

GOUVERNANCE DE LA PGSSI-S

Version 1.0



SOMMAIRE

AVANT-PROPOS	2
1. COMITOLOGIE DE LA PGSSI-S.....	3
1.1. Comité de pilotage.....	3
1.1.1. <i>Rôle.....</i>	3
1.1.2. <i>Composition</i>	3
1.1.3. <i>Fonctions</i>	3
1.1.4. <i>Fréquence.....</i>	3
1.2. Comités de concertation.....	3
1.2.1. <i>Rôle.....</i>	3
1.2.2. <i>Composition</i>	4
1.2.3. <i>Fonctions</i>	4
1.2.4. <i>Fréquence.....</i>	4
1.3. Comité d'instruction	4
1.3.1. <i>Rôle.....</i>	4
1.3.2. <i>Composition</i>	4
1.3.3. <i>Fonctions</i>	4
1.3.4. <i>Fréquence.....</i>	5
2. ELABORATION DE LA STRATEGIE CYBERSECURITE ET DE LA FEUILLE DE ROUTE DE LA PGSSI-S	6
3. ELABORATION ET EVOLUTION DES DOCUMENTS DE LA PGSSI-S	7
3.1. Phase amont : collecte de la demande, instruction et planification	7
3.1.1. <i>Collecte de la demande.....</i>	7
3.1.2. <i>Contenu d'une expression de besoin</i>	7
3.1.3. <i>Instruction de la demande</i>	8
3.1.4. <i>Décision, priorisation et planification</i>	8
3.2. Phase de réalisation – Cas des référentiels.....	8
3.3. Phase de réalisation – Cas des documents autres que les référentiels	10

AVANT-PROPOS

Le numérique améliore la prise en charge du patient en santé, mais les menaces associées ont conduit à une politique de gestion des risques par l'État. Avec la PGSSI-S, l'Agence du Numérique en Santé fixe le cadre de référence pour la cybersécurité de la e-santé. Ce cadre s'applique au service public et au privé, pour les usagers, les professionnels de santé, les secteurs médico-social et social, les établissements de soins et les fournisseurs de services en santé. A cette fin, la PGSSI-S est constituée de référentiels, opposables une fois approuvés par arrêté du ministre chargé de la santé, et d'autres documents non opposables destinés à informer, sensibiliser ou guider les différents publics concernés.

Afin que la PGSSIS puisse répondre de manière continue aux évolutions des enjeux, de la législation et des besoins des différents acteurs, une gouvernance est mise en place en s'appuyant sur une comitologie qui associe les parties concernées aux décisions d'évolution de la stratégie de cybersécurité pour la e-santé et d'adaptation de la PGSSI-S qui en découlent.

1. COMITOLOGIE DE LA PGSSI-S

La comitologie de gouvernance de la PGSSI-S est constituée de trois organes :

- un comité de pilotage, organe décisionnel regroupant les institutions publiques impliquées dans la sécurité des systèmes d'information de santé (SSIS) ;
- des comités de concertation, organes consultatifs ad hoc regroupant chacun les parties prenantes à un document ou un sujet de la PGSSI-S en particulier, et chacun constitué d'une partie de l'ensemble des parties-prenantes à la PGSSI-S ;
- un comité d'instruction, organe opérationnel regroupant des experts en sécurité des systèmes d'information de santé.

1.1. Comité de pilotage

1.1.1. Rôle

Le comité de pilotage (COFIL) a un rôle décisionnel, sur la stratégie de cybersécurité comme sur le contenu documentaire de la PGSSI-S.

1.1.2. Composition

Il est composé des institutions publiques impliquées dans la SSIS : DNS, SHFDS, CNAM, ANSSI, ANS.

1.1.3. Fonctions

- Définir, mettre à jour régulièrement et partager à l'écosystème les orientations de la stratégie SSIS traduites dans la PGSSI-S, décidées en commun par les membres du COFIL ;
- Prendre les décisions relatives à la validation et à la priorisation des besoins relatifs à PGSSI-S et au lancement des projets d'évolution de la PGSSI-S permettant de répondre à ces besoins, en tenant compte des recommandations des comités de concertation et en s'appuyant sur le comité d'instruction ;
- Valider la composition des comités de concertation en fonction des sujets ;
- Valider les référentiels de la PGSSI-S avant publication ;
- Valider, faire vivre et partager à l'écosystème la feuille de route de la PGSSI-S ;
- Suivre l'avancement des travaux en cours relatifs à la PGSSI-S.

1.1.4. Fréquence

Le comité de pilotage se réunit trois fois par an : en janvier / février (COFIL 1), mai / juin (COFIL 2) et en septembre / octobre (COFIL 3).

Le COFIL est également sollicité par messagerie sur certains sujets pour vérifier s'il a des amendements à apporter aux propositions du comité d'instruction.

1.2. Comités de concertation

1.2.1. Rôle

Les comités de concertation ont un rôle consultatif, notamment au cours de l'élaboration ou de l'évolution des documents de la PGSSI-S.

1.2.2. Composition

Ils sont composés :

- de représentants des fédérations d'industriels de la santé, du social et du médico-social ;
- de représentants des utilisateurs de la PGSSIS : ARS, GRADeS, fédérations hospitalières, ordres professionnels, unions professionnelles et syndicats de du secteur de la santé, du social et du médico-social, Club RSSI... ;
- d'experts des institutions publiques membres du comité de pilotage.

Pour chaque document ou thématique de la PGSSI-S à traiter, une partie des représentants et experts désignés ci-dessus sont invités à participer à un comité de concertation ad hoc, en fonction de leurs liens avec le sujet concerné. Le nombre de participants doit être restreint afin de préserver l'efficacité des échanges.

La liste des participants à un comité de concertation est proposée au COPIL par le comité d'instruction. Elle peut être amendée à cette occasion par le COPIL.

Cette composition peut également être revue sur demande d'ajout d'une partie prenante après validation par le COPIL.

1.2.3. Fonctions

- Participer aux concertations internes sur les documents de la PGSSI-S ;
- Participer aux arbitrages lors de la consolidation des contributions suite aux concertations internes ou publiques ;
- Prendre position si des points d'arbitrage lui sont soumis sur des points autres que les documents de la PGSSI-S, afin d'éclairer les décisions à prendre par le COPIL ;
- Identifier les besoins documentaires relevant de la PGSSI-S et non couverts à date, ou les évolutions à apporter aux documents existants.

1.2.4. Fréquence

Les comités de concertation se réunissent autant que de besoin, avec un délai minimal de deux mois entre deux réunions consécutives.

Ils échangent autant que de besoin en interne entre les réunions.

1.3. Comité d'instruction

1.3.1. Rôle

Le comité d'instruction a un rôle opérationnel dans la stratégie SSIS, la gestion de la feuille de route et les travaux sur les documents de la PGSSI-S.

1.3.2. Composition

Il est organisé et animé par l'ANS qui réunit au besoin des petits groupes d'experts de l'écosystème.

Il rapporte au COPIL et informe régulièrement la DNS de l'avancement de ses travaux.

1.3.3. Fonctions

- Collecter les besoins documentaires relevant de la PGSSI-S communiqués par les organismes susceptibles de participer aux comités de concertation, par le COPIL ou par d'autres acteurs concernés ;
- Instruire les besoins documentaires collectés et non couverts à date, et proposer les projets de travaux correspondants au COPIL ;
- Proposer au COPIL la liste des participants à chaque comité de concertation ;
- Préparer les évolutions de la stratégie SSIS selon les orientations fixées par le COPIL et les soumettre à la validation du COPIL ;
- Préparer et gérer la feuille de route de la PGSSI-S soumise au COPIL ;
- Rédiger ou faire évoluer les documents constituant le corpus documentaire de la PGSSI-S ;
- Préparer et animer les réunions du comité de pilotage ;
- Préparer et animer les réunions des comités de concertation.

1.3.4. Fréquence

Le comité d'instruction se réunit autant que de besoin.

2. ELABORATION DE LA STRATEGIE CYBERSECURITE ET DE LA FEUILLE DE ROUTE DE LA PGSSI-S

La stratégie relative à la SSIS (ou stratégie cybersécurité de la e-santé) et sa traduction dans la PGSSI-S sont élaborées par le comité d'instruction selon les orientations fixées par le COPIL. Elles sont approuvées par le COPIL en tenant compte des documents fondateurs publiés par les institutions publiques nationales et européennes, comme par exemple :

- la feuille de route du numérique en santé portée par la DNS ;
- la doctrine du numérique en santé portée par l'ANS et la DNS en lien avec d'autres partenaires, publiée tous les ans depuis 2020 et mise en concertation à chaque nouvelle version ;
- l'Observatoire des signalements d'incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social publié annuellement par le CERT Santé ;
- le panorama de la menace annuel de l'ANSSI et sa déclinaison sectorielle le cas échéant ;
- la réglementation française et européenne en matière de sécurité des systèmes d'information des données de santé.

L'analyse de ces documents ainsi que la connaissance terrain et contextuelle des membres du COPIL doivent permettre à ce dernier de dégager les éléments clés de sécurité des systèmes d'information de santé sur la base desquels il fixe les orientations en matière de SSIS et la stratégie d'évolution de la PGSSI-S.

La feuille de route de la PGSSI-S est consolidée par le comité d'instruction, sous l'égide du COPIL, en fonction des priorités fixées par le COPIL en matière de travaux sur les documents de la PGSSI-S et des ressources affectées à ces travaux.

La feuille de route pour l'année suivante est proposée à la validation du COPIL lors de sa réunion « COPIL 3 ». Le COPIL conserve cependant la possibilité de l'amender à tout moment en cours d'année sous réserve des moyens affectés au comité d'instruction.

3. ELABORATION ET EVOLUTION DES DOCUMENTS DE LA PGSSI-S

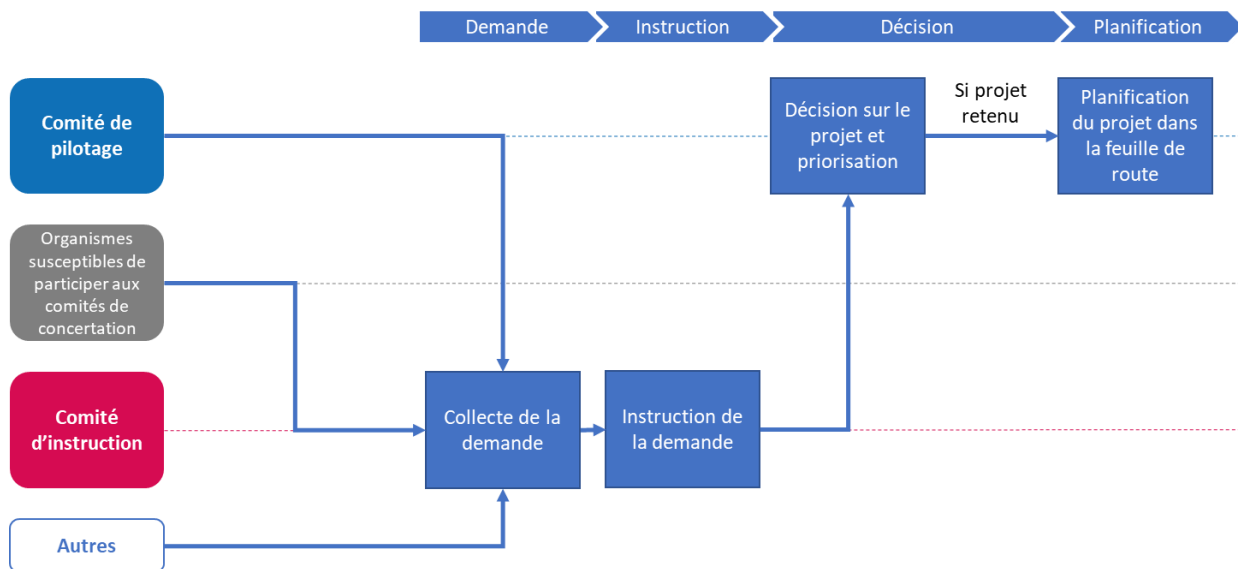
L'élaboration ou l'évolution d'un document de la PGSSI-S se déroule en deux grandes phases :

1. la phase amont : collecte de la demande, instruction et planification ;
2. la phase de réalisation : réalisation des travaux d'élaboration ou d'évolution du document.

Le déroulement de la phase de réalisation diffère selon que le document est un référentiel, dont la vocation est d'être opposable, ou un document d'une autre nature, non opposable (guide, support d'information, support de sensibilisation...).

3.1. Phase amont : collecte de la demande, instruction et planification

Cette phase est présentée dans le schéma ci-dessous, et détaillée ensuite.



3.1.1. Collecte de la demande

La formulation des besoins documentaires ou, plus explicitement, la demande de production ou d'évolution de document de la PGSSI-S peut être effectuée par :

- les organismes susceptibles de participer aux comités de concertation, qui constituent la source naturelle de telles demandes du fait de la variété d'acteurs qu'ils représentent ;
- les membres du COPIL ;
- tout autre acteur concerné par des sujets de SSIS.

Ces expressions de besoins sont collectées par le comité d'instruction.

3.1.2. Contenu d'une expression de besoin

Une expression de besoin de document doit notamment expliciter :

- le sujet à traiter ;
- la nature du document attendu : information, sensibilisation, guide (organisationnel ou technique, général ou détaillé), référentiel (opposable) organisationnel ou technique... ;

- la ou les populations destinataires du document, en précisant le niveau de maîtrise de la sécurité considéré pour ces destinataires, afin que le langage, le niveau de détail et la technicité du document soient pertinents pour le lectorat ciblé ;
- la finalité du document, c'est-à-dire l'objectif que l'on cherche à atteindre à l'aide de ce document. Il faut veiller à ce que la finalité du document soit concise et clairement décrite. Elle peut éventuellement être complétée par des objectifs secondaires si l'on juge que cela est nécessaire.

3.1.3. Instruction de la demande

Chaque expression de besoin est instruite par le comité d'instruction pour déterminer :

- si le besoin n'est pas déjà couvert, en partie ou en totalité, par d'autres documents existants de la PGSSI-S, ou s'il pourrait être intégré à un document existant de la PGSSI-S ;
- si le besoin pourrait être couvert par des documents d'origine externe pérenne (ANSSI, CNIL...) ;
- les éventuelles sources documentaires externes pouvant être utilisées pour l'élaboration du document, ainsi que les textes légaux et réglementaires existants ou attendus devant être pris en compte ;
- si et comment la demande initiale pourrait être amendée afin de s'inscrire au mieux dans la stratégie SSIS ;
- les représentants d'organismes susceptibles de participer aux comités de concertation qu'il semble pertinent d'intégrer au comité de concertation pour ce document ;
- les acteurs qu'il semble pertinent d'associer aux travaux du comité d'instruction pour la réalisation du document ;
- les moyens nécessaires à l'élaboration du document.

Le comité d'instruction formule un avis global à l'attention du COPIL sur l'opportunité de réalisation de ce document et sur sa priorisation.

3.1.4. Décision, priorisation et planification

Les demandes instruites par le comité d'instruction sont présentées au COPIL et proposées pour validation et priorisation.

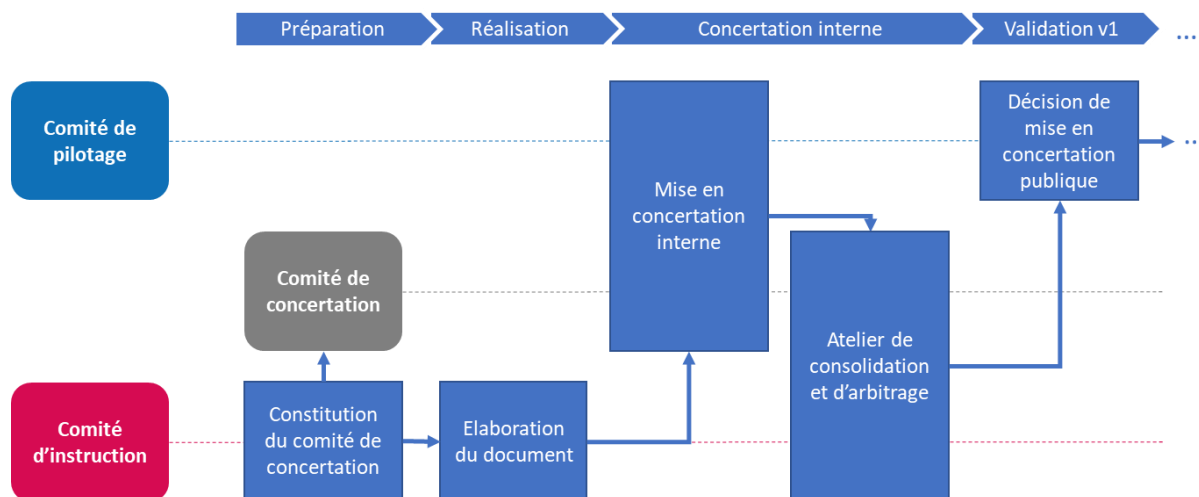
Le comité d'instruction intègre à la feuille de route les nouvelles demandes acceptées par le COPIL en fonction de leur priorité retenue par le COPIL et de la disponibilité des moyens requis pour les travaux. Les travaux correspondant aux différents documents sont déclenchés et menés dans l'ordre prévu par la feuille de route.

En cas de rejet de la demande, son émetteur en est informé ainsi que de la raison de la décision.

En cas d'acceptation de la demande, son émetteur en est informé à la communication suivante de la feuille de route, dans laquelle le document correspondant est positionné.

3.2. Phase de réalisation – Cas des référentiels

La phase de réalisation d'un référentiel est présentée dans les deux schémas ci-dessous, chacun étant suivi du détail des étapes correspondantes.



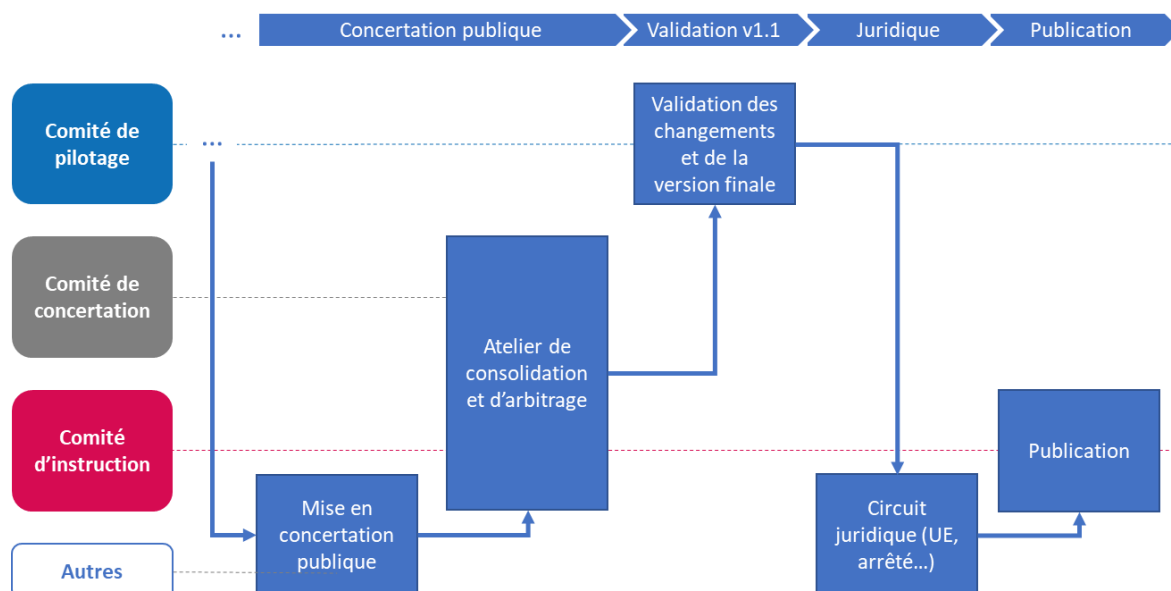
Le comité de concertation pour le document considéré est constitué selon les principes exposés au chapitre consacré au comité de concertation, au démarrage des travaux.

Débute alors l'élaboration du document par le comité d'instruction, après si besoin adjonction temporaire d'expertises complémentaires au comité.

Une fois produite, la version préliminaire du document est mise en concertation interne par partage avec le comité de concertation et avec le COPI. Les propositions de modifications sont formulées par chaque participant à la concertation qui le souhaite et transmises au comité d'instruction.

Le comité d'instruction intègre directement au document les modifications mineures et consolide les autres propositions de modification pour les soumettre à arbitrage dans un atelier qui rassemble le comité de concertation et le comité d'instruction.

La version « v1 » du document résultant de ces travaux est transmise au COPI pour validation et décision de mise en concertation publique.



Au cours de la concertation publique, les propositions de modifications sont formulées par les contributeurs et collectées par le comité d'instruction.

Le comité d'instruction intègre directement au document les modifications mineures et consolide les autres propositions de modification pour les soumettre à arbitrage dans un atelier qui rassemble le comité de concertation et le comité d'instruction.

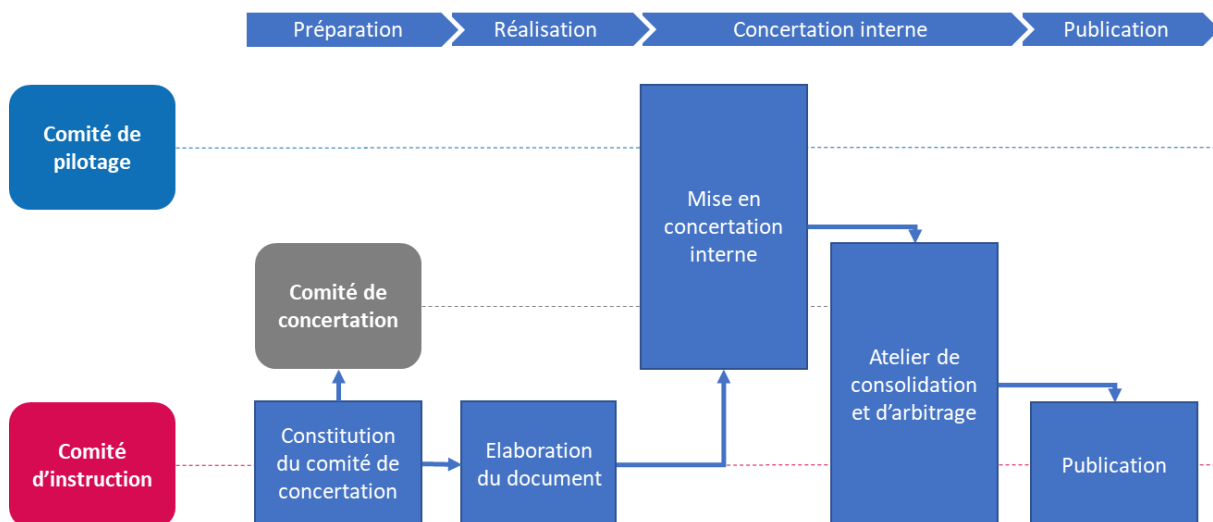
La version « v1.1 » du document résultant de ces travaux est transmise au COPIL, accompagnée de la liste des changements apportés depuis la v1, pour validation de cette version v1.1 finale et décision d'engager le processus nécessaire à sa publication.

Il est publié une synthèse des principales contributions à la concertation publique indiquant leur prise en compte sur la plateforme de concertation.

Le document est transmis au service en charge du circuit juridique du document (préparation de l'arrêté ministériel d'approbation du référentiel, transmission à la Commission Européenne...) qui se conclut normalement par la publication de l'arrêté et du référentiel, et l'intégration du référentiel au corpus documentaire de la PGSSI-S.

3.3. Phase de réalisation – Cas des documents autres que les référentiels

La phase de réalisation d'un document autre qu'un référentiel est présentée dans le schéma ci-dessous, suivi du détail des étapes correspondantes.



Le comité de concertation pour le document considéré est constitué selon les principes exposés au chapitre consacré au comité de concertation, au démarrage des travaux.

Début alors l'élaboration du document par le comité d'instruction, après si besoin adjonction temporaire d'expertises complémentaires au comité.

Une fois produite, la version préliminaire du document est mise en concertation interne par partage avec le comité de concertation et avec le COPIL. Les propositions de modifications sont formulées par chaque participant à la concertation qui le souhaite et transmises au comité d'instruction.

Le comité d'instruction intègre directement au document les modifications mineures et consolide les autres propositions de modification pour les soumettre à arbitrage dans un atelier qui rassemble le comité de concertation et le comité d'instruction.

La version « v1 » du document résultant de ces travaux est intégrée au corpus documentaire de la PGSSI-S et publiée.