AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

PGSSI-S : Politique générale de sécurité des systèmes d'information de santé « Référentiel de gouvernance et de mise en œuvre de la PGSSI-S»

Version pour concertation publique

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T.+33 (0)1 58 45 32 50
esante.gouv.fr

Agir ensemble pour soigner mieux

Sommaire

1 Propos liminaires

Le développement rapide de l'usage des technologies de l'information dans le domaine de la santé constitue un facteur important d'amélioration de la qualité des soins. Il s'accompagne toutefois d'un accroissement significatif des menaces et des risques d'atteinte aux informations conservées sous forme électronique et plus généralement aux processus de santé s'appuyant sur les systèmes d'information de santé (SIS).

Conscient de ces enjeux et face à ces risques, l'Etat élabore une politique générale de sécurité des systèmes d'Information de santé (PGSSI-S), **en concertation avec l'ensemble des acteurs partie prenante**, afin de fixer le cadre de la sécurisation des SIS.

La mise en œuvre de la PGSSI-S permettra notamment de renforcer la confiance et l'adhésion des professionnels, des patients et plus largement du grand public.

La méthode d'élaboration de la PGSSI-S est donc conçue pour prendre en compte les besoins et aussi les contributions de tous les acteurs du secteur.

2 Icône utilisée dans le document

📖 : Référence aux textes normatifs

3 Objet de la PGSSI-S

La PGSSI-S est **un corpus documentaire** définissant et organisant les exigences incontournables en matière de sécurité s'appliquant à tout SIS, dans le **respect des droits du patient. Elle tend à fixer des contraintes opérationnelles et économiques cohérentes pour l'ensemble des acteurs du secteur**.

Par l'ensemble de ses documents, la PGSSI-S décline les différentes thématiques et règles abordées par la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS).

Afin de rendre pleinement lisible l'articulation entre la PGSSI-S et la PSSI-MCAS, chaque document PGSSI-S fera référence aux règles PSSI-MCAS qu'il décline.

La PSSI-MCAS est elle-même déclinée de la politique de sécurité des systèmes d'information de l'Etat (PSSIE).

En outre, chaque document de la PGSSI-S tient compte du cadre juridique applicable à l'objet qu'il traite, relevant tant du droit interne que du droit européen.

3.1 Champ d'application de la PGSSI-S

🕮 Article L1110-4-1 créé par LOI n° 2016-41 du 26 janvier 2016 - art. 96 (V)

« Afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, les établissements et services de santé, les hébergeurs de données de santé à caractère personnel et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés. »

Le champ d'application de la PGSSI-S est déterminé par la combinaison de trois critères fixés à l'article L1110-4-1 du code de la santé publique.

3.1.1 Les personnes concernées

Sont tenus de l'appliquer les professionnels de santé visés à la quatrième partie du code de la santé publique, les établissements et services de santé de la sixième partie du code de la santé publique.

L'offre de soins, entendue au sens large, prend également de nombreuses autres formes désignées par l'expression « *tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social* ». Sont ainsi visées toutes les structures de soins, telles que les maisons et centres de santé mais aussi les laboratoires de biologie médicale, les services de protection maternelle infantile ou encore les services de santé au travail. Ces structures ne sont pas toutes régies par le code de la santé publique. Néanmoins, des actes de prévention de diagnostic, de soins ou de suivi social et médico-social y sont réalisés par des professionnels habilités et nécessitent que les données de santé ainsi produites soient préservées dans les mêmes conditions de sécurité et de confidentialité.

Les référentiels de sécurité et d'interopérabilité de l'article L1110-4-1 s'appliquent par conséquent à toutes les personnes physiques et morales relevant du secteur sanitaire et du secteur social et médico-social, dès lors qu'elles contribuent à la réalisation d'acte de prévention, de soins ou du suivi social et médico-social d'une personne, dans le cadre d'activités précisées au 3.1.2 et d'usage de systèmes d'information précisés au 3.1.3.

Les hébergeurs de données de santé à caractère personnel sont également soumis à ces référentiels de l'article L1110-4-1. Sont hébergeurs, en application de l'article L1111-8 du code de la santé publique, les personnes dont l'activité consiste à héberger des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou pour le compte du patient lui-même.

Les assureurs dans le cadre de leur activité consacrée au remboursement des soins ne sont pas concernés. Ils entrent en revanche dans le champ d'application dès lorsqu'ils mettent en place un programme d'éducation thérapeutique dans les conditions fixées notamment par l'article L.1161-2 du code de la santé publique en tant qu'organisme participant à la prévention, aux soins ou au suivi médico-social et social .

3.1.2 Activités concernées

Il résulte de la liste des personnes concernées décrites ci-dessus que les référentiels de sécurité et d'interopérabilité de l'article L1110-4-1 s'appliquent aux activités de prise en charge sanitaire et de suivi social et médico-social des personnes, ce qui recouvre tout acte de prévention, diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur, de prévention de perte d'autonomie.

Sont également couvertes toutes les activités qui en constituent les accessoires indispensables ou qui s'inscrivent dans leur prolongement direct :

- les activités dites supports telle que la facturation des actes;
- les actes de coordination des actes de prévention, de soins ou de suivi social et médico-social;
- les activités d'étude, de recherche et d'évaluation.

Les référentiels s'appliquent à toute activité, quel que soit son ressort territorial. Ainsi, comme le rappelle l'article R. 1111-27 du code de la santé publique, le dossier médical partagé (DMP), dossier national de coordination des soins dont la Caisse nationale d'assurance maladie des travailleurs salariés est le responsable de traitement, doit être conforme aux référentiels de l'article L. 1110-4-1.

3.1.3 Les systèmes d'information concernés

Les référentiels s'appliquent à tout système d'information utilisé par ces personnes, physiques ou morales, qui ont pour finalité le traitement, la conservation sur support informatique et la transmission par voie électronique des données de santé à caractère personnel.

Cela inclut toutes les fonctionnalités liées à la prise en charge des personnes. Sont également intégrées les fonctionnalités accessoires, c'est-à-dire toutes les fonctionnalités relative à la gestion administrative des personnes concernées, dont la facturation , dès lors qu'elles sont mises en œuvre sous la responsabilité des personnes décrites au point 3.1.1 et qu'elles sont nécessaires pour la prise en charge des personnes.

A titre d'illustration, entrent ainsi dans le champ d'application des référentiels de sécurité et d'interopérabilité les systèmes d'information mis en œuvre par les utilisateurs visés au point 3.1.1 contribuant notamment à :

- la gestion du dossier patient
- la facturation,
- la gestion du PMSI ;
- la gestion de la médecine du travail.

Les utilisateurs de ces systèmes d'information n'en sont pas nécessairement les responsables du point de vue juridique. Cela dépend en effet des modalités d'exercice professionnel de l'utilisateur.

Les contours du champ d'application de la PGSSI-S peuvent également être éclairés par la lecture du considérant 35 du règlement européen (UE) 2016/679, qui précise la notion de donnée de santé et de façon indissociable les traitements qui en manipulent :

- traitements qui collectent lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil (1) au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé;
- traitements gérant des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un établissement de santé, d'un dispositif médical ou d'un test de diagnostic in vitro.

Il est rappelé que les systèmes d'informations concernés sont composés d'actifs très divers représentant tous un facteur de risque à prendre en compte.

4 Les responsables de la mise en œuvre des référentiels de la PGSSI-S

Les référentiels de sécurité et d'interopérabilité ont pour finalité de veiller à la qualité et à la sécurité des données de santé à caractère personnel et à leur protection dès lors qu'elles sont traitées, conservées sur support informatique ou transmises par voie électronique.

Quelles que soient l'organisation et les modalités d'exercice professionnel de chacune des personnes visées par l'article L1110-4-1, l'obligation de mise en œuvre des référentiels de sécurité et d'interopérabilité pèse sur le responsable de traitement au sens de l'article 3 de la loi n°78-17 du 6 janvier 1978 modifiée dite loi Informatique et libertés.

📖 **Article 3 de la loi n°78-17 du 6 janvier 1978 modifiée dite loi Informatique et libertés**

« Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. »

«Responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre; »

Article 4-7° du règlement européen (UE) 2016/679 relatif à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données abrogeant la directive 95/46/CE (règlement général sur la protection des données personnelles) dit RGDP dans la suite du présent document

Aux fins du présent règlement , on entend par «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

Article 26 du RGDP - *Responsables conjoints du traitement*

1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

3.Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement.

L'organisation de la sécurité du système d'information par les personnes visées à l'article L. 1110-4-1 doit être conforme aux exigences exposées au quatrième chapitre de la PSSI-MCAS.

4.1 L'identification du responsable de traitement

L'identification du responsable de traitement dépend des modalités d'exercice professionnel.

Sous réserve d'une analyse au cas par cas, un professionnel de santé exerçant seul et qui est intégralement responsable du choix des moyens informatiques qu'il utilise, est le responsable du traitement des données à caractère personnel.

Dans l'hypothèse dans laquelle un professionnel de santé exerce dans un contexte collectif (cabinet de groupe, EHPAD, laboratoire, réseau de soins, pôle de santé, ...) et utilise des moyens informatiques mutualisés ou mis à disposition par la structure, le responsable du traitement peut être soit le professionnel de santé lui-même soit la structure prise en la personne de son représentant légal (le directeur dans un établissement public de santé, par exemple). La désignation du responsable de traitement doit être effectuée au cas par cas, pour déterminer celui qui dispose du choix de la finalité et des moyens informatiques.

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès (article 34 de la loi Informatique et libertés).

Ces mesures doivent être prises en veillant au respect des référentiels de la PGSSI-S.

4.2 Les contours de la responsabilité du responsable de traitement

Le responsable de traitement agit dans un écosystème complexe, au sein duquel il noue des relations avec de nombreux intervenants qui contribuent directement ou indirectement à la prise en charge des personnes. En cas de contentieux, il appartiendra au juge d'apprécier au cas d'espèce la répartition des responsabilités des différents intervenants.

L'exemple de l'écosystème des objets connectés recourant à internet illustre ce constat d'une multiplicité d'acteurs allant du fabricant, en passant par les agrégateurs des données, les développeurs d'applications, les fournisseurs de réseau, les prestataires de cloud, jusqu'au professionnel de santé. Il en résulte une multiplicité des responsables potentiels à l'égard des obligations relatives au respect de la confidentialité et de la sécurité des données de santé.

Cela souligne l'importance de clarifier au plus tôt la qualité de responsable de traitement dans tout projet de système d'information traitant de donnée de santé.

4.3 Point d'attention sur les relations contractuelles avec les prestataires

Il importe pour le professionnel de santé, ou la structure dans laquelle il exerce, qui assume la qualité de responsable de traitement, de veiller à la nature et à l'encadrement des relations qu'il noue avec les intervenants de l'écosystème et tout particulièrement des prestataires de services auxquels il a recours pour réaliser son activité.

Ces prestataires établissent fréquemment des contrats standards, ne tenant pas forcément compte des référentiels de sécurité et d'interopérabilité.

Le professionnel de santé, ou la structure dans laquelle il exerce, en qualité de responsable du traitement de données à caractère personnel, doit veiller à ne pas accepter de clauses et conditions contractuelles qui seraient contraires aux règles relatives à la protection des données de santé à caractère personnel, dont relèvent les référentiels de sécurité et d'interopérabilité de l'article L1110-4-1 du code de la santé publique.

5 Opposabilité des référentiels de la PGSSI-S

5.1 Principes généraux

La loi n° 2009-879 du 21 juillet 2009 dite loi HPST a introduit les référentiels de sécurité et d'interopérabilité définis par l'ASIP Santé (L1111-8 alinéa 4). D'autres référentiels étaient également prévus par l'article L1110-4. Le nouvel article L1110-4-1 du code de la santé publique dans sa rédaction issue de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé a fusionné ces deux articles en un seul.

Ces référentiels de sécurité et d'interopérabilité sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés. L'arrêté rend ainsi ces référentiels opposables.

L'opposabilité a pour effet juridique de rendre le texte contraignant, de lui donner force obligatoire. Concrètement, l'administration, comme les administrés, pourront s'en prévaloir, y compris dans le cadre d'un recours contentieux, pour défendre leurs intérêts respectifs. Un texte est dit opposable à la date de sa publication au Journal Officiel, sauf dispositif spécial reportant l'entrée en vigueur.

Seuls les documents dont le contenu a acquis une maturité suffisante et porteurs d'un sujet nécessitant de veiller à une homogénéité des mesures mises en œuvre par les acteurs de terrain ont vocation à être rendus opposables par voie d'arrêté.

Ce sont les référentiels dits thématiques de la PGSSI-S (référentiel d'authentification, etc.).

Les documents qui n'ont pas vocation à être rendu opposables sont des guides représentant un état de l'art à respecter dans le cadre de la sécurisation des systèmes d'information de santé. Il s'agit de documents d'information et d'aide pour une utilisation sécurisée de l'informatique de santé. Ce sont des outils juridiques permettant de répondre aux nouvelles situations suscitées par le développement des nouvelles technologies appliquées à la santé. Ils constituent une réponse à la volatilité et vélocité des nouvelles technologies appliquées au secteur de la santé. Ils permettent de guider les acteurs de terrain, tout en accompagnant et encadrant l'effort d'innovation.

5.2 Conséquence de l'opposabilité du référentiel de gouvernance et de mise en œuvre

S'il est de la responsabilité de chaque responsable de SIS de déterminer les conditions d'application d'un référentiel thématique à sa situation particulière, le Ministère des Affaires Sociales et de la Santé est responsable, en application du présent référentiel de gouvernance et de mise en œuvre, du contenu des référentiels dans la limite des missions décrites au point 7 relatif à la méthode d'élaboration de la PGSSI-S.

5.3 Typologie des documents

Les documents publiés de la PGSSI-S sont donc divisés en 2 catégories :

- des référentiels opposables ou à vocation opposable ; c'est à dire des documents à vocation normative qui, sont ou seront rendus opposables par arrêté ministériel.
- des guides non opposables ; c'est-à-dire des documents d'information et d'aide pour une utilisation sécurisée de l'informatique de santé.

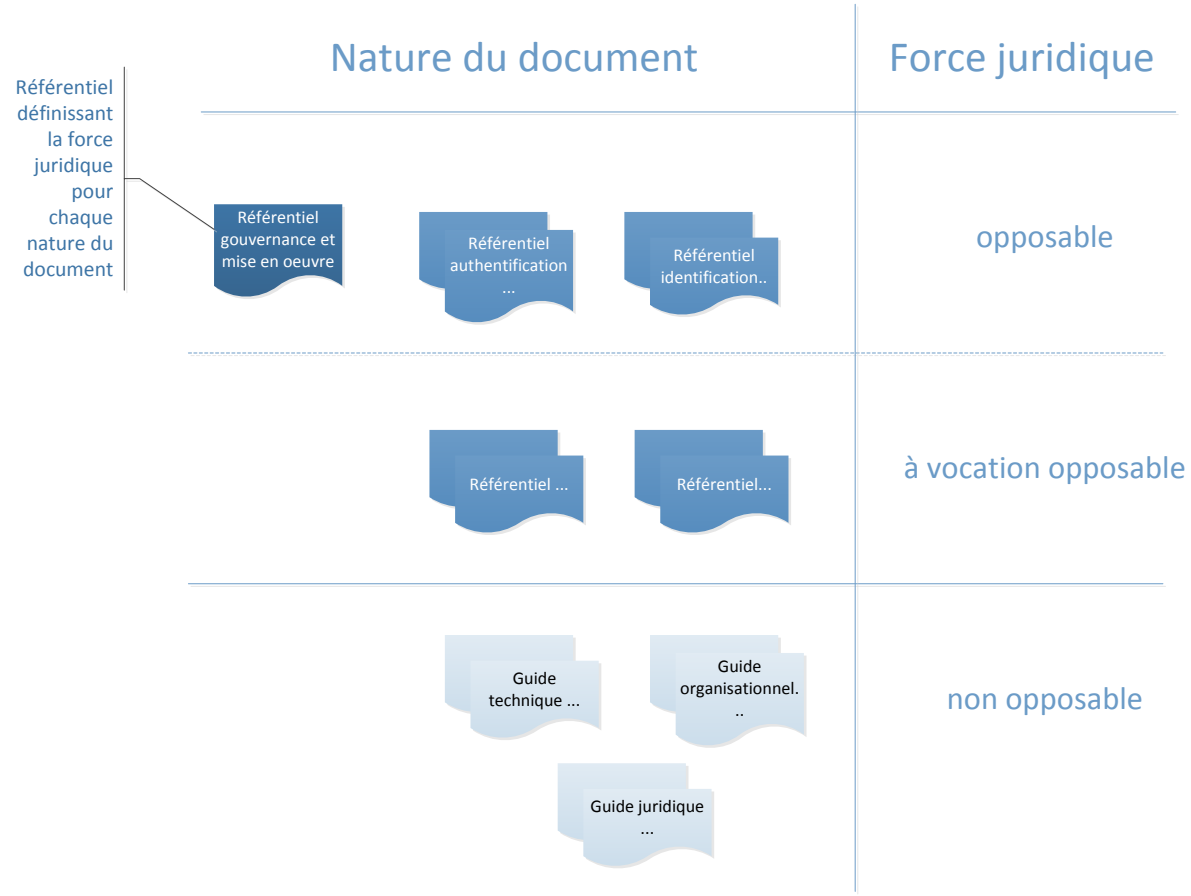

Figure 1: force juridique des documents

6 Présentation de la logique de paliers et des contextes d'applicabilité

Compte tenu de la diversité de l'existant et du niveau actuel de maturité en matière de sécurité du secteur sanitaire et médico-social, il apparait opportun de fournir aux responsables de SIS la possibilité de progresser par palier d'exigence.

Les paliers constituent les niveaux de maturité de la sécurité des systèmes d'information de santé. Ils permettent aux responsables de traitement de situer la réalité opérationnelle de leur système selon les niveaux de maturité et d'élaborer une trajectoire vers le palier identifié comme cible pour leur traitement.

A chaque palier, le document définit un ensemble cohérent de mesures de sécurité répondant progressivement à la couverture de plus en plus importante de risques de sécurité.

Chaque montée de palier correspond à la prise en compte d'un nombre croissant de risques pour le système d'information et /ou la prise en compte du temps de déploiement pour mettre en œuvre les mesures de sécurité.

6.1 Principe de trajectoire pour les référentiels

Chaque référentiel, sauf le présent référentiel relatif à la gouvernance et à la mise en œuvre de la PGSSI-S, présente différents niveaux d'exigences, appelés « paliers » dont le contenu a été établi conformément au processus de concertation décrit au point 7.

Les paliers sont présentés en ordre croissant.

Le premier palier n'est pas systématiquement le niveau minimum d'exigences à atteindre.

Le palier minimum à atteindre est déterminé par la combinaison de deux critères :

- le contexte d'applicabilité ;
- le cas échéant, l'obligation légale.

Le dernier palier représente la cible optimale de l'organisation.

Les paliers intermédiaires indiquent la trajectoire pour atteindre la cible optimale

6.1.1 Les grilles d'applicabilité

Des contextes d'applicabilité déterminent pour chaque référentiel le palier minimum à appliquer. Ces contextes sont synthétisés dans une grille d'applicabilité annexée à chaque référentiel.

Les grilles d'applicabilité peuvent être différentes selon les référentiels.

Les grilles d'applicabilité sont le point d'entrée pour les décideurs en charge de choix des paliers des référentiels.

6.1.2 Modification des paliers lors d'une mise à jour en version majeure

Le cycle de révision des référentiels présenté en §7.2 peut amener à une modification des valeurs de palier minimum ainsi que des dispositifs associés.

Lorsqu'un palier minimum a été modifié pour un ou plusieurs référentiels, les structures et les établissements de santé ont obligation de s'aligner sur les nouvelles exigences.

Ces nouvelles exigences doivent être prises en compte lors de l'analyse de risque suivant la date de mise à jour du ou des référentiels concernés.

La durée nécessaire de mise en œuvre d'un changement de palier par les acteurs concernés sera estimée par les groupes de travail et soumis à concertation.

6.1.3 Obligation de répondre aux exigences des référentiels

Les responsables du système d'information de santé ont pour obligation de réaliser une analyse de risque avant toute mise en œuvre d'un SIS afin de déterminer la pertinence du niveau de palier choisi pour chaque référentiel.

Une revue annuelle des modifications de contexte et des changements majeurs du SIS est requise afin de déterminer la nécessité d'une mise à jour de l'analyse de risque initiale.

Cette analyse de risque peut être mutualisée avec des demandes issues d'autres dispositifs tels que le programme Hôpital Numérique, ou encore le règlement européen sur la protection des données publié au Journal Officiel de l'Union Européenne le 4 mai 2016.

Toutefois, en cas de changement de paliers, il ne peut pas être imposé le renouvellement d'une homologation ou d'une certification du SIS avant la date fixée par l'autorité en charge de cette homologation ou de cette certification.

6.2 Principe de trajectoire pour les guides

6.2.1 Principe de paliers non obligatoire pour les guides

Dès que cela est possible, la logique de palier décrite pour les référentiels est appliquée aux guides de la PGSSI-S.

Toutefois, quand cela est jugé inadéquat, certains guides n'incluent pas cette notion de trajectoire.

6.2.2 Choix du palier pour les guides

Il appartient aux responsables du SIS d'apprécier quel palier d'un guide correspond à son organisation et aux moyens mobilisables lors de la mise en œuvre de son SIS.

Ce choix n'est pas obligatoirement à inscrire dans une analyse de risque formelle. Toutefois, le responsable de traitement doit peser les risques juridiques encourus si une situation d'écart avec un palier minimum d'un guide, cause d'un incident de sécurité, est constatée.

7 Méthode d'élaboration du corpus documentaire

7.1 Principes respectés pour l'élaboration des documents de la PGSSI-S

Lors de l'élaboration de chaque document de la PGSSI-S, les principes directeurs suivants sont pris en compte :

- le cadre juridique applicable au thème traité par le document en procédant si nécessaire au renvoi à des fiches juridiques spécifiques ;
    - à titre d'exemple, le référencement des données de santé à l'aide de l'identifiant national de santé est une obligation fixée par l'article L1111-8-1 du code de la santé publique, dont les modalités sont précisées par décret ;
- les règles et exigences de la PSSI-MCAS ;
- à aucun moment, un choix inadéquat de mesures de sécurité ne doit se faire au détriment de la qualité de la prise en charge des patients ;
- la mise en œuvre de SIS doit prendre en compte les droits fondamentaux de l'usager des systèmes de santé en garantissant notamment la confidentialité, la traçabilité et la pérennité et l'intégrité des données de santé à caractère personnel tout au long du cycle de vie des données (de leur création ou saisie à leur archivage et destruction) ;
- les principes de sécurité existants et éprouvés dans des secteurs d'activités, comme le secteur bancaire ou encore l'administration électronique, sont adoptés pour tirer parti des retours d'expérience de ces secteurs ; ces principes sont ensuite complétés pour répondre aux besoins spécifiques du secteur de la santé.

7.1.1 Prise en compte des principes de sécurité

L'élaboration des documents de la PGSSI-S se fonde sur les bonnes pratiques capitalisées dans des documents de référence (les normes ISO 2700x, la méthode EBIOS de l'ANSSI[1], le règlement général de sécurité, la PSSI-MCAS).

En rappel, les grands critères de sécurité utilisés sont les suivants :

- Disponibilité : un niveau contextualisé et encadré

Tout SIS doit garantir la disponibilité des données de santé en fonction des besoins.

Le besoin de disponibilité des données de santé et des fonctions d'un système d'information de santé dépend de la finalité de ce système. Selon la disponibilité requise, les réponses possibles sont variées et peuvent être plus ou moins lourdes à mettre en œuvre. Ainsi, un système destiné à assurer des fonctions liées à la production ou à la coordination des soins aura des exigences de disponibilité a priori très supérieures à un système destiné à la recherche médicale.

Le responsable de traitement est libre, sur la base d'une analyse de risques complète, d'adopter des niveaux spécifiques de disponibilité correspondant à ses contraintes métier.

- Intégrité : une fiabilité maximale des données de santé

Tout SIS doit garantir l'intégrité des données de santé, à tous les stades de leur cycle de vie.

Les données de santé ont un besoin d'exactitude, de pérennité et d'exhaustivité souvent très élevé. Ce besoin d'intégrité est par défaut à considérer au niveau maximum dans l'ensemble des systèmes.

Le responsable de traitement est libre, sur la base d'une analyse de risques complète, d'adopter des niveaux spécifiques d'intégrité correspondant à ses contraintes métier.

- Confidentialité : un accès maitrisé aux données de santé

Le besoin de confidentialité des données de santé doit être déterminé en cohérence avec leur nature et la nécessité pour un individu d'y accéder.

Les facteurs de la confiance pendant l'utilisation d'un SIS reposent sur le principe que les identités utilisées pour gérer les utilisateurs des services offerts par le SIS sont à jour, de bonne qualité, vérifiées par un mécanisme d'authentification et qu'elles constituent la base de la mise en œuvre des droits d'accès. Ces prérequis peuvent être remplis différemment selon que les utilisateurs concernés sont des acteurs de santé ou des patients.

- Auditabilité, traçabilité et imputabilité : des traces à valeur de preuve face au détournement de finalité

La traçabilité et l'imputabilité des actions concernent tous les acteurs du traitement, qui doivent être informés de la mise en place de telles mesures. Elles permettent à l'ensemble des acteurs de s'appuyer, en toute confiance, sur les données fournies par les SIS. En particulier elles permettent au responsable de traitement de disposer d'éléments exploitables pour les étudier ou pour les fournir en tant qu'élément de preuves dans le cadre d'enquêtes ainsi que de détecter de façon précoce, via l'analyse des informations journalisées, les incidents concernant des données de santé.

En cohérence avec la protection juridique des données de santé, les traces des actions sur le SIS doivent être recueillies dans les systèmes, être imputables à leur auteur et avoir valeur de preuve en cas de mésusage ou de détournement de finalité. A cet effet, les traces

[1] EBIOS 2010 - Expression des Besoins et Identification des Objectifs de Sécurité publiée par l'Agence Nationale de la Sécurité des Systèmes d'Information.

des actions doivent être considérées comme ayant un besoin en intégrité maximal identique au besoin d'intégrité des données de santé sur lesquelles portent les actions tracées.

7.2 Comitologie

Le corpus documentaire est conçu dans un cadre collaboratif regroupant les représentants des institutions publiques, des acteurs de santé, des usagers et des industriels.

La liste exhaustive des institutions participant aux différentes instances décrites ci-dessous est publiée sur le site internet de l'ASIP Santé et régulièrement mise à jour.

7.2.1 Maîtrises d'ouvrage

L'ASIP Santé a été missionnée par la secrétaire générale des ministères chargés des affaires sociales le 22 septembre 2011 pour apporter son concours à la Délégation à la stratégie des systèmes d'information de santé (DSSIS), MOA stratégique de la PGSSI-S, et assurer les fonctions de MOA opérationnelle.

L'ASIP Santé a un rôle initial de production et de mise à jour des documents de la PGSSI-S.

Elle organise et gère le secrétariat des différents groupes de travail (GT).

Sur son site internet, l'ASIP Santé publie les documents validés et gère l'espace de concertation publique, la FAQ et le portail bibliographique.

Elle est en charge de la promotion des documents publiés et de l'accompagnement des acteurs de santé dans la compréhension de la PGSSI-S.

L'ASIP Santé réalise un état des lieux annuel des versions des guides et le transmet aux groupes de travail, comité de concertation et au comité de pilotage.

7.2.2 Comité de pilotage

7.2.2.1 Rôle et organisation

Ce comité a pour rôle principal le pilotage du projet PGSSI-S.

Il est décidé lors des comités de pilotage de la mise en concertation publique des documents, de la validation de la prise en compte des commentaires issus de la concertation, du choix de montée de version majeure ou mineure, de la publication et du retrait d'un document. C'est le comité de pilotage qui décide du statut, opposable ou non, des documents élaborés.

7.2.2.2 Composition

Le comité de pilotage, présidé par la DSSIS, comprend les représentants dûment mandatés :

- des directions d'administration centrale du ministère et des services du Haut fonctionnaire de défense et de sécurité,
- de l'ANSSI,
- de la CNAMTS,
- de la CNIL,
- de la CNSA.

L'ASIP Santé peut être consultée lors du comité de pilotage pour apporter les précisions nécessaires sur les documents en discussion et les travaux en cours.

7.2.3 Groupes de travail PGSSI-S

7.2.3.1 Rôle et organisation

Les groupes de travail (GT) contribuent à l'élaboration des documents et alimentent la réflexion sur les documents initiés par la MOA opérationnelle, l'ASIP Santé.

Les groupes de travail peuvent être réunis sur différentes thématiques, juridiques ou liées à la sécurité du système d'information par exemple.

La fréquence des réunions de travail est fonction de l'actualité PGSSI-S et du besoin de production de nouveaux livrables. Un rythme bimestriel est constaté depuis 2015.

L'ASIP Santé assure l'organisation des réunions des différents groupes de travail en gérant les convocations, l'animation des réunions et les compte-rendu.

7.2.3.2 Composition

La composition des groupes de travail évolue selon la thématique abordée.

Les groupes de travail sont par nature ouverts et tout représentant d'acteur de santé peut se porter volontaire auprès de l'ASIP Santé pour y participer.

Sont notamment invités à participer aux groupes de travail les représentants :

- des institutions publiques liées au secteur de la santé ;
- des directions d'administration centrale concernées du ministère de la santé;
- des services du HFDS et de la DSSIS ;
- des ARS ;
- des 7 ordres professionnels ;
- des usagers du système de santé ;
- des fédérations hospitalières ;
- des industriels du secteur ;
- de sociétés savantes du secteur des soins ou de l'informatique.

La liste des représentants est tenue à jour par l'ASIP Santé.

7.2.4 Comité de concertation

7.2.4.1 Rôle et organisation

Le comité de concertation valide le travail des différents groupes de travail et décide de la mise en concertation privée puis publique, ainsi que des durées de concertation ;

La fréquence des comités de concertation est fonction de l'actualité PGSSI-S et du besoin de production de nouveaux livrables. Un rythme biannuel est constaté depuis 2015.

La DSSIS assure l'organisation des comités de concertation en gérant les convocations, l'animation des réunions et les comptes rendus.

7.2.4.2 Composition

Le comité de concertation, présidé par la DSSIS, comprend des représentants dûment mandatés :

- des professionnels et établissements ;
- des usagers du système de santé ;
- des industriels du secteur ;
- de sociétés savantes du secteur des soins ou de l'informatique.

La liste des représentants est maintenue par la DSSIS.

7.3 Cycle de vie du document

Le cycle de vie des référentiels et des guides sont dissociés.

7.3.1 Les référentiels

Les référentiels se voient imposer une mise à jour majeure au minimum tous les 3 ans.

Toutefois, une version majeure peut être proposée dans cet intervalle, pour un changement de contexte juridique par exemple.

- Cycle de version majeure obligatoire pour les référentiels : 36 mois.
  - 1ère année : diffusion, communication, implémentation de la nouvelle version
  - 2ème année : premiers retours d'expérience
  - 3ème année : initiation de la nouvelle version, lancement GT puis concertation

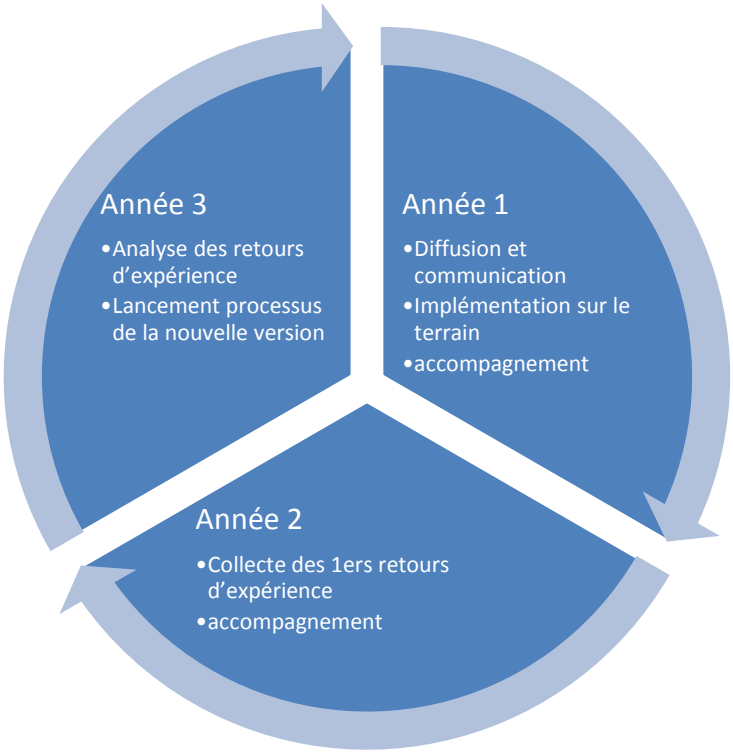

Figure 2: cycle de version majeure sur 3 ans

Des mises à jour mineures peuvent être proposées également.

A la différence des versions majeures, ce type de mises à jour doit être sans impact sur les usages terrain, métiers et sur les offres industrielles (pas d'impact sur les cahiers des charges, pas de changement de dispositifs en établissement de santé..).

Il n'y a pas de notion de cycle obligatoire pour les versions mineures.

Le comité de pilotage décide si le changement voulu est porté dans une version majeure ou mineure.

7.3.2 Les guides

Pour les guides, il n'existe pas de cycle obligatoire de mises à jour.

Ces dernières sont proposées selon l'évolution et le besoin technique, métier ou juridique.

Le comité de pilotage décide si le changement voulu est porté dans une version majeure ou mineure.

Un état des lieux annuel des versions des guides sera réalisé par l'ASIP Santé et transmis aux groupes de travail, comité de concertation et au comité de pilotage.

7.3.3 Les procédures de mises à jour

Une version majeure nécessite obligatoirement une procédure de validation complète.

La procédure de validation complète est présentée ci-dessous.

La phase de conception est constituée des étapes suivantes:

- toute instance peut être à l'origine d'une proposition de document ou d'évolution de document ;
- le comité de pilotage valide ou non la proposition ;
- l'ASIP Santé rédige la version initiale ;
- cette version initiale est relue et amendée en GT ; les mises à jour sont assurées par l'ASIP Santé ; plusieurs réunions de GT peuvent être nécessaires à l'élaboration du document ;
- une fois le document validé en GT, le comité de pilotage donne son aval pour l'envoi en comité de concertation ou décide d'abandonner l'élaboration du document ;
- en cas d'absence de consensus sur un sujet en GT, le comité de pilotage prend position et décide de la suite des travaux.

La phase de concertation est constituée des étapes suivantes:

- le comité de concertation, réuni par la DSSIS, décide de la mise en concertation privée puis publique et de la durée de ces concertations ; ou il peut décider également de renvoyer le document en GT avec un ensemble de remarques précises ;
- le suivi des retours de concertation privée est assuré par la DSSIS, le suivi des retours de concertation publique par l'ASIP Santé.

La phase de validation est constituée des étapes suivantes:

- suite aux différentes concertations, le comité de pilotage décide de publier le document dans sa nouvelle version, de l'abandonner ou de le renvoyer en GT ;
- la publication du nouveau document se fait sur le site internet de l'ASIP Santé ;
- l'ASIP Santé assure la promotion et la diffusion du document.
    - Le contenu des documents de la PGSSI-S est porté à la connaissance des acteurs concernés par différents canaux de communication (site internet, liste de diffusion ….) fournis par l'ASIP Santé.
    - L'accompagnement à la compréhension et la diffusion des documents de la PGSSI-S est réalisé par tous les moyens jugés nécessaires par l'ASIP Santé.

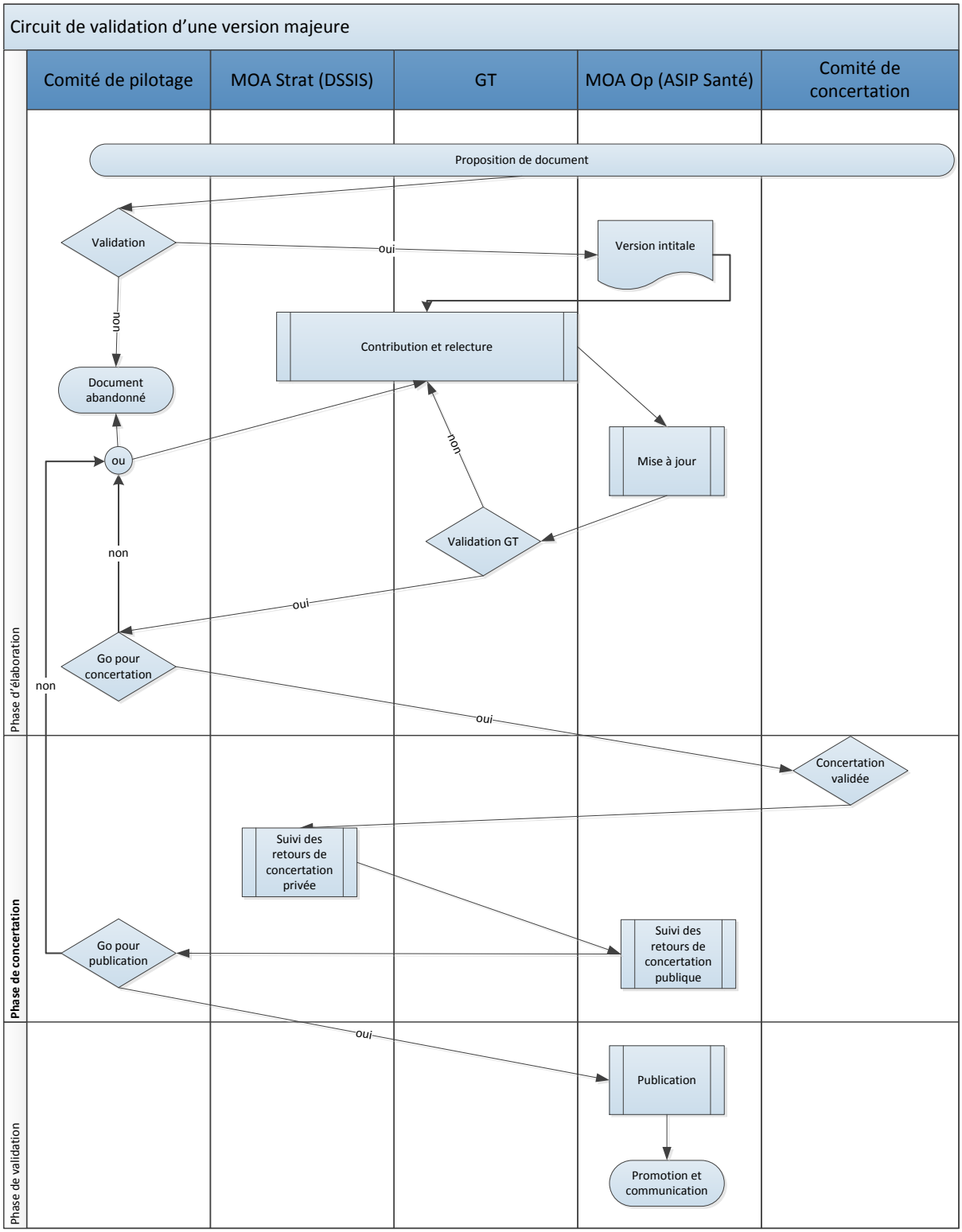

Figure 3: procédure version majeure

Une version mineure nécessite un circuit de validation raccourci.

La procédure de validation raccourcie est la suivante :

- toute instance peut proposer une version mineure de document ;

- le comité de pilotage valide la proposition, l'abandonne ou décide que la proposition mérite une nouvelle version majeure du document ;
- l'ASIP Santé est en charge de la rédaction ;
- le comité de pilotage valide le document, l'abandonne ou décide que la proposition mérite une nouvelle version majeure du document ;
- si le document est validé, l'ASIP Santé informe les GT, la DSSIS informe le comité de concertation ;
- la publication du nouveau document se fait sur le site internet de l'ASIP Santé ;
- l'ASIP Santé assure la promotion et la diffusion du document.

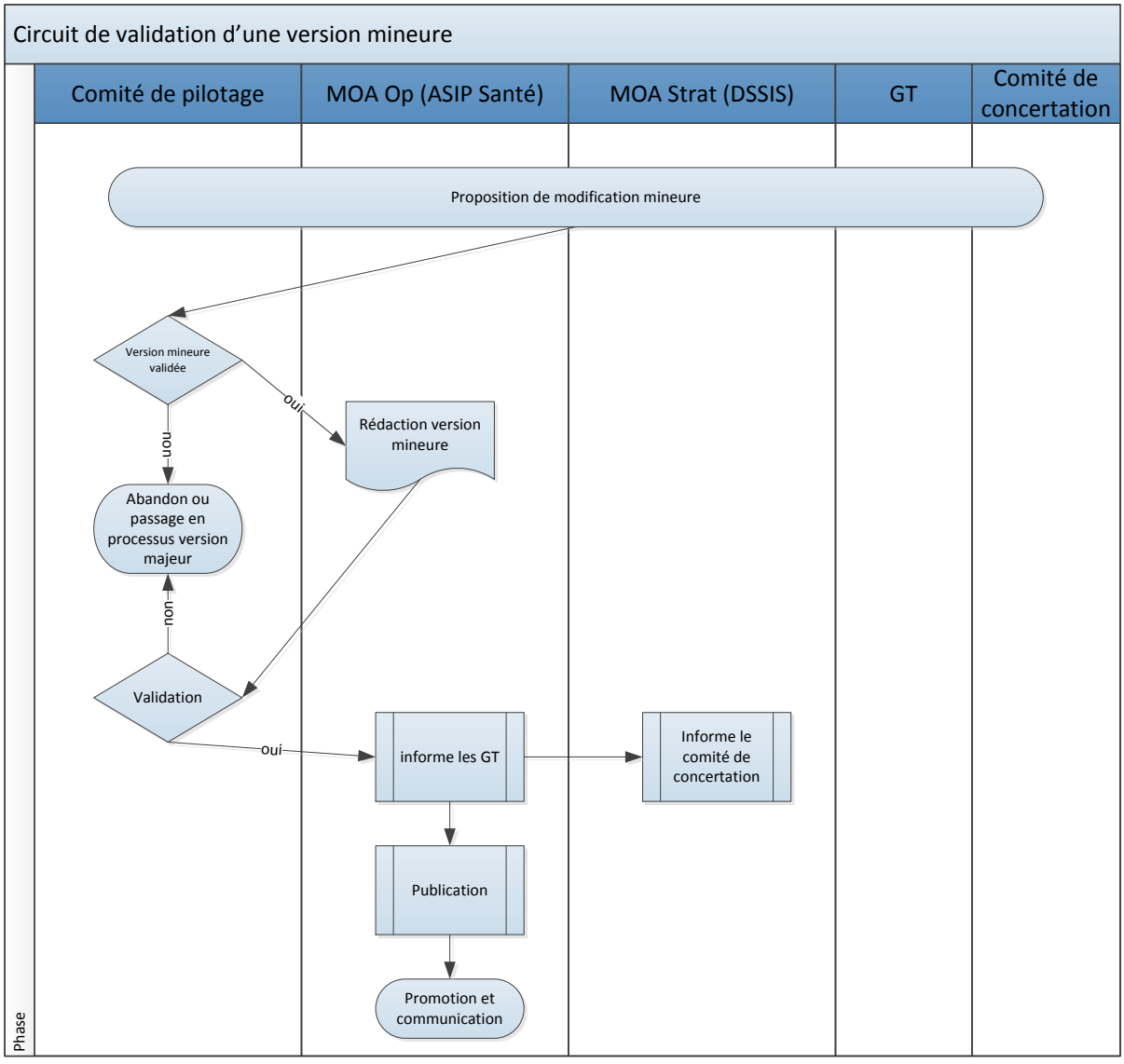

Figure 4: procédure version mineure

7.3.4 La procédure de retrait d'un document du corpus

Le retrait d'un document PGSSI-S est décidé et validé par le comité de pilotage. La communication de cette action est faite vers les autres instances.

8 Annexes

8.1 Glossaire

ANSSI	agence nationale de la sécurité des systèmes d'information
ARS	agence régionale de santé
ASIP Santé	agence des systèmes d'information partagés de santé
CNAMTS	caisse nationale de l'assurance maladie des travailleurs salariés
CNIL	commission nationale de l'informatique et des libertés
CNSA	caisse nationale de solidarité pour l'autonomie
DMP	dossier médical partagé
DSSIS	délégation à la stratégie des systèmes d'information de santé
EBIOS	expression des besoins et identification des objectifs de sécurité
EHPAD	établissement d'hébergement pour personnes âgées dépendantes
FAQ	foire aux questions
GRADES	groupement régionaux d'appui pour le développement de l'e-santé
GT	groupe de travail
HFDS	haut fonctionnaire de défense et de sécurité
MCAS	ministères chargés des affaires sociales
MOA	maîtrise d'ouvrage
PGSSI-S	politique générale de sécurité des systèmes d'Information de santé
PSSI	politique de sécurité du système d'information
PSSIE	politique de sécurité des systèmes d'information de l'Etat
PSSI-MCAS	politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales
RGS	règlement général de sécurité
SAAS	software as a service
SIS	systèmes d'information de santé
SSI	sécurité du système d'information

8.2 Table des illustrations