré les interruptions du système.

IV.A.2. Raisonnement :

Étant donné que les soins aux patients sont considérés comme une priorité, tous les systèmes critiques doivent être construits conformément aux principes de tolérance aux pannes, de telle sorte que la priorité soit accordée à la fiabilité de ces systèmes tout au long de leur conception, de leur déploiement, de leur développement et de leur utilisation. Les partenaires médicaux, les fonctions métiers et techniques de l'entreprise doivent être en mesure de remplir leurs tâches indépendamment des événements externes. Les pannes matérielles, les attaques ciblées, les catastrophes naturelles et la corruption des données ne doivent pas perturber ou à arrêter les activités de l'entreprise.

IV.A.3. Implications :

La dépendance vis-à-vis des applications système partagées exige que les risques d'interruption des activités soient établis à l'avance et traités lorsqu'ils se présentent. La gestion comprend, sans s'y limiter :

- Principes SRE (Site Reliability Engineering) qui surveillent et mesurent en continu les SLI cibles (Service Level Indicators).
- Examens périodiques de la santé et des risques du système.● Tests incrémentiels de performances, de vulnérabilité et d'exposition pour chaque incrément de la plateforme technique.
- Services critiques conçus pour assurer la continuité des fonctions de l'entreprise grâce à des capacités redondantes ou alternatives.
- La récupérabilité, la redondance et la maintenabilité doivent être prises en compte au moment de la conception.
- Les demandes doivent être évaluées selon leur criticité et leur impact sur la mission de l'entreprise, laquelle est d’assurer les soins aux patients.
- Des plans de reprise doivent exister pour tous les systèmes critiques.

IV.B. (-) Principe C2 : Clarté grâce à une séparation fine des préoccupations

Anciennement labellisé : ***Principe B2***

IV.B.1. Déclaration :

Il faut éviter de regrouper ensemble des responsabilités disparates. Il faut éviter les systèmes centralisés.

IV.B.2. Raisonnement :

Par entropie naturelle, les architectures complexes ont tendance à évoluer au fil du temps vers des réseaux régis par des dépendances complexes et difficiles à définir, et des responsabilités mal placées. Les composants d'une telle architecture sont souvent étroitement et fortement couplés.

Cela peut, au fil du temps, entraîner une perte des fonctions de l’architecture qui limite l'agilité d'une plateforme à répondre à l'évolution des besoins de l'entreprise ou des patients. Il faut connaître les limites du système. Il faut rendre le système transparents, c'est à dire :

- tout est bien découpé et on sait ce qui fait quoi exactement ;
- on connaît les dépendances entre chaque fonction.

IV.B.3. Implications :

Les décisions architecturales doivent suivre les principes et les meilleures pratiques de la conception pilotée par le domaine et des architectures de microservices. Cela implique un partenariat actif entre les équipes techniques et métier pour fournir des capacités à l'entreprise en utilisant un modèle partagé et un langage qui reflète le domaine des soins aux patients. Les dépendances étroites entre les capacités techniques doivent être identifiées et, dans la mesure du possible, doivent apporter une réponse aux situations problématiques traités dans le contexte métier et dans le monderéel. Les solutions techniques doivent toutes être justifiées et modélisées en fonction de leur contribution globale aux scénarios de soins aux patients.

IV.C. (-) Principe C3 : Intégration et livraison continues

Anciennement labellisé : ***Principe B3***

IV.C.1. Déclaration :

L'intégration et la livraison continues de petits changements incrémentiels sont favorisées par rapport aux temps de cycle lents et aux intégrations majeures.

IV.C.2. Raisonnement :

L'intégration continue de petites fonctions et pipelines jusqu'à la production réduit les risques et permet d’avoir un retour précoce au sein des grandes équipes en cas de problèmes d'intégration. Une cadence de livraison rapide et régulière encourage également les équipes à réduire les risques en proposant des tests plus approfondis et de meilleurs résultats.

IV.C.3. Implications :

Les pipelines CI/CD doivent être facilement (ou automatiquement) déclenchés par des événements appropriés dépendant de l’état du code poussé sur le répertoire.

Pour faciliter cela, les points suivants sont également à considérer :

- Les fonctionnalités doivent être clairement traçables dans le contrôle de version en utilisant des techniques d'étiquetage appropriées.
- Les exécutions CI/CD doivent être liées à une livraison de fonctionnalité donnée.
- Les exécutions CI/CD génèrent des journaux ou des sorties clairs qui peuvent être analysés pour isoler les builds en échec ou les erreurs dans les étapes de build, de test et de livraison.

IV.D. (-) Principe C4 : Tests automatisés précoces, complets et appropriés

Anciennement labellisé : ***Principe B4***

IV.D.1. Déclaration :

Les applications doivent être construites à l'aide de tests automatisés qui garantissent la fiabilité à la fois fonctionnelle et non fonctionnelle de la mise en œuvre.

IV.D.2. Raisonnement :

Les bogues logiciels sont inévitables et peuvent être causés par des erreurs de code ou d’analyse.

Des tests précoces garantissent que le logiciel est construit selon les spécifications et que chaque spécification est validée avant d’investir dans de mauvaises solutions.

IV.D.3. Implications :

Ce principe encourage l'utilisation de techniques de développement dirigé par des tests (TDD pour Test-Driven Development en anglais).

Afin de valider rapidement les exigences, il est recommandé d'utiliser le langage du domaine métier lors des tests.

Les premières exigences devraient être rédigées sous une forme qui facilite les tests.

Les équipes devraient suivre la pyramide des tests et mettre en œuvre un niveau de test approprié pour chacune des catégories de tests suivantes :

- unitaire,
- intégration,
- E2E.

Lorsque les services sont interdépendants, il est également conseillé d'envisager des tests centrés sur le consommateur.

IV.E. (-) Principe C5 : Sécurité de type « shift-left »

Anciennement labellisé : ***Principe B5***

IV.E.1. Déclaration :

Le risque global de sécurité de la plateforme est réduit en spécifiant et en respectant les exigences de sécurité dès le début de chaque incrément.

IV.E.2. Raisonnement :

Il a été démontré que l'omission de problèmes de sécurité lors de la conception et de la mise en œuvre d'une solution entraîne souvent un coût et un risque plus élevés pour l'entreprise, car ces problèmes ne sont détectés que plus tard. Les problèmes de sécurité non identifiés dans de tels scénarios présentent un risque plus élevé pour l'entreprise s'ils ne sont pas détectés ou s'ils deviennent des vulnérabilités exploitées ou connues.

IV.E.3. Implications :

En considérant, par incrément, les exigences de sécurité de chaque plateforme et chaque itération logicielle, ce risque est compensé et peut se traduire par une culture de la sécurité d'abord, qui diminue le risque de non-respect des réglementations et de perte de la confiance des patients et des médecins.

Les pratiques suivantes devraient être examinées et adaptées pour permettre une culture de la sécurité de type « shift-left » :

- utiliser les ressources de sécurité actuellement limitées du Consortium (et du secteur dans son ensemble) comme des catalyseurs pour encourager une sécurité de type « shift-left ».
- Utiliser des méthodes pour prendre en compte les exigences non fonctionnelles liées à la sécurité, en fonction du risque, lors de la définition précoce des scénarios et des exigences.
- Effectuer des tests de sécurité continus et automatisés pour réduire le risque dû à une erreur ou à une omission humaine.
- Sensibiliser le personnel à la sécurité et l'encourager à suivre les bonnes pratiques à l'échelle de l'entreprise.

IV.F.(-) Principe C6 : Possibilité d'extension grâce à des fonctionnalités

Anciennement labellisé : ***Principe B6***

IV.F.1. Déclaration :

Tous les composants techniques doivent être conçus pour publier en continu les événements métiers, dont l’apparition déclenche d’autres fonctions métiers.

IV.F.2. Raisonnement :

Les systèmes initialement conçus pour assumer une seule responsabilité peuvent au fil du temps s’étendre à de nouveaux comportements, qui ne sont pas toujours directement liés à la responsabilité d'origine.

De telles extensions peuvent à la fois ralentir le système d'origine, brouiller sa responsabilité et violer le principe de la responsabilité unique.

IV.F.3. Implications :

Les architectures pilotées par les événements simplifient l'extension des systèmes existants avec de nouvelles capacités qui réagissent aux événements métiers qui se produisent ailleurs sur la plateforme. Cela peut également présenter des avantages en termes de performances, grâce à une mise à l'échelle horizontale des abonnés aux événements métiers.

IV.G. (+) Principe C7 : Changement basé sur les exigences

IV.G.1. Déclaration :

Ce n'est qu'en réponse aux besoins du Consortium que des modifications seront apportées aux applications et à la technologie médicale associée.

IV.G.2. Raisonnement :

Ce principe favorisera une atmosphère où l'environnement de l'information change en réponse aux besoins du Consortium, plutôt que de voir une entreprise changer en réponse aux changements informatiques effectués. Il s'agit donc de s'assurer que l'objectif du support d'information, embarqué au sein du processus médical, est bien la base de tout changement proposé.

Les effets imprévus sur l'activité médicale dus aux changements informatiques seront ainsi minimisés.

Un changement de technologie peut fournir une opportunité d'améliorer le processus médical et, par conséquent, de modifier les besoins du Consortium. Néanmoins, ce principe n’est en rien prioritaire en comparaison des **Principe A4 : Adhésion au serment d’Hippocrate** et **Principe A9 : Responsabilité technologique.**

IV.G.3. Conséquences :

Les changements relatifs à la mise en œuvre des technologies informatiques devront suivre un examen complet de la part de l'ensemble des équipes technico-médicales du Consortium.

Il n'y aura pas de financement d'amélioration technique ou de développement de système technologique tiers sans un besoin médical avéré et documenté.

Des processus de gestion du changement conformes à ce principe seront élaborés et mis en œuvre à chaque transition ou migration informatique préconisée.

Ce principe peut se heurter au principe du changement réactif. Néanmoins, celui-ci devra être un critère décisionnel pour atteindre la plus grande valeur-ajoutée possible.

Le Consortium devra s'assurer que le processus de documentation des exigences n'entrave pas les changements réactifs pour répondre aux besoins médicaux légitimes.

L'objectif de ce principe est de maintenir l'accent sur les besoins médicaux, et non sur les besoins technologiques - un changement réactif est également un besoin médical.

IV.H. (+) Principe C8 : Gestion réactive du changement

IV.H.1. Déclaration :

Les modifications apportées à l'environnement d'information du consortium sont mises en œuvre en temps opportun.

IV.H.2. Raisonnement :

Le Consortium met en œuvre des systèmes d'information adaptés aux différents soins prodigués à un patient et imposera que ces systèmes d'information, utilisés quotidiennement par des personnels médicaux, répondent à leurs besoins.

IV.H.3. Conséquences :

Des processus de gestion et de mise en œuvre du changement doivent être développés, afin que l'adaptation à ce changement ne créent pas de manquement vis à vis des soins prodigués à un patient.

Un personnel médical ressentant un besoin de changement devra communiquer avec un "spécialiste médical" pour faciliter l'explication et la mise en œuvre de ce besoin.

Si des modifications doivent être apportées, l'architecture associée doit être maintenue à jour.

L'adoption de ce principe pourrait nécessiter des ressources supplémentaires et pourrait entrer en conflit avec d'autres principes. Il conviendra donc au personnel médical d'étayer ce besoin et au Consortium de décider quant à sa prise en compte.

IV.I. (+) Principe C8 : Maîtrise de la diversité technique

IV.I.1. Déclaration :

La diversité technologique est contrôlée pour minimiser le coût du maintien de l'expertise et de la connectivité entre plusieurs environnements de traitement.

IV.I.2. Raisonnement :

Il existe un coût réel, non négligeable, de l'infrastructure requise pour prendre en charge les technologies alternatives pour les environnements de traitement. D'autres coûts d'infrastructure sont encourus pour maintenir l'interconnexion et la maintenance de plusieurs constructions de processeurs.

A cet état de fait, le Consortium s’impose de limiter le nombre de composants pris en charge pour simplifier leur maintenabilité et en ainsi en réduir les coûts d’exploitation.

Les avantages médicaux d'une diversité technique minimale comprennent :

- un conditionnement standard des composants ;
- un impact prévisible de la mise en œuvre ;
- des évaluations et des rendements prévisibles ;
- des tests redéfinis et maintenus à jour afin qu’ils soient toujours les plus pertinents possibles ;
- un statut d'utilité ;
- une flexibilité accrue pour s'adapter aux progrès technologiques.

Une technologie commune à l'ensemble du Consortium apportera les avantages des économies d'échelle à celui-ci. Les coûts d'administration technique et de support en seront mieux maîtrisés lorsque des ressources limitées seront concentrées sur l’ensemble des technologies communes et partagées.

IV.I.3. Conséquences :

Les politiques, les normes et les procédures qui régissent l'acquisition de la technologie doivent être directement liées à ce principe.

Les choix technologiques seront limités par les choix disponibles dans le plan technologique.

Des procédures visant à augmenter l'ensemble de technologies médicales, acceptables pour répondre aux exigences en constante évolution, devront être élaborées et mises en place.

La base technologique n'est jamais gelée.

Les avancées technologiques sont toujours les bienvenues et modifieront le modèle technologique lorsque la compatibilité avec l'infrastructure actuelle, l'amélioration de l'efficacité opérationnelle ou une capacité médicale requise aura été démontrée.

IV.J. (+) Principe C9 : Interopérabilité

IV.J.1. Déclaration :

Les logiciels et le matériel médical doivent être conformes aux normes définies qui favorisent l'interopérabilité des données, des applications et de la technologie.

IV.J.2. Raisonnement :

Les normes aident à assurer la cohérence, améliorant ainsi la capacité à gérer les systèmes et à améliorer la satisfaction des patients, et à protéger les investissements technologiques existants, maximisant ainsi le retour sur investissement et réduisant les coûts. Les normes d'interopérabilité aident, en outre, à assurer le support de plusieurs fournisseurs pour leurs produits et facilitent l'intégration de la chaîne d'approvisionnement.

IV.J.3. Conséquences :

Les normes d'interopérabilité des systèmes, dont notamment les normes médicales, seront suivies à moins qu'il n'y ait une raison médicale impérieuse de la mise en œuvre d’une solution non standard ; par exemple, ceci pourrait s’avérer dans un contexte au sein duquel le **Principe A4 : Adhésion au serment d’Hippocrate** viendrait imposer des processus non standards impérieux vis à vis des soins prodigués au patient.

Un processus pour établir des normes, les examiner, les réviser périodiquement et accorder des exceptions doit être établi.

Les systèmes technologiques existants doivent être identifiées et documentées.

V.Principes de données

V.A. (+) Principe D1 : Données en tant qu’atouts

V.A.1. Déclaration :

Les données sont un actif qui a de la valeur pour l'entreprise et qui est gérée en conséquence.

V.A.2. Raisonnement :

Les données sont une ressource du Consortium précieuse; ayant une valeur réelle et mesurable. En termes simples, la finalité des données est d'aider à la prise de décision. Des données précises et opportunes sont essentielles pour prendre des décisions précises et opportunes, peu importe le contexte d’application.

Les actifs du Consortium seront gérés avec soin, et les données n’y feront pas exception.

Les données sont le fondement de la prise de décision, le Consortium gérerera donc soigneusement ses données pour s’assurer de :

- leur positionnement,
- leur authenticité,
- leur exactitude,
- leur disponibilité.

V.A.3. Conséquences :

Ce principe représente un pilier de ceux régissant les données :

- **les données sont un atout,**
- les données sont partagées,
- les données sont facilement accessibles.

En conséquence, le Consortium s’engage à fournir la formation indispensable, nécessaire et suffisante au personnel médical le constituant. Cet engagement de formation a pour objectif de s'assurer que tout le personnel médical du Consortium comprenne la relation entre la valeur des données, leur partage et leur accessibilité.

Ainsi, en prenant en compte le fait que les données sont un actif de valeur pour l'ensemble du Consortium, des responsables de la bonne gestion de ces données seront affectés à des postes pertinents pour l’amélioration des soins prodigués à un patient par le personnel médical du Consortium. Ces intendants, ou responsable de données, auront l'autorité et les moyens de gérer les données dont ils sont responsables.

En délégant cette responsabilité, le Consortium s’assura de mettre en place une politique de transition culturelle pour passer d’un mode de pensée de *« propriété des données »* à celle d’une *« intendance des données »*.

Ce rôle de responsable de données est essentie ; des données obsolètes, incorrectes ou incohérentes pourraient être transmises au personnel médical et affecter négativement les décisions dans l'ensemble du Consortium. Cela pourrait même avoir des répercutions sur la prise en charge d’un patient.

Une partie du rôle du responsable de données est de s'assurer la qualité de celles-ci.
Des procédures seront développées et utilisées pour :

- prévenir et corriger les erreurs dans les informations ;
- améliorer les processus qui produisent des informations erronées.

En outre, la qualité des données devra être mesurée : ces métriques serviront alors à mettre en place des mesures d'amélioration de la qualité de ces données ; il est d'ailleurs probable que des politiques et des procédures seront également élaborées à cet effet.

Enfin, un forum avec une représentation complète, à l'échelle du Consortium, devra décider des changements de processus suggérés par les délégués syndicaux représentant le personnel médical.

V.B. (+) Principe D2 : Partage des données

V.B.1. Déclaration :

Le personnel médical a accès aux données nécessaires à l'exercice de ses fonctions.
Par conséquent, les données sont partagées entre les fonctions et les équipes du Consortium, après avoir pris en compte le besoin d'en connaitre.

V.B.2. Raisonnement :

L'accès rapide à des données précises est essentiel pour améliorer la qualité et l'efficacité de la prise de décision médicale.
Axiome : il est moins coûteux de conserver des données précises et actualisées dans une seule application, puis de les partager, que de conserver des données en double dans plusieurs applications.
Au vu de la quantité de données disponibles au sein du Consortium, celles-ci seront stockées au sein d'un système de gestion de base unique.
La vitesse de collecte, de création, de transfert et d'assimilation des données sera proportionnelle à la capacité du Consortium à partager efficacement l'ensemble de ces mêmes données. Celles-ci devront donc être partagées pour traduire la volonté de prendre les meilleures décisions possibles en s'appuyant sur le moins de sources possibles. En effet, la gestion centralisées des données les rendra plus précises et opportunes pour l'ensemble du personnel médical en charge de cette prise de décision.
En outre, les données partagées électroniquement se traduiront par une efficacité accrue lorsque les entités de données existantes pourront être utilisées, sans ressaisie, pour créer de nouvelles entités.

V.B.3. Conséquences :

Ce principe représente un pilier de ceux régissant les données :

- les données sont un atout,
- **les données sont partagées,**
- les données sont facilement accessibles.

En conséquence, le Consortium s’engage à fournir la formation indispensable, nécessaire et suffisante au personnel médical le constituant. Cet engagement de formation a pour objectif de s'assurer que tout le personnel médical du Consortium comprenne la relation entre la valeur des données, leur partage et leur accessibilité.

Pour permettre le partage des données, le Consortium devra développer et respecter un ensemble commun de politiques, de procédures et de normes régissant la gestion et l'accès aux données médicales et techniques à court et à long terme.

À court terme, en prenant en compte l’investissement important des systèmes hérités par chacune de entreprises, le Consortium devra lui-même investir dans des logiciels capables de migrer ces données du système hérité vers un environnement de données partagé.

Il développera également des modèles de données standard, des éléments de données et d'autres métadonnées définissant l’environnement partagé. De plus, le Consortium réalisera un système de référentiel unique pour stocker ces métadonnées afin de les rendre accessibles.

À long terme, à mesure que les anciens systèmes seront remplacés, le Consortium adoptera et appliquera des politiques et des directives communes d'accès aux données. Ainsi, les développeurs de nouvelles applications pourront garantir que les données de ces nouvelles applications :

- restent disponibles pour l'environnement partagé
- continuent à être utilisées par ces nouvelles applications.

À court et à long terme, le Consortium adoptera des méthodes et des outils communs pour créer, maintenir et accéder à ses données partagées.

Le partage de données nécessitera un changement culturel important ; ce principe de partage de données se heurtera continuellement au principe de sécurité des données, pour lequel, en aucun cas, le principe de partage de données ne devra compromettre des données confidentielles.

Les données mises à disposition pour le partage pourront être utilisées par le personnel médical pour préparer et/ou exécuter les soins les plus pertinents et adaptés pour le patient.

L’application de ce principe garantira que seules les données les plus précises et les plus récentes seront utilisées pour la prise de décision. Les données partagées deviendront la *« source unique virtuelle »* de données à l'échelle du Consortium.

V.C. (+) Principe D3 : Accessibilité des données

V.C.1. Déclaration :

Les données sont accessibles au personnel médical pour exécuter leurs fonctions.

V.C.2. Raisonnement :

Un large accès aux données conduit à l'efficience et à l'efficacité de la prise de décision médicale et permet une réponse rapide aux demandes d'informations et à la prestation de services de soin.
L'utilisation des informations doit être considérée, du point de vue du Consortium, pour permettre l'accès à une grande variété de spécialités médicales ; le temps du personnel médical est alors économisé et la cohérence des données est améliorée.

V.C.3. Conséquences :

Ce principe représente un pilier de ceux régissant les données :

- les données sont un atout,
- les données sont partagées,
- **les données sont facilement accessibles.**

En conséquence, le Consortium s’engage à fournir la formation indispensable, nécessaire et suffisante au personnel médical le constituant. Cet engagement de formation a pour objectif de s'assurer que tout le personnel médical du Consortium comprenne la relation entre la valeur des données, leur partage et leur accessibilité.

Ainsi, l'accessibilité implique la facilité avec laquelle le personnel médical obtient des informations.

La manière dont ces informations sont accessibles et affichées doit être suffisamment adaptable pour répondre à un large éventail de spécialité médicale et leurs méthodes d'accès correspondantes.

L'accès aux données ne constitue pas une compréhension des données : le personnel doit veiller à la bonne interprétation de l’information.

L'accès aux données n'accorde pas nécessairement au personnel médical des droits d'accès pour modifier ou divulguer les données.

Ces concepts de Sécurité nécessiteront un processus de formation et un changement dans la culture organisationnelle. Ainsi, le Consortium définira et mettra en œuvre une politique de transition culturelle pour passer d’un mode de pensée de *« propriété des données »* à celle d’une *« intendance des données »*.

V.D. (+) Principe D4 : Intégrité des données

V.D.1. Déclaration :

Chaque élément de données a un administrateur responsable de la qualité des données.

V.D.2. Raisonnement :

L'un des avantages d'un environnement architecturé est la possibilité de partager des données (par exemple, du texte, de la vidéo, du son, etc.) au sein du Concortium.

À mesure que le degré de partage des données augmente et que les spécialités médicales s'appuient sur des informations communes, il devient essentiel que seul l'administrateur des données prenne des décisions sur le contenu des données.

En prenant en compte la perte d’intégrité des données saisies plusieurs fois, le dépositaire de ces données sera seul responsable de la saisie des données, ce qui élimine les efforts humains et les ressources de stockage de données redondants.

Nota: un administrateur de données est différent d'un responsable de données. Un administrateur de données est responsable de l'exactitude et de l'actualité des données, tandis que le responsabilité de données a à sa charge des tâches de normalisation et de définition des données.

V.D.3. Conséquences :

La tutelle réelle résout les problèmes de "*propriété*" des données et permet aux données d'être disponibles pour répondre aux besoins de toule personnel médical.

Cet axoime implique qu'un changement culturel de la « *propriété* » des données à la « *tutelle* » des données est nécessaire.

Ainsi, le dépositaire des données sera responsable du respect des exigences de qualité imposées sur les données dont il est lui-même est responsable.

De plus, l'administrateur de données doit avoir la capacité de donner confiance au personnel médical dans les données, en affichant, par exemple, l’attribut relatif à la "*source de données*" dont elles sont issues.

Le Consortium devra identifier une véritable source des données unique afin que l'autorité responsable des données puisse se voir attribuer cette responsabilité de dépositaire. Cela ne signifie pas que les sources classifiées seront révélées ni que la source en sera forcément le dépositaire.

Les informations doivent être saisies électroniquement une seule fois et immédiatement validées aussi près que possible de la source.

Des mesures de contrôle de la qualité doivent être mises en place pour assurer l'intégrité des données. En raison du partage de données au sein du Consortium, l'administrateur de données est comptable et responsable de l'exactitude et de l'actualité de ses éléments de données désignés. Il est de la responsabilité du consortium de reconnaître l'importance de cette responsabilité de tutelle.

V.E. (+) Principe D5 : Vocabulaire commun et définitions de données

V.E.1. Déclaration :

Les données sont définies de manière cohérente au sein du Consortium ; les définitions sont compréhensibles et disponibles pour tout le personnel médical.

V.E.2. Raisonnement :

Les données qui seront utilisées dans le développement des applications doivent avoir une définition commune à l'ensemble du Consortium pour permettre le partage des données.

Un vocabulaire commun facilitera les communications et permettra au dialogue d'être efficace.

De plus, il est nécessaire d'interfacer les systèmes et d'échanger des données.

V.E.3. Conséquences :

L’existence de poste intitulé "*administrateur de données*" et de forums avec des chartes impliquant une telle responsabilité ne doit pas être dénué de sémantique.

Un apport d’énergie et de ressources supplémentaires importantes doivent être consacrées à cette seule tâche ; ces efforts visant à améliorer l'environnement de l'information.

Ce principe est, à la fois, distinct et lié à la question de définition des éléments de données, tels que la constitution d’un vocabulaire et de définitions communs.

Le Consortium établira le vocabulaire commun initial pour le métier en prenant en compte les spécificités médicales représentées.

En ce qui concerne les définitions, elles devront être utilisées uniformément au sein du Consortium.

Chaque fois qu'une nouvelle définition de données est requise, l'effort de définition sera coordonné et réconcilié avec un "*glossaire*" comprenant les descriptions de données impliquées.

Les administrateurs de données du consortium assureront cette coordination.

Les ambiguïtés résultant de multiples définitions paroissiales des données céderont la place à des définitions et à une compréhension acceptées à l'échelle du Consortium.

Plusieurs initiatives de normalisation des données doivent être coordonnées.

Des responsabilités fonctionnelles en matière d'administration des données seront attribuées.

V.F. (+) Principe D6 : Sécurité des données

V.F.1. Déclaration :

Les données sont protégées contre toute utilisation et divulgation non autorisées.

Outre les aspects traditionnels de la classification de sécurité nationale, cela inclut, sans s'y limiter, la protection des informations :

- pré-décisionnelles,
- sensibles,
- sensibles à la sélection des sources,
- exclusives.

V.F.2. Raisonnement :

Le partage ouvert d'informations et la diffusion d'informations médicales, via la législation pertinente, doivent être mis en balance avec la nécessité de restreindre la disponibilité d'informations classifiées, exclusives et sensibles.

Les lois et réglementations existantes exigent la sauvegarde de la sécurité nationale et de la confidentialité des données, tout en permettant un accès libre et ouvert : le patient a accès aux informations qui le concerne. Les informations pré-décisionnelles (travail en cours, dont la diffusion n'est pas encore autorisée) doivent être protégées pour éviter les spéculations injustifiées, les interprétations erronées, les utilisations inappropriées ou toute autre sorte de tracas pour le patient.

V.F.3. Conséquences :

L'agrégation des données, classifiées ou non, créera une cible importante nécessitant des procédures d'examen et de déclassification, avec l’autorisation du patient, pour maintenir un contrôle approprié.

Le patient et/ou lepersonnel médical doivent déterminer si l'agrégation entraîne une augmentation du niveau de classification. Une politique et des procédures appropriées seront nécessaires pour gérer cet examen et cette déclassification. L'accès à l'information fondé sur une **politique du besoin d'en connaître** forcera des examens réguliers de l'ensemble de l'information.

A l’échelle du Consortium, il ne conviendra pas de pratiquer le sillotage de données au sein de systèmes séparés contenant différents niveaux de classifications...

En ce qui concerne la séparation des informations dites « *sensibles* »: afin de fournir un accès adéquat à des informations, tout en maintenant un certain niveau de sécurité au sein du système d’information, **ces besoins de sécurité seront identifiés et développés au niveau des données**, et non au niveau de l'application. Des mesures de sécurité des données seront mises en place pour restreindre l'accès au moyen de différents libellés r’affichage, tels que « *afficher uniquement* » ou « *secret médical* ». L'étiquetage de sensibilité pour l'accès aux informations pré-décisionnelles, décisionnelles, classifiées, sensibles ou exclusives doit être déterminé en amont de création de la données. Ainsi, la sécurité sera intégrée aux éléments de données dès le départ et ne saurait être ajouté plus tard.

Les systèmes, les données et les technologies doivent être protégés contre l'accès et la manipulation non autorisés. Les informations du Consortium doivent être protégées contre toute altération, sabotage, catastrophe ou divulgation accidentelle ou non autorisée.

De nouvelles politiques nécessaires seront instaurées pour gérer la durée de protection des informations pré-décisionnelles et d'autres travaux en cours, en tenant compte de la fraîcheur du contenu et des décisions du patient.


MedHead