PRÉREQUIS HOP'EN

BOITE A OUTILS
POUR L'ATTEINTE DES PRÉREQUIS HOP'EN

Contact : numerique@anap.fr – http://numerique.anap.fr

JUIN 2019

OBJET

Cette boîte à outils rassemble les éléments de méthodes utiles aux établissements de santé pour l'atteinte des prérequis définis dans le cadre du programme HOP'EN. Elle rassemble également des documents types associés, proposés pour faciliter la mise en œuvre des méthodes proposées.

Ces productions s'adressent aux DSI-RSI des établissements de santé.

Cette boîte à outils a été élaborée initialement dans le cadre du programme Hôpital Numérique et a été mise à jour pour répondre aux nouvelles exigences du programme HOP'EN.

Sa mise à jour a été réalisée par :

- Dominique LORIOUX, Directeur de la clinique La Parisière
- Nicolas DELAPORTE, DSI du GHT de l'Artois
- Dr Pierre CHAMPSAUR, chef du service radiologie - Hôpital Sainte-Marguerite (AP-HM)
- Mickaël TAINE, DSI du CHU de Reims

Avec l'appui des cabinets Ersnt & Young et OpusLine.

SOMMAIRE

1. FICHE 1 — MISE EN ŒUVRE DE L'IDENTITO-VIGILANCE

1.1. Contexte et périmètre

Contexte et objectifs

Le socle commun du programme HOP'EN est constitué de 4 prérequis indispensables à une gestion sécurisée des soins dans un contexte de décloisonnement des prises en charge, dont la mise en place, par l'ensemble des établissements de santé est attendue d'ici la fin du programme :

- Identités, mouvements (P1) ;
- Sécurité (P2) ;
- Confidentialité (P3) ;
- Échanges et partages (P4).

Il comprend également 7 domaines fonctionnels pour lesquels le programme définit des exigences en matière d'usage du système d'information.

- Les résultats d'imagerie, de biologie et d'anapath (D1) ;
- Le dossier patient informatisé et interopérable et le DMP (D2) ;
- La prescription électronique alimentant le plan de soins (D3) ;
- La programmation des ressources et l'agenda du patient (D4) ;
- Le pilotage médico-économique (D5) ;
- La communication et les échanges avec les partenaires (D6) ;
- La mise à disposition de services en ligne aux usagers et aux patients (D7).

Le présent document propose une méthode pour la mise en œuvre d'une démarche d'identito-vigilance ; méthode correspondant à celle du plan d'action proposé aux établissements de santé pour atteindre les prérequis du programme HOP'EN.

Cette fiche ne constitue pas une recommandation, mais vise à présenter aux établissements un cadre méthodologique pour mettre en œuvre une démarche d'identito-vigilance. Elle concerne les aspects techniques de l'identitovigilance et non organisationnels.

La méthode qui est proposée dans cette fiche pratique correspond à une démarche globale de mise en œuvre de l'identito-vigilance qui va ainsi au-delà de l'exigence fixée par le programme, laquelle porte sur l'existence d'une cellule d'identito-vigilance opérationnelle.

Indicateur concerné

La fiche concourt principalement à l'obtention de :

– **L'indicateur P1.2 du prérequis « identité-mouvement » : existence d'une cellule d'identito-vigilance opérationnelle.**

1.2. L'INS en pratique

Enjeux

L'identifiant national de santé (INS) est utilisé pour référencer les données de santé et les données administratives de toute personne bénéficiant ou appelée à bénéficier d'un acte diagnostique, thérapeutique, de prévention, de soulagement de la douleur, de compensation du handicap ou de prévention de la perte d'autonomie, ou d'interventions nécessaires à la coordination de plusieurs de ces actes.

Ce référencement est indispensable afin d'éviter des erreurs d'identification des personnes prises en charge (doublons, collisions, documents mal attribués). En outre, l'identification fiable des personnes permet de faciliter l'échange et le partage des données de santé.

Cela contribue à la qualité de la prise en charge et à la sécurité des soins.

L'identifiant utilisé pour les patients en tant que porteurs de données de santé à caractère personnel doit être unique, univoque, pérenne et reconnu par tous les acteurs de santé. Il s'agit du Numéro d'Inscription au Répertoire National d'identification des personnes physiques (NIR).

Attribution du NIR

Le NIR est attribué dès les premiers jours pour les naissances en France et sur demande, dans les conditions prévues par la loi, pour les personnes nées à l'étranger. Tous les bénéficiaires de l'Assurance Maladie disposent d'un NIR, utilisé notamment pour gérer les droits aux prestations.

Le NIR est formé de 13 caractères : le sexe (1 chiffre), l'année de naissance (2 chiffres), le mois de naissance (2 chiffres) et le lieu de naissance (5 caractères). Les 3 chiffres suivants correspondent à un numéro d'ordre qui permet de distinguer les personnes nées au même lieu à la même période ; une clé de contrôle à 2 chiffres complète le NIR.

Le NIR est communément appelé « numéro de sécurité sociale ».

Cadre légal

La loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé consacre le NIR — à défaut le NIA pour les personnes en cours d'immatriculation — comme identifiant national de santé (INS). « Le numéro d'inscription au répertoire national d'identification des personnes physiques est utilisé comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales, dans les conditions prévues à l'article L. 1110-4.Pour les personnes en instance d'attribution d'un numéro d'inscription au répertoire national d'identification des personnes physiques et jusqu'à l'attribution de ce numéro, l'identifiant national de santé est le numéro identifiant d'attente (NIA) […] mentionné au 1 ° de l'article R. 114-26 du code de la sécurité sociale ».

Les modalités d'utilisation de l'INS sont précisées par le décret n° 2017-412 du 27 mars 2017.

À compter du 1er janvier 2020, toute donnée de santé devra être référencée avec l'identifiant national de santé — le NIR ou le NIA — et les traits d'identité de l'usager, tels que connus dans l'état civil.

Lorsque l'identification d'une personne par un professionnel, quel que soit son mode d'exercice, est nécessaire pour sa prise en charge à des fins sanitaires ou médico — sociales, cette identification ne peut être faite que par l'INS.

Tout autre identifiant ne peut être utilisé qu'en cas d'impossibilité de pouvoir accéder à l'INS, afin de ne pas empêcher la prise en charge sanitaire et médico-sociale des personnes. Il est procédé au référencement des données de santé avec l'INS dès qu'il est possible d'y accéder.

Identité patient au sein du GHT

L'article 107 de la loi du 26 janvier 2016 de modernisation de notre système de santé prévoit l'optimisation et la gestion commune d'un système d'information hospitalier convergent, avec en particulier la mise en place d'un dossier patient permettant une prise en charge coordonnée des patients au sein des établissements du groupement. **L'identifiant unique pour les patients est l'une des priorités de convergence identifiée dans le décret 2016-524 du 27 avril 2016 relatif aux GHT** (articles 1 et 5 du décret, article R.6132-15 du code de la santé publique).

L'identifiant patient unique est en effet fondamental pour éviter les doublons et permettre la prise en charge coordonnée des patients. Le patient sera suivi avec un identifiant unique au niveau du GHT afin de permettre aux professionnels, participant à la prise en charge du patient, d'accéder à l'ensemble des données de santé disponibles au sein du GHT. Il permet ainsi :

- De garantir la cohérence des données d'identités des patients pour toutes les applications du SI hospitalier ;
- De garantir la cohérence de gestion des identités au sein des applications médicales, d'une part, et des mouvements des patients d'autre part ;
- De garantir une bonne identification du patient lors de son parcours de soins au sein du GHT.

L'identification des patients au sein des GHT s'inscrit également dans un environnement en évolution, caractérisé par le **développement des parcours au niveau d'un ou plusieurs territoires**, impliquant la nécessité de se projeter vers un identifiant patient unique qui ne se limite pas au GHT (instruction n° DGOS/PF5/2017/135 du 24 avril 2017 relative à l'accompagnement du déploiement des services numériques d'appui à la coordination [SNAC] dans les régions).

La **loi de modernisation de notre système de santé du 26 janvier 2016** consacre le **numéro d'inscription au répertoire des personnes physiques (NIR) comme identifiant national de santé (INS).**

INS au sein du GHT

L'INS et les traits d'identité provenant des bases de référence sont des données qui doivent être gérées dans les systèmes d'information de santé, médico-sociaux et sociaux.

Il y a une obligation de référencement par l'INS (R. 1111-8-3 III), mais il n'y a pas d'obligation de remplacement de l'identifiant local (exemple : IPP) par l'INS ni des traits d'identité gérés dans le SIS par les données provenant des bases de référence.

L'INS (et les traits d'identité provenant des bases de référence) s'ajoute aux données déjà gérées dans le SIS ou les remplace.

L'acteur de santé doit pouvoir associer l'INS à toute donnée de santé à caractère personnel produite par son SIS (y compris les données historisées).

A minima, l'INS (et les traits d'identité provenant des bases de référence) doit être géré avec les traits d'identités des usagers (exemple : le cas échéant, dans l'outil de gestion d'identité des patient) et le logiciel de gestion du dossier informatisé des usagers (exemple : dossier patient informatisé).

Exemples :

– En général, les structures de soins sont en mesure de rattacher un IPP à toute donnée de santé produite ; l'association entre ces données et l'INS peut se faire grâce au logiciel de gestion des identités des usagers qui gère l'association entre l'INS et l'IPP ;

– Dans les logiciels de certains acteurs de santé (exemple : professionnel libéral), les données peuvent être directement référencées avec l'INS.

INS dans le cadre des échanges avec l'extérieur de l'établissement

Dans le cadre d'échanges et de partages de données de santé, l'INS et les traits d'identité qualifiés doivent être utilisés pour référencer ces données.

Dans le cadre d'échanges et de partages de données de santé, les traits d'identité suivants doivent obligatoirement être envoyés avec l'INS : le nom, un des prénoms, le sexe et la date de naissance sont obligatoires. Le lieu de naissance et tous les prénoms sont facultatifs.

À la réception de données de santé, la vérification de la cohérence de l'INS avec les traits d'identité est obligatoire sauf s'ils ont déjà été récupérés ou vérifiés par le téléservice INS chez le récepteur des données de santé.

À la réception de données de santé, l'INS et les traits d'identité peuvent être conservés par le récepteur après la vérification de l'INS en utilisant l'opération de vérification du téléservice INS. Cette vérification devra être complétée par une procédure d'identito vigilance pour que l'INS soit considéré comme qualifié.

Téléservices de la CNAM

Deux téléservices seront proposés par la CNAM :

- **Téléservice de récupération de l'INS (court terme)** : Ce téléservice permet de collecter l'INS et les traits d'identité de l'état civil provenant des bases nationales de référence. Ce téléservice est appelé par le professionnel : de façon prioritaire, à partir de la carte vitale de l'usager ; ou, si celui-ci ne dispose pas de sa carte vitale, à partir de ses traits d'identité.
- **Téléservice de vérification de l'INS** : Ce second type de téléservice sera mis en œuvre par la Cnam, à une date restant à déterminer. Ce téléservice permet de vérifier la cohérence de l'INS et des traits d'identité transmis par un autre professionnel, par rapport aux bases nationales de référence. Il est utilisé dans le cadre d'un échange ou d'un partage de donnée de santé entre professionnels.

1.3. La cellule d'identito-vigilance

Les missions de la cellule d'identito-vigilance

Les **missions de la Cellule d'identito-vigilance** sont les suivantes :

- Mettre en œuvre la **politique d'identification** ;
- Accompagner au quotidien, ou de manière régulière, le **bureau des entrées et tous les autres services en charge de l'identification** pour le traitement et le suivi des anomalies (doublons, collisions...) ;
- Gérer les problèmes liés aux **actions d'identification du patient** ;
- Transmettre les informations nécessaires aux autres domaines d'identification pour réaliser des **rapprochements d'identités** ;
- **Alerter l'instance compétente** des éventuels dysfonctionnements dans la mise en œuvre de la politique d'identification ;

- Produire, suivre et transmettre à l'Autorité de gestion de l'identification les **indicateurs qualité** ;
- Conduire des **actions de formation, d'assistance et de sensibilisation aux politiques d'identification et de rapprochement** ;
- **Valider ou modifier les actions de rapprochement** (mise à jour, fusions, modifications, éclatement) de l'identité, et **informer** les acteurs concernés qui les répercute dans l'infrastructure centrale et les diffuse à l'ensemble des domaines concernés

La composition de la cellule d'identito-vigilance

La Cellule d'identito-vigilance est généralement composée des représentants suivants :

- Le DIM ;
- Le représentant de la direction des systèmes d'information ;
- Le représentant des admissions ;
- Un représentant des services concernés par l'identification ;
- Les membres du Comité de coordination des vigilances et de gestion des risques ;
- Toute autre personne qualifiée.

Le fonctionnement de la cellule d'identito-vigilance

La Cellule d'identito-vigilance se réunit selon une périodicité semestrielle ou un rythme permettant d'assurer une identification fiable au regard du flux de création. Les échanges tenus au cours de ces réunions sont formalisés dans des comptes-rendus.

Un système de permanence peut être assuré par un ou deux membres de la Cellule d'identito-vigilance pour traiter les cas les plus simples. Les cas les plus complexes nécessitant l'intervention du médecin DIM pour consulter les dossiers médicaux sont traités de manière périodique selon les besoins de l'établissement.

La Cellule d'identito-vigilance est l'administrateur de l'identité au sein du domaine d'identification. Ses membres disposent donc de l'ensemble des droits sur les services. Cependant au sein de la Cellule d'identito-vigilance, seul un professionnel de santé tenu au secret médical et ayant les compétences médicales adéquates dispose de l'habilitation nécessaire pour consulter les informations complémentaires du patient de nature médicale.

Enfin, la Cellule d'identito-vigilance élabore un rapport d'activité recensant notamment les actions menées pour la mise en œuvre de la politique de gestion des identités (élaboration de procédures, actions de communication, formation...) et les indicateurs d'évaluation de la qualité de l'identification des patients par les acteurs de l'établissement.

Elle met à jour la charte d'identito-vigilance.

L'identito-vigilance à l'échelle du GHT

La **Cellule d'identito-vigilance territoriale** est l'organe en charge de la surveillance et de la prévention des erreurs et des risques liés à l'identification des patients au sein d'un établissement et d'un GHT — groupe d'établissements. Elle est l'instance qui met en œuvre la politique d'identification de l'établissement et du GHT[1].

Pour mettre en place une Cellule d'identito-vigilance, le GHT – groupe d'établissements doit dans un premier temps déterminer et formaliser les éléments suivants :

- Les missions de la Cellule d'identito-vigilance ;

[1] Cf. fiche pratique « étape 3. Élaboration de la politique de gestion des identités des patients de l'établissement »

- La composition de la Cellule d'identito-vigilance ;
- Le mode de fonctionnement de la Cellule.

Les **missions de la Cellule d'identito-vigilance** sont les suivantes :

- Mettre en œuvre la **politique d'identification** du GHT — groupe d'établissements ;
- Produire, suivre et transmettre à la structure désignée les **indicateurs qualité** ;
- Élaborer les **règles de gestion** concernant le GHT — groupe d'établissements ;
- **Rédiger des manuels de procédures.**

La Cellule d'identito-vigilance territoriale est généralement composée des représentants du GHT — groupe d'établissements suivants :

- Le DIM territorial/DIM du groupe d'établissements ;
- Les DIM des établissements ;
- Les responsables des CIV des établissements ;
- Les représentants de la direction des systèmes d'information ;
- Les représentants des admissions ;
- Un représentant des services concernés par l'identification ;
- Les membres du Comité de coordination des vigilances et de gestion des risques ;
- Toute autre personne qualifiée.

La Cellule d'identito-vigilance territoriale se réunit selon une **périodicité semestrielle** ou un rythme permettant d'assurer une identification fiable au regard du flux de création. Les échanges tenus au cours de ces réunions sont formalisés dans des comptes-rendus.

La Cellule d'identito-vigilance élabore un **rapport d'activité** recensant notamment les actions menées pour la mise en œuvre de la politique de gestion des identités (élaboration de procédures, actions de communication, formation...) et les indicateurs d'évaluation de la qualité de l'identification des patients par les acteurs de l'établissement.

1.4. La politique d'identito-vigilance

Le GHT — groupe d'établissements définit sa politique d'identification et de rapprochement d'identités qu'il formalise respectivement dans une **Charte d'identification** et une **Charte de rapprochement d'identités**. Ces deux chartes peuvent être regroupées dans un seul document.

Politique et charte d'identification des patients

La politique d'identification des patients vise à garantir une identification fiable et de qualité des patients. Cette politique formalisée dans la Charte d'identification définit notamment :

- Le **périmètre de la politique** : population de patients concernée, type de prise en charge concerné, périmètre technique... ;
- Les **instances du domaine d'identification** : décrire les instances en charge de l'identification des patients (rôle, composition, modes de fonctionnement, etc.). Deux types d'instances sont décrits : l'autorité de gestion de l'identification (AGI), échelon stratégique, responsable de la définition de la politique d'identification et la cellule d'identito-vigilance (CIV) ;
- Les **principes et les processus d'identification à respecter** : procédures de création, de contrôle interne et qualité, traçabilité... ;
- Les **services d'identification** : description des grandes familles de fonctionnalités associées à l'identification des patients
- Les **états, liens et indicateurs d'identité particulière**s ;

- La **description des services d'identification** : décrire les services d'identification que peuvent utiliser les différents profils utilisateurs (patient, administratif, médical et soignant, administrateur de l'identité) ;
- La **sécurité** : principes d'authentification des utilisateurs et des applications, les habilitations des utilisateurs et des applications, les règles en matière de confidentialité, de disponibilité, etc.
- Les **critères qualité** ;
- Les **moyens techniques utilisés** ;
- Les **actions d'information — formation** ;
- Les **modalités mises en œuvre** pour assurer le respect des droits du patient, la protection de la vie privée et le respect de la confidentialité des informations médicales.

La politique d'identification prend en compte l'Identifiant National de Santé (INS).

Cette Charte doit être cohérente avec les principes énoncés dans la politique de rapprochement lorsque celle-ci existe.

Politique et charte de rapprochement des identités

La politique de rapprochement d'identités permet d'assurer la cohérence des identités partagées au sein des établissements et du GHT/groupe d'établissements ou d'organisations de santé souhaitant communiquer. La politique de rapprochement doit être élaborée par l'ensemble des établissements concernés par le serveur de rapprochement d'identités. Elle constitue un engagement entre ces établissements.

Cette politique formalisée dans la Charte de rapprochement d'identités définit notamment :

- Les règles de gestion des rapprochements ;
- Les relations entre domaines et le partage des responsabilités ;
- Le format de l'identifiant et des traits utilisés ;
- Les services disponibles ;
- Les droits d'accès à la structure de rapprochement (habilitations) ;
- Le mode d'authentification des accès (cartes ou autres) ;
- Les normes et standards utilisés ;
- Les principes de sécurisation des données[2].

Elle doit être cohérente avec la politique d'identification des organisations impliquées. Le cas échéant, elle peut amener à une modification de la politique d'identification.

Mise à jour des chartes

Ces Chartes sont définies et mises à jour par les Autorités Gestion de l'Identification/du Rapprochement (AGI/AGR) mises en place à cet effet. Ces Autorités sont également en charge de l'allocation des moyens nécessaires à la mise en œuvre de ces politiques et l'adaptation de l'organisation permettant d'assurer une identification fiable du patient. Afin de ne pas multiplier les instances faisant appel à la Direction générale, des établissements ont choisi de confier les missions de ces instances à une structure existante, telle que le Comité de pilotage « Qualité », le Comité « Qualité et gestion des risques », le Collège de l'Information Médicale, le Conseil de la Direction de l'Information médicale… .

[2] GMSIH ; Guide méthodologique à l'usage des établissements : Réalisation d'un état des lieux de l'identification du patient ; octobre 2007

Eléments d'appréciation de la HAS

Dans le cadre de l'élaboration de ces politiques, l'établissement de santé doit tenir compte des dispositions du critère 15.a. « Identification du patient à toutes les étapes de sa prise en charge » du manuel de certification v2014 de la Haute Autorité de Santé (HAS)[3]. Il trouve dans le document décrivant les éléments de vérification des experts visiteurs, les éléments qu'il veille à prendre en compte, notamment :

- **Élément d'appréciation E1.** Une organisation et des moyens permettant de fiabiliser l'identification du patient, à toutes les étapes de sa prise en charge, sont définis ;
- **Élément d'appréciation E2.** Les personnels de l'accueil administratif et les professionnels de santé sont formés à la surveillance et à la prévention des erreurs d'identification du patient. Les personnels de l'accueil administratif mettent en œuvre les procédures de vérification de l'identité du patient. Les professionnels de santé vérifient la concordance entre l'identité du bénéficiaire de l'acte et la prescription avant tout acte diagnostique ou thérapeutique ;
- **Élément d'appréciation E3**. La fiabilité de l'identification du patient à toutes les étapes de la prise en charge est évaluée à périodicité définie (indicateurs, audits) et les erreurs sont analysées et corrigées.

L'harmonisation des pratiques à l'échelle du GHT

La Cellule d'identito-vigilance territoriale met en œuvre la politique d'identification et de rapprochement d'identités du GHT — groupe d'établissements.

Pour mener à bien son activité, la Cellule d'identito-vigilance territoriale est notamment accompagnée du gestionnaire des risques et du Comité de coordination des vigilances et de gestion des risques désigné par le GHT — groupe d'établissements.

Les activités de la Cellule sont les suivantes :

- Élaboration des procédures d'identification et de rapprochement d'identités ;
- Mise en place de plans de communication et de formation au sujet de l'identification auprès du personnel de l'établissement de santé ;
- Mise en place d'un système d'évaluation et d'un suivi qualité

Harmonisation des procédures d'identification et de rapprochement d'identités au sein du GHT — groupe d'établissements :

La Cellule d'identito-vigilance territoriale rédige et établit des procédures ayant pour objectif d'appliquer la politique d'identification et de rapprochement d'identités du GHT — groupe d'établissements. Ces procédures décrivent notamment les processus d'identification du patient tels que la création, la validation ou la recherche d'une identité.

Mise en place de plans de communication et de formation au sujet de l'identification auprès du personnel du GHT — groupe d'établissements :

Afin de sensibiliser le personnel aux enjeux de l'identification du patient et porter à sa connaissance la politique d'identification de la structure, la Cellule d'identito-vigilance territoriale définit les actions. La cellule d'identito-vigilance de chaque établissement réalise les actions de communication et de formation. Deux actions de sensibilisation et de formation doivent être envisagées :

[3] Haute Autorité de Santé (HAS) ; Manuel de certification v2014 – critère 15.a « Identification du patient à toutes les étapes de sa prise en charge » ; 2014

- **Une action d'information et de communication générale** afin que l'ensemble des acteurs soit sensibilisé aux enjeux de l'identification (sessions d'information, affiches de communication).
- **Une action de formation spécifique à l'utilisation des outils au quotidien** à destination du personnel concerné (sessions de formation, assistance téléphonique, aide en ligne...).

Mise en place d'un système d'évaluation et d'un suivi qualité :

La Cellule d'identito-vigilance territoriale consolide et analyse périodiquement un tableau de bord recensant des indicateurs de qualité. Parmi ceux-ci pourront être suivis :

- **Les indicateurs portant sur la qualité des données** (taux de doublons, taux de collisions, taux de modifications de l'identité, taux d'identités créées à l'état provisoire...) ;
- **Les indicateurs portant sur l'utilisation des services** (taux de fusions, classement des informations le plus fréquemment accédées...) ;
- **Les indicateurs portant sur l'organisation de l'identification** (taux de fusions par service, classement des informations le plus fréquemment accédées par service...).

Ces indicateurs permettent d'évaluer le niveau de qualité de l'identification des patients au sein du GHT et la bonne application de la politique d'identification par les acteurs.

Ces indicateurs sont consolidés par la cellule d'identito-vigilance territoriale.

En complément de ces activités, la Cellule d'identito-vigilance territoriale peut également être amenée à réaliser en collaboration avec d'autres acteurs la définition d'une architecture technique cible du système d'identification du patient, ainsi que l'adaptation des applications « métier » existantes.

L'établissement veillera à mettre en place une gestion structurée de la documentation relative à la politique d'identification des patients au sein de la structure (charte d'identification, charte de rapprochement, procédures associées, etc.).

1.5. Les outils pour la mise en œuvre

La **démarche à suivre pour mettre à jour sa politique d'identification et de rapprochement d'identité à l'échelle de l'établissement ou dans un contexte d'harmonisation des pratiques à l'échelle d'un GHT est décrite dans documents associés à la présente fiche pratique**.

Deux documents types vous sont proposés :

- Elaborer une méthode d'identito-vigilance pour la structure
- Elaborer une méthode d'identito-vigilance pour le GHT

Dans le cadre de la mise en place de sa démarche d'identito-vigilance, le GHT / groupe d'établissements, établissement pourra également s'appuyer sur les documents suivants :

- *HAS ; Guide pour préparer et conduire votre démarche de certification V2014 : Élément de vérification des critères, 2014*
- *GMSIH ; Accompagnement à la rédaction de la politique d'identification des établissements de santé ; Octobre 2007*
- *GMSIH ; Evaluer l'existant organisationnel et technique mis en place par mon établissement (identification du patient ; Octobre 2007 ;*
- *GMSIH ; Travaux relatifs à l'identification du patient ; Avril 2002 ;*
- *ASIP Santé, Fiche pratique — Identifiant national de santé ; 2012*
- *Décret n° 2017-412 du 27 mars 2017*
- *Asip_sante_ght_identification_patients_version_publiee_v1.0.0_20180214 ; septembre 2017*
- *Article L1110-4 du Code de santé publique décrivant le périmètre d'usage de l'INS*

- *ASIP Santé, Référentiel Identifiant National de Santé ; février 2018*
- *Fil de discussion sur le site de l'ANAP — appel à commentaires sur les futurs usages de l'INS*
- *ASIP Santé, Le référencement des données de santé avec l'INS ; mai 2018*
- *RREVA, Article sur l'identito vigilance dans la région Nouvelle Aquitaine ; janvier 2019*
- *CTRI Nouvelle Aquitaine — Référentiel_identito_NA_V2.2 ; janvier 2019*

2. FICHE 2 — MISE A JOUR DU REFERENTIEL UNIQUE DE STRUCTURE

2.1. Contexte et périmètre

Contexte et objectifs

Le socle commun du **programme HOP'EN** est constitué de **4 prérequis** indispensables à une gestion sécurisée des soins dans un contexte de décloisonnement des prises en charge, dont la mise en place, par l'ensemble des établissements de santé est attendue d'ici la fin du programme :

- Identités, mouvements (P1) ;
- Sécurité (P2) ;
- Confidentialité (P3) ;
- Échanges et partages (P4).

Il comprend également **7 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.

- Les résultats d'imagerie, de biologie et d'anatomopathologie (D1) ;
- Le dossier patient informatisé et interopérable et le DMP (D2) ;
- La prescription électronique alimentant le plan de soins (D3) ;
- La programmation des ressources et l'agenda du patient (D4) ;
- Le pilotage médico-économique (D5) ;
- La communication et les échanges avec les partenaires (D6) ;
- La mise à disposition de services en ligne aux usagers et aux patients (D7).

Le prérequis « Identités, mouvements » comprend 4 indicateurs, dont **l'indicateur P1.4 portant sur l'existence d'un référentiel unique de structure de l'établissement (juridique, géographique et fonctionnel) piloté et mis à jour régulièrement dans les applicatifs, en temps utile**.

La présente fiche a pour objectif d'aider les établissements de santé à **mettre en place ou à amender leur procédure de mise à jour du référentiel unique de structure** pour accompagner **:**

- Les évolutions **organisationnelles** des établissements de santé, qui résultent notamment de la mise en place des GHT : convergence des fonctions médico-techniques et administratives, mutualisation des ressources et des moyens, partage des référentiels.
- Les évolutions **informatiques et techniques** en termes de convergence applicative : la définition d'un fichier commun des structures de l'ensemble des établissements parties du GHT constitue un prérequis à la convergence applicative de celui-ci ainsi que pour assurer la cohérence des différents recueils médico administratifs.

Indicateur concerné

La fiche concourt principalement à l'obtention de :

- **L'indicateur P1.4 Existence d'un référentiel unique de structure de l'établissement (juridique, géographique, fonctionnel) piloté et mis à jour régulièrement dans les applicatifs.**

L'élaboration d'une procédure de mise à jour du référentiel unique de structure a pour objectif de décrire les modalités d'actualisation du référentiel susvisé d'une part, et le mode d'intégration de ces mises à jour dans les applicatifs d'autre part. Elle concerne le découpage interne de l'établissement et les relations avec les autres membres dans le cadre des établissements regroupés en GHT, mais n'exclut pas la cohérence avec d'autres sources de données.

2.2. Procédure de mise à jour du référentiel unique de structure

Pour accompagner les établissements dans la mise en place ou l'actualisation d'une Procédure de mise à jour du référentiel unique de structure, vous trouverez ci-après des prérequis à sa mise en œuvre. Un modèle de Procédure est ensuite présenté dans la boîte à outils.

Objectifs de la procédure

La Procédure a pour objectifs de :

- Décrire le processus de mise à jour du référentiel unique de structure en précisant les modalités de mise à jour du référentiel susvisé.
- Définir le mode d'intégration de ces mises à jour dans les applicatifs constituant le SIH.
- Décrire les procédures de mise à jour et de leur intégration dans un contexte de GHT

Procédure de mise à jour et GHT

L'établissement support devra s'assurer que chaque établissement partie du GHT a mis en place une procédure de mise à jour du référentiel unique de structure de l'établissement et de la propagation de ces évolutions aux diverses applications.

L'objectif est que ce document soit harmonisé au sein du GHT en produisant, par exemple, une procédure commune de GHT dont les dispositions s'appliquent à tous, complétée si besoin par des procédures par établissement partie.

L'harmonisation des organisations des structures (arborescence, formats, principes de mise à jour et diffusion) doit permettre de produire une version consolidée de la structure au niveau du GHT qui représente un référentiel essentiel à la production des indicateurs médico-économiques et aux processus transverses du GHT.

Diffusion de la procédure

Une fois validé par les instances concernées, le référentiel commun de structure doit être communiqué à tous les utilisateurs et responsables pour diffusion dans les services respectifs (chefs de services médicaux et médico-techniques, chefs de pôles, cadres de santé, directeur et directeurs adjoints, cadres et ingénieurs). Il convient que les responsables fassent le lien avec leurs équipes respectives (notamment avec les secrétaires médicales), afin que cette information soit connue et maitrisée par l'ensemble du personnel.

Il est conseillé de prévoir dans le document de diffusion de ce référentiel commun, un glossaire clair des abréviations utilisées afin que tous les lecteurs, ayant des domaines de compétences différents, puissent le lire en toute compréhension.

2.3. Les outils pour la mise en œuvre

Un **modèle de procédure de mise à jour du référentiel unique de structure de l'établissement** est proposé pour être adaptée au contexte et à l'organisation en place.

Le modèle type de procédure est composé des sections :

- Le **champ d'application du document** : décrit les types de structure et acteurs concernés par la présente procédure. Elle sera adaptée par l'établissement en fonction de l'organisation interne qu'il aura choisi de mettre en place pour maintenir à jour le référentiel unique de structure et les données associées contenues dans les applicatifs présentées au point 3. « Organisation interne et responsabilités » ;
- **L'organisation interne et les responsabilités** : décrit l'organisation interne retenue par l'établissement pour maintenir à jour le référentiel unique de structure et les données associées dans les applicatifs. La proposition d'organisation ci-dessous sera donc adaptée par l'établissement en fonction de celle qu'il aura choisi de retenir. Il pourra par ailleurs ajouter ici toute autre information portant sur les responsabilités confiées aux acteurs qui sera jugée pertinente ;
- Le **mode opératoire** : présente le mode opératoire de mise à jour du référentiel unique de structure et des données associées contenues dans les applicatifs tel que défini par l'établissement. Une proposition de mode opératoire est présentée ci-dessous ; celle-ci sera adaptée par l'établissement en fonction du processus qu'il souhaite mettre en place pour maintenir à jour le référentiel unique de structure et les données associées dans les applicatifs. Enfin, il pourra être ajouté dans la présente section toute information jugée pertinente par l'établissement ;
- La **propagation des mises à jour au sein du système d'information** : décrit le mode de propagation des modifications effectuées dans le référentiel unique de structure au sein du système d'information retenu par l'établissement de santé. Plusieurs modes de propagation peuvent coexister, selon les applications et selon le type de modifications à apporter (évolutions mineures des structures existantes, ou refonte majeure). Il s'agit de décrire chaque mode de propagation possible, les applications concernées, ainsi que les règles d'application de chacun ;
- Le **suivi de la mise en œuvre de la procédure** : présente les modalités de suivi de la mise en œuvre de la procédure. Elle sera donc adaptée aux modalités de suivi que souhaite mettre en œuvre l'établissement de santé. Toute autre information jugée pertinente pourra être ajoutée par l'établissement de santé.

Pour aller plus loin, l'établissement de santé pourra se référer aux documents suivants :

- Direction Générale de l'Offre de Soins (DGOS) ; Guide méthodologique de comptabilité analytique hospitalière, 2011 ;
- Agence Technique de l'Information Hospitalière (ATIH) ; Guides méthodologiques de production du PMSI ;
- Groupement de Modernisation des Systèmes d'Information Hospitaliers (GMSIH) ; Référentiels SID des ES — Synthèse globale — Bien gérer ses référentiels de données : Un enjeu pour mieux piloter la performance de son établissement ; pages 23-30 ; octobre 2008 ;
- Agence Régionale de l'Hospitalisation (ARH) Aquitaine ; Formation Fichier structure ; 22 février 2008
- Livre Blanc « Distribution de définition de structure d'établissement », Interop'Santé

3. FICHE 3 — PLAN DE REPRISE D'ACTIVITE ET PROCEDURES DE FONCTIONNEMENT EN MODE DEGRADE

3.1. Contexte et périmètre

Contexte et objectifs

Le socle commun du **programme HOP'EN** est constitué de **4 prérequis** indispensables à une gestion sécurisée des soins dans un contexte de décloisonnement des prises en charge, dont la mise en place, par l'ensemble des établissements de santé est attendue d'ici la fin du programme :

- Identités, mouvements (P1) ;
- Sécurité (P2) ;
- Confidentialité (P3) ;
- Échanges et partages (P4).

Il comprend également **7 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.

- Les résultats d'imagerie, de biologie et d'anatomopathologie (D1) ;
- Le dossier patient informatisé et interopérable et le DMP (D2) ;
- La prescription électronique alimentant le plan de soins (D3) ;
- La programmation des ressources et l'agenda du patient (D4) ;
- Le pilotage médico-économique (D5) ;
- La communication et les échanges avec les partenaires (D6) ;
- La mise à disposition de services en ligne aux usagers et aux patients (D7).

En lien avec le prérequis 2 « Sécurité », le présent document met à la disposition des établissements de santé une méthode de formalisation d'un Plan de Reprise d'Activité ainsi que pour l'élaboration de procédures de fonctionnement en mode dégradé.

Les méthodes décrites dans cette fiche ont vocation à être améliorées et partagées au sein de la communauté de pratique ainsi que les réseaux et groupes d'entraide.

Indicateurs concernés

La fiche concourt principalement à l'obtention de :

- **L'indicateur P2.1 portant sur l'existence d'un Plan de Reprise d'Activité (PRA) du système d'information formalisé.**
- **L'indicateur P2.3 portant sur l'existence de procédures assurant d'une part un fonctionnement dégradé du système d'information au cœur du processus de soins en cas de panne et d'autre part un retour à la normale.**

Enjeux

Les exigences réglementaires en matière de sécurité des données et notamment l'application de la PGSSI-S imposent aux établissements de santé de prévoir et de mettre en place un ensemble de dispositions pour assurer le fonctionnement en mode dégradé en cas de crise temporaire perturbant ou arrêtant de fonctionnement au l'accès au centre informatique et la reprise de l'activité de son système d'information pour un retour à la normale avec récupération des données et réactivation des services perdus.

Chaque service ou entité qui utilise des applications logicielles « métier » critiques doit pouvoir maintenir son activité afin de prévenir tout dysfonctionnement pouvant engendrer des conséquences cliniques majeures tel que l'absence ou le retard dans l'administration du traitement et des actes, des répétitions d'actes, des retards voire des erreurs de diagnostic, l'impossibilité de réaliser des actes ou des examens, la discontinuité du suivi médical.

3.2. Plan de Reprise d'Activité

Objectif du document

Le Plan de Reprise d'Activité (PRA) du système d'information représente un plan d'action décrivant les moyens techniques, organisationnels et humains permettant d'assurer la reprise de l'activité du système d'information en cas d'indisponibilité totale ou partielle.

Plan de reprise dans le contexte d'un GHT

Les enjeux de continuité des services et de reprise de l'activité des systèmes d'information sont renforcés dans le cadre de la mise en place des GHT et des évolutions applicatives que cela engendre : Concentration des services numériques sur une architecture centralisée (interne ou externe) augmentant le nombre d'utilisateurs et donc l'impact d'un dysfonctionnement ; augmentation du nombre et de la complexité des dispositifs techniques nécessaires à l'accès aux services numérique (Réseau physique, VPN, Firewall…) ; hétérogénéité des configurations des terminaux utilisateurs.

Pour ces raisons, il est souhaitable que l'ensemble des établissements du GHT élaborent un PRA harmonisé tenant compte des particularités de chaque établissement et de l'organisation mise en place dans le cadre du GHT notamment en termes d'astreintes.

Cette démarche d'harmonisation est d'autant plus importante lorsque des établissements sont en situation de partage des infrastructures telles que des salles serveur impliquant, dans ce cas particulier, la nécessité d'une mise en commun de leur PRA.

Contrôle et mise à jour du PRA

Le plan de Reprise d'Activité est un ensemble de procédure et de dispositifs techniques qu'il est indispensable de faire évoluer en cohérence avec les évolutions du système d'information et de son déploiement. Ainsi, l'opportunité de mettre à jour le PRA doit être étudiée dans les cas suivants :

- Déploiement d'un nouveau service numérique au sein du SIH ;
- Mise en place d'une fonctionnalité significative pouvant entrainer une modification dans l'analyse de la criticité d'un système ;
- Changement ou déplacement d'un composant d'architecture technique soutenant un service numérique ;
- Évolution organisationnelle ou dans l'activité de l'établissement incluant une dépendance au système d'information ;
- Périodiquement pour garantir la pertinence du PRA.

En complément de ce dernier point, le PRA doit être éprouvé et testé de façon régulière afin d'en évaluer la fiabilité au travers de phases de tests ou de remontées suite à échec en condition maitrisée sans attendre sa mise en application lors de l'apparition d'un incident réel.

3.3. Fonctionnement en mode dégradé et retour à la normale du système d'information

Objet

Le « fonctionnement en mode dégradé » couvre :

- La bascule du mode de fonctionnement nominal vers le mode dégradé ;
- Le fonctionnement en mode dégradé durant la durée d'indisponibilité du système ;
- Le retour au fonctionnement nominal une fois le système disponible et la reprise de l'activité réalisée en mode dégradé.

Cette démarche est à faire globalement en impliquant chaque service ou entité qui utilise des applications métier critiques pour assurer ses activités :

- Les unités de soins ;
- Les unités de soins critiques ;
- Le bloc opératoire ;
- Les plateaux techniques : radiologie, biologie ;
- Etc.

Elle est menée en association entre un référent des services concernés et le référent de la DSI.

En pratique, chaque service doit s'approprier les procédures dégradées définies par l'établissement, s'assurer de leur mise à jour et les adapter, le cas échéant, à ses modalités spécifiques de fonctionnement..

Une démarche en 4 étapes

Étape 1 : Lister les procédures à élaborer

A minima il faut prévoir pour chacune des applications critiques (recensées dans la cartographie applicative) une procédure pour basculer en mode dégradé, une procédure de fonctionnement en mode dégradé et une procédure pour revenir en fonctionnement normal. Pour une même application, ces procédures devraient être adaptées aux services et usages.

Pour les procédures, Il faut d'abord envisager le cas de l'arrêt programmé ; il est dans ce cas, possible d'anticiper et de préparer l'arrêt et le basculement en mode dégradé. Les documents nécessaires au maintien de l'activité peuvent être imprimés avant l'arrêt. Cette tâche sera d'autant moins lourde que l'arrêt programmé doit être prévu dans une période d'activité réduite (nuit, week-end).

Les procédures prévues pour le cas de l'arrêt programmé doivent être adaptées à ce qui est possible pour les cas de pannes.

Étape 2 : Identifier les fonctions et les informations essentielles pour le service concerne

Parmi toutes les fonctionnalités de l'application métier concernée, se limiter aux fonctions majeures, indispensables au maintien de l'activité, en distinguant :

- Les activités relatives aux échanges avec des services extérieurs ;
- Les activités propres au fonctionnement interne du service.

Activités relatives aux échanges avec les services extérieurs

Pour une unité de soins, il s'agit d'une part de pouvoir continuer à produire des demandes (imagerie, biologie, examens complémentaires, prescription de médicaments), d'autre part de recevoir et consulter les résultats.

Pour un plateau technique, il s'agit de recevoir les prescriptions et demandes diverses, et pouvoir y répondre.

Recenser l'ensemble des services avec lequel le service concerné travaille et les informations échangées avec ces services, par exemple :

- L'identité du patient ;
- L'objet de la demande ;
- Le service prestataire ;
- Des informations complémentaires du patient ;
- Etc.

Activités propres au fonctionnement interne du service

Pour une unité de soins, il faut par exemple pouvoir continuer à prescrire et administrer les soins et les produits de santé.

Pour un plateau technique, il faut pouvoir continuer à réaliser les examens demandés et produire les résultats, donc par exemple pour la radiologie, avoir la liste des rendez-vous et examens programmés pour la journée.

Chaque service liste les informations nécessaires à son fonctionnement, par exemple :

- Les prescriptions ;
- Le plan de soins ;
- Les rendez-vous du jour ;
- Etc.

Étape 3 : Mettre en œuvre les moyens techniques pour maintenir les activités

Une fois identifiées les informations indispensables à la poursuite des activités, il s'agit de préciser et définir :

- Les documents et modèles à utiliser ;
- Comment trouver ces documents en l'absence de l'application informatique

Pour ce faire, il conviendra de tenir compte des logiciels associés aux dispositifs médicaux susceptibles de détenir ces informations.

Pour mettre en œuvre ces moyens, il faut s'appuyer sur les solutions proposées par les éditeurs des applications informatiques et bâtir la procédure à mettre en œuvre avec son support. Souvent, les solutions et procédures sont différentes pour les arrêts programmés et pour les pannes. Tout arrêt programmé d'une application critique doit faire l'objet d'une proposition de fonctionnement en mode dégradé par l'éditeur ou l'intégrateur.

Le principe général de ces solutions est de dupliquer les informations essentielles (typiquement une synthèse du dossier patient, le plan de soins, la prescription en cours, etc.) en dehors de la base de données de l'application, sous une forme directement imprimable (par exemple des PDF.). Cette extraction des données sous un format imprimable peut être faite à une fréquence adaptée aux besoins ; les données sont alors stockées sur un serveur central ou des postes locaux dans les services (cette étape peut nécessiter un paramétrage spécifique à réaliser dans l'application, avec le support de l'éditeur (paramétrage des traitements batch, réalisation des modèles de documents à imprimer, etc.). Il faut veiller à la confidentialité des informations contenues dans ces postes.

Il faut ensuite prévoir les procédures pour imprimer les supports en cas d'arrêt programmé ou de panne pour assurer le fonctionnement en mode dégradé ; la diffusion des documents aux utilisateurs est à prévoir.

Pour d'autres cas, des moyens simples doivent être prévus, souvent en s'appuyant sur les suggestions des utilisateurs, par exemple l'impression de bordereaux vierges (par exemple, aux admissions, ou pour les demandes d'examens des unités de soins) conservés dans les services.

Étape 4 : Définir le mode de bascule du fonctionnement nominal vers le fonctionnement en mode dégradé

Une fois les moyens « techniques » préparés qui permettent d'assurer le fonctionnement en mode dégradé, il est nécessaire de préciser les procédures de bascule en mode dégradé, en continuant à distinguer les arrêts programmés et les pannes.

En effet en cas d'arrêt programmé (typiquement pour une mise à jour de version), la direction et le personnel sont informés à l'avance ; en particulier, la durée prévisionnelle de l'arrêt est indiquée (sur la base des informations fournies par l'industriel réalisant la maintenance) ; les informations et documents nécessaires sont imprimés avant l'arrêt de l'application de façon à ce qu'ils soient déjà disponibles dans le service au moment de l'arrêt. Les arrêts programmés sont prévus à des moments de plus faible activité ; le volume d'informations à imprimer est de ce fait réduit.

En cas de panne, les mêmes documents sont imprimés, autant qu'il est possible avec les moyens disponibles, et transmis aux utilisateurs. Informer la direction et les utilisateurs doit être prévu.

Étape 5 : Définir le mode de bascule du fonctionnement nominal vers le fonctionnement en mode dégradé

La procédure de fonctionnement en mode dégradé doit prévoir le retour à la normale.

Durant la période de fonctionnement en mode dégradé, des informations ont été produites principalement sur des documents papier.

Une fois le système de nouveau disponible, il est nécessaire de reprendre manuellement dans le système les informations, pour que l'application soit de nouveau à jour. Il faut donc conserver les documents utilisés et définir quelles sont les données à reprendre et par qui. Il est nécessaire de prendre en compte le temps total de perte de données qui peut être supérieur au temps de l'arrêt lorsque les données sont restaurées à partir de la sauvegarde.

Exemples de procédures

Pour une unité de soins :

- **En fonctionnement normal**
  - Un correspondant de la DSI est identifié pour préparer le fonctionnement en mode dégradé et faciliter la bascule (par exemple, il s'assure de la disponibilité des documents et supports nécessaires au fonctionnement en mode dégradé) ;
  - Anticiper la disponibilité dans les services des différents bordereaux vierges de demandes nécessaires aux échanges avec les autres services ;
  - Informer de l'existence de cette procédure et la tenir à disposition dans le service.
  - Maintenir la procédure à jour en fonction des changements fonctionnels, techniques, de paramétrage, de déploiement de fonctionnalités.
- **Fonctionnement en mode dégradé**
  - Décision de déclencher le fonctionnement en mode dégradé ;
  - Information des personnels (du service et des services extérieurs) que la procédure de fonctionnement en mode dégradé s'applique ;
  - Utilisation des supports prévus et mise en œuvre de l'organisation prévue ;
  - Mise à disposition du service des données de secours permettant la poursuite de l'activité (impression des documents stockés sur un serveur centralisé ou localement, mise à disposition de matériel autonome…).
- **Retour à la normale**

- Décision de reprise suite à une confirmation de la remise en fonction des services numériques ;
- Information des personnels (du service et des services extérieurs) ;
- Identification des données « perdues » (*en cas de restauration des données à partir des données de sauvegarde, il peut y avoir eu perte de données, entre la date de la dernière sauvegarde et le moment où la procédure en mode dégradé a été appliquée)*
- Collecte des informations à reprendre dans le système ;
- Saisie des informations dans le système.

Procédures de fonctionnement en mode dégradé dans le contexte d'un GHT

Dans le cadre d'un GHT, il est recommandé qu'un travail soit mené entre les établissements parties du GHT sur l'uniformisation des procédures dégradées et particulièrement sur les applicatifs en cours de convergence ou convergés dans le cadre d'un Système d'Information de GHT tel que la loi n° 2016-41 et Décret n° 2016-524 du 27 avril 2016 le définissent.

3.4. Les outils pour la mise en œuvre

Un modèle de plan de reprise d'activité est proposé.

De plus, dans le cadre de l'élaboration de son PRA du système d'information, ainsi que des procédures de fonctionnement en mode dégradé et de retour à la normale du système d'information l'établissement de santé pourra également s'appuyer sur les documents suivants :

- Club de la Sécurité de l'Information Français (CLUSIF) ; Plan de continuité d'activité — Stratégie et solutions de secours du SI ; Septembre 2003 ;
- AFNOR Normalisation ; Plan de continuité d'Activité pour les PME/PMI de la région Centre — outil méthodologique ; 2010

4. FICHE 4 — ÉVALUATION DES TAUX DE DISPONIBILITE

4.1. Contexte et périmètre

Contexte et objectifs

Le socle commun du programme HOP'EN est constitué de 4 prérequis indispensables à une gestion sécurisée des soins dans un contexte de décloisonnement des prises en charge, dont la mise en place, par l'ensemble des établissements de santé est attendue d'ici la fin du programme :

- Identités, mouvements (P1) ;
- Sécurité (P2) ;
- Confidentialité (P3) ;
- Échanges et partages (P4).

Il comprend également 7 domaines fonctionnels pour lesquels le programme définit des exigences en matière d'usage du système d'information.

- Les résultats d'imagerie, de biologie et d'anapath (D1) ;
- Le dossier patient informatisé et interopérable et le DMP (D2) ;
- La prescription électronique alimentant le plan de soins (D3) ;
- La programmation des ressources et l'agenda du patient (D4) ;
- Le pilotage médico-économique (D5) ;
- La communication et les échanges avec les partenaires (D6) ;
- La mise à disposition de services en ligne aux usagers et aux patients (D7).

Le présent document propose une méthode pour la mise en œuvre d'une démarche d'évaluation des taux de disponibilité cibles des applicatifs au sein d'un établissement de santé lui permettant ainsi d'atteindre les prérequis du programme HOP'EN.

Indicateur concerné

La fiche concourt principalement à l'obtention de :

– **L'indicateur P2.2 portant sur la définition d'un taux de disponibilité cible des applicatifs et mise en œuvre d'une évaluation de ce taux.**

4.2. Présentation

Enjeux

La définition des taux de disponibilité et leur évaluation continue permettent de répondre aux exigences réglementaires en matière de continuité et de sécurité des soins ainsi qu'aux notions fondamentales de la sécurité « DICP » qui regroupe les 4 notions : la disponibilité (D), l'intégrité (I), la confidentialité (C) et la preuve (P).

L'appréciation des risques d'indisponibilité pour chaque applicatif représente donc un enjeu pour la qualité de la prise en charge des patients et se situe au centre des priorités des établissements de santé en termes de qualité et de sécurité.

Le besoin en disponibilité des applications

Ce paragraphe est basé sur les travaux menés dans le cadre de l'élaboration de la Politique Générale de sécurité du Système d'Information de Santé, travaux menés par l'ASIP Santé et pilotés par la DSSIS.

La disponibilité est l'aptitude d'un dispositif à être en état de fonctionner dans des conditions données. C'est la disponibilité opérationnelle des applications dont il s'agit ici, pour fournir aux utilisateurs le service attendu.

Les besoins en disponibilité sont évalués en fonction de la criticité de chaque application en termes de risques et d'impact sur la qualité/sécurité de la prise en charge des patients. Cette évaluation doit être réalisée par chaque établissement en concertation avec les utilisateurs des différentes applications.

NB : Dans le cas où les services de l'établissement expriment des besoins de disponibilité différents pour une même application, c'est le besoin en disponibilité le plus élevé qui doit être retenu.

Un effort de pédagogie doit cependant être réalisé auprès des acteurs sollicités pour identifier le juste niveau de disponibilité attendu et ainsi permettre de focaliser les moyens de l'établissement.

Une échelle de 1 à 4 permet de classifier les applications selon leur besoin en disponibilité :

1	Faible	Absence de besoin de disponibilité. L'application peut être indisponible sans limites.
2	Significatif	L'application peut être indisponible pendant une durée importante, mais limitée.
3	Important	L'application peut être indisponible pendant une courte durée.
4	Critique	L'application ne doit pas être indisponible.

Les besoins en disponibilité sont valorisés comme suit (selon les travaux menés dans le cadre de la PGSSI-S) :

1. Faible : taux de disponibilité supérieur à 95 % ce qui correspond à une durée d'indisponibilité de 36 h par mois ou de 18 j par an
2. Significatif : taux de disponibilité supérieur à 99 % ce qui correspond à une durée d'indisponibilité de 7 h par mois ou de 3,5 j par an
3. Important : taux de disponibilité supérieur à 99,5 % ce qui correspond à une durée d'indisponibilité de 3 h 30 par mois ou de 2 j par an
4. Critique : taux de disponibilité supérieur à 99,9 % ce qui correspond à une durée d'indisponibilité de 40 min par mois ou de 8 h 30 par an

NB : L'évaluation de la durée acceptable d'indisponibilité s'entend sans mise en œuvre de la procédure dégradée de contunité d'activité.

Méthode d'évaluation du taux de disponibilité

Il est fortement recommandé que chaque établissement définisse des processus d'évaluation des taux de disponibilité de ses applicatifs et qu'il effectue son choix en fonction de sa situation. Le programme HOP'EN n'impose pas de méthode de calcul et d'évaluation du taux de disponibilité d'une application. Il propose cependant, dans le cadre de la présente fiche, un moyen simple pouvant être adopté par l'établissement.

En règle générale il existe 2 grandes façons de mesurer le taux de disponibilité :

- Mesure du fonctionnement de l'application au niveau des serveurs ;

- Mesure du bon fonctionnement de l'application au niveau du poste de travail.

Ce dernier type de mesure permet de prendre en compte un nombre plus large de causes de dysfonctionnement (indisponibilité réseau, anomalie au niveau du poste de travail…). Cependant, il est très dépendant des conditions de mesure au niveau du poste de travail.

Dans le cadre des prérequis du programme HOP'EN, il est proposé une mesure simple faite au niveau des serveurs de production de l'application.

La mise en œuvre d'un outil de supervision au niveau des serveurs suffit. Il permet de réaliser un calcul automatique des temps d'indisponibilité et de relever a minima :

- La date et l'heure de l'incident ou de l'arrêt programmé ;
- L'application concernée ;
- La date et l'heure de retour à la normale.

En cas d'absence d'outil de supervision système, ces temps pourront être calculés de manière manuelle par une personne habilitée. Une procédure sera alors élaborée afin de décrire le processus de mesure manuelle des temps d'indisponibilité.

Cette traçabilité est effectuée au fil de l'eau, pour chaque incident et arrêt programmé. Le taux de disponibilité est évalué de façon régulière à partir de ces données, pour chaque application. Le suivi de l'indicateur permet de détecter des dérives ou de mesurer les progrès de disponibilité.

Le taux de disponibilité des applications du SIH est ensuite défini par la médiane des taux de disponilité par application.

Il est évalué à fréquence régulière, a minima par trimestre et si possible mensuellement.

Exemples de besoin en disponibilité pour les applications

Besoin faible

- Base de données anonymisée pour calculs statistiques
- Supports multimédias destinés à l'illustration des dossiers et à l'enseignement
- Réseau social d'entreprise et espaces de travail collaboratifs

Besoin significatif

- Liste des essais cliniques, études et projets
- Gestion des échantillons biologiques
- Système de commande de repas
- Check-list opératoire
- Archives médicales
- Gestion économique et financière
- Gestion RH

Besoin important

- Accès au SGL (Système de Gestion de laboratoire) pour consulter un résultat d'analyses (si indisponible, possibilité de récupérer les résultats directement à partir des automates)
- Accès au PACS pour comparaison examens antérieurs à des fins d'interprétation (possibilité de différer l'interprétation)
- Accès au système de gestion des rendez-vous (possibilité d'interrompre temporairement la prise de rendez-vous)
- Worklists pour modalités d'imagerie
- Messagerie électronique
- Facturation des séjours et des actes et consultations externes

Besoin critique

- Accès aux images radiologiques (via le PACS) ainsi qu'aux dossiers de consultations préopératoires et préanesthésiques en contexte d'intervention au bloc opératoire
- Accès à la carte de groupe et aux RAI (Recherche d'Agglutinines Irrégulières) avant un acte transfusionnel
- Accès aux dernières prescriptions et administrations dans une unité d'hospitalisation (risque d'erreur de médication : de double prescription ou administration, risque d'absence d'administration)
- Accès au serveur d'identité pour la création d'un nouveau dossier patient
- Accès aux transmissions infirmières

4.3. Les outils pour la mise en œuvre

Un modèle de méthode d'évaluation des taux de disponibilité du SI est proposé.

5. FICHE 6 — ROLES DE RSSI ET DPO

5.1. Contexte et périmètre

Contexte et objectifs

Le socle commun du **programme HOP'EN** est constitué de **4 prérequis** indispensables à une gestion sécurisée des soins dans un contexte de décloisonnement des prises en charge, dont la mise en place, par l'ensemble des établissements de santé est attendue d'ici la fin du programme :

- Identités, mouvements (P1) ;
- Sécurité (P2) ;
- Confidentialité (P3) ;
- Échanges et partages (P4).

Il comprend également **7 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.

- Les résultats d'imagerie, de biologie et d'anapath (D1) ;
- Le dossier patient informatisé et interopérable et le DMP (D2) ;
- La prescription électronique alimentant le plan de soins (D3) ;
- La programmation des ressources et l'agenda du patient (D4) ;
- Le pilotage médico-économique (D5) ;
- La communication et les échanges avec les partenaires (D6) ;
- La mise à disposition de services en ligne aux usagers et aux patients (D7).

Cette fiche pratique a pour objectifs d'aider les établissements dans le recrutement et la rédaction des fiches de postes de RSSI / DPO en présentant les fonctions relevant du RSSI et celles relevant du DPO, ainsi que les compétences techniques et personnelles requises pour accomplir ces tâches à l'échelle :

- D'un établissement de santé ;
- D'un groupe d'établissements / groupement hospitalier de territoire (GHT).

Il est à noter que les postes de RSSI et de DPO peuvent être assurés par une même personne. Le poste de DPO peut par ailleurs être assuré à l'échelle d'un GHT.

Indicateur concerné

La fiche concourt principalement à l'obtention de :

- **L'indicateur P2.4 du prérequis « Sécurité » : présence d'une politique de sécurité et plan d'action SSI réalisé, existence d'un responsable sécurité.**
- **L'indicateur P3.6 du prérequis « confidentialité » : existence d'une fonction DPO et présence d'un registre des traitements de DCP qualifié avec droits d'accès.**

Les enjeux de la sécurité des SI de santé

L'accélération du développement du numérique dans le domaine du soin, du dépistage ou encore de la prévention fait exploser le nombre de données de santé. Ces données sont sensibles, exposées et peuvent être convoitées comme l'indique l'ASIP Santé sur son site internet :

- Sensibles, parce qu'elles sont privées et convoitées. Encadrées par la loi Kouchner de 2002, les données de santé relèvent de la vie privée du patient et sont de ce fait soumises au secret professionnel, donc protégées.

- Vulnérables, parce que les équipements sont vieillissants et les protections moins efficaces que dans d'autres secteurs. Moins d'outils de scan de vulnérabilité, moindre connaissance des menaces, obsolescence du matériel bureautique…
- Exposées, parce que le système de santé est nécessairement ouvert à une multitude d'acteurs et d'objets connectés peu sécurisés. Avec des patients et des médecins, qui veulent échanger de plus en plus. Un défi puisque près de 150 000 structures et 1 million de personnels de santé qui ont une appréhension hétérogène des enjeux de sécurité.

C'est dans ce contexte que s'inscrivent les mesures relatives à la sécurité des SI portées par notamment par la PGSSI.

Les établissements de santé doivent impérativement se saisir de cette problématique compte tenu des enjeux. La mise en place des RSSI au sein des établissements de santé a marqué un premier temps fort en matière de reconnaissance des enjeux liés à la sécurité des SI. Il s'agit pour les établissements de poursuivre leurs efforts dans ce domaine à l'échelle des GHT et en définissant une stratégie de sécurité des SI, composante du SDSI et que les établissements déclineront ensuite. L'adossement de la stratégie de sécurité des SI au SDSI valorisera ce sujet qui reste encore assez confidentiel ou en tout cas diversement approprié dans les établissements de santé.

C'est dans le contexte d'enjeux croissants en matière de sécurité des SI que la fonction de RSSI a été mise en place.

Création du rôle de DPO dans le cadre de la mise en œuvre du RGPD

Tous les établissements de santé sont concernés par le RGPD en tant que responsables de traitement de données personnelles dans leur organisme, et parfois également comme sous-traitants (dans le cadre d'un groupement par exemple). Le RGPD porte sur toutes les données personnelles issues des activités de l'établissement de santé, et pas uniquement sur les données de santé générées par la prise en charge des personnes.

Dans le cadre de la mise en œuvre du règlement depuis mai 2018, les établissements de santé sont tenus à certaines obligations : les établissements publics de santé sont ainsi tous obligés de désigner un délégué à la protection des données (DPD ou DPO), tandis que les établissements privés de santé sont potentiellement concernés, selon qu'ils mettent ou non en œuvre un traitement de données sensibles « à grande échelle ».

Responsable de la conformité en matière de protection des données au sein de l'établissement, le délégué à la protection des données est principalement chargé :

- D'informer et de conseiller le responsable de traitement ou le sous-traitant ainsi que leurs employés ;
- De contrôler le respect du règlement et du droit national en matière de protection des données ;
- De conseiller l'établissement sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- De coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

GHT

La mise en œuvre, dans le cadre d'un GHT, d'un projet commun de convergence des systèmes d'information vers un système d'information unique et homogène rend indispensable une réflexion sur la gestion de la sécurité des systèmes d'information à l'échelle du GHT. C'est dans ce nouveau contexte que l'exercice des fonctions de responsable de la sécurité des systèmes d'information (RSSI) et de délégué à la protection des données (DPO) doivent être pensés.

Leur exercice au sein d'un GHT n'est pas fondamentalement différent de celui au sein d'un établissement, mais il se voit complexifié par la multiplicité des acteurs, des enjeux et des contraintes. Il en ressort une nécessité encore plus grande de définir avec précision son cadre d'exercice et les missions qui leur sont confiées.

Le RSSI est obligatoirement mutualisé entre plusieurs structures à l'échelle d'un GHT. Le DPO peut quant à lui être mutualisé à l'échelle d'un GHT. Les fonctions de RSSI et de DPO peuvent être assurées par la même personne.

5.2. Les outils pour la mise en œuvre

Les fiches de poste du RSSI / DPO élaborées par l'établissement de santé / le GHT / le groupe d'établissements précisent *a minima* les informations suivantes :

1. La présentation de l'établissement de santé / du service de rattachement du RSSI / DPO ;
2. Le contexte d'intervention du RSSI / DPO ;
3. La description des missions et des activités du RSSI / DPO ;
4. Le profil et les compétences attendues pour occuper ces fonctions ;
5. Les moyens mis à disposition du RSSI / DPO par l'établissement de santé.

Pour accompagner les établissements de santé / GHT / groupe d'établissement dans l'élaboration d'une fiche de poste du RSSI et/ou DPO adaptée à leurs besoins, deux modèles de fiches de poste sont proposés :

- Modèle de fiche de poste de DPO
- Modèle de fiche de poste de RSSI

Pour réaliser la fiche de poste RSSI / DPO, l'établissement / le GHT pourra également s'appuyer sur les documents suivants :

- ANAP, référentiel de compétences SI, 2013
- CNIL, attendus du DPO en lien avec le RGPD, 2017
- CNIL, détails sur les fonctions et missions d'un DPO, 2017
- GHT 72, illustration d'une fiche de poste RSSI à l'échelle d'un GHT, 2017
- CLUSIF, définition des synergies entre RSSI et DPO, 2018
- CLUSIF, fiche méthode sur le rôle d'un DPO, 2018
- CNIL, règlement européen sur la protection des données
- CNIL, chapitre 4 du RGDP, Délégué à la protection des données

6. FICHE 7 — CHARTE D'ACCES AU SI

6.1. Contexte et périmètre

Contexte et objectifs

Le socle commun du **programme HOP'EN** est constitué de **4 prérequis** indispensables à une gestion sécurisée des soins dans un contexte de décloisonnement des prises en charge, dont la mise en place, par l'ensemble des établissements de santé est attendue d'ici la fin du programme :

- Identités, mouvements (P1) ;
- Sécurité (P2) ;
- Confidentialité (P3) ;
- Échanges et partages (P4).

Il comprend également **7 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.

- Les résultats d'imagerie, de biologie et d'anapath (D1) ;
- Le dossier patient informatisé et interopérable et le DMP (D2) ;
- La prescription électronique alimentant le plan de soins (D3) ;
- La programmation des ressources et l'agenda du patient (D4) ;
- Le pilotage médico-économique (D5) ;
- La communication et les échanges avec les partenaires (D6) ;
- La mise à disposition de services en ligne aux usagers et aux patients (D7).

La fiche a pour objectif d'aider les établissements de santé à amender leur Charte d'accès et d'usage du SI pour accompagner :

- Les évolutions **organisationnelles** des établissements de santé, qui résultent notamment de la mise en place des GHT — groupes d'établissements et de l'évolution des modes de travail : accessibilité des SI en mobilité, connexion au SI hospitalier depuis un appareil personnel, etc.
- Les évolutions **réglementaires** en matière de sécurité des données, et notamment à intégrer les impacts du règlement général de protection des données (RGPD) : le RGPD inverse la charge de la preuve par rapport à la loi Informatique et Liberté. Il appartient désormais à l'entité juridique de procéder elle-même à une appréciation des risques pour chaque traitement de données, de déterminer les risques acceptables et ceux qui ne le sont pas et de prendre les mesures de réduction du risque pour ramener ce dernier au niveau acceptable, si nécessaire.

Indicateur concerné

La fiche concourt principalement à l'obtention de :

- **L'indicateur P3.2 du prérequis confidentialité : existence d'un document lié au règlement intérieur formalisant des règles d'accès et d'usage du SI, en particulier pour les applications gérant des données de santé à caractère personnel, diffusé au personnel, aux nouveaux arrivants, prestataires et fournisseurs.**

L'élaboration d'une charte participe à la gestion des risques, à la sensibilisation et à l'information du personnel sur les règles appliquées au sein de la structure. Elle est obligatoire à partir du moment où l'entité collecte des données à caractère personnel.

6.2. Méthode proposée

Objectifs de la charte

La Charte a pour objectifs de :

- Décrire les règles d'accès et d'utilisation des ressources informatiques et des services internet d'un établissement de santé, notamment liées au dossier patient informatisé, par les professionnels habilités ;
- Préciser les processus d'acceptation et de diffusion de ces règles ;
- Rappeler aux utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information, conformément à la politique de sécurité des systèmes d'information définie par l'établissement de santé ;
- Responsabiliser les utilisateurs du système d'information dans leurs usages et face à certaines infractions ; Décrire les règles de fonctionnement du système d'information de l'établissement, d'un GHT ou d'un groupe d'établissements.

Lien avec le règlement intérieur

La Charte d'accès et d'usage du système d'information n'a pas de valeur juridique opposable en tant que telle. C'est pourquoi elle doit être annexée au règlement intérieur, ce qui lui confère la valeur d'acte réglementaire (Article L1321-5 du Code du travail).

De cette manière, la charte est opposable à l'ensemble des membres du personnel recrutés avant ou après son élaboration ainsi qu'aux prestataires et partenaires qui s'engagent à respecter le règlement intérieur de l'établissement.

Il convient alors de consulter les instances représentatives du personnel, lesquelles doivent donner leur avis sur la charte. Leur accord n'étant pas nécessaire à la validité du règlement intérieur et donc de la charte, cet avis ne lie pas l'employeur.

Déclaration légale de la charte

Pour les personnes morales de droit privé et les personnes morales de droit public qui disposent d'agents de droit privé, le règlement, ainsi que la charte, doivent être déposés au Greffe du Conseil des Prud'hommes et transmis à l'Inspection du travail en deux exemplaires pour être opposables (Art. R. 1321-2 et R. 1321-4 du Code du travail).

La charte ne deviendra exécutoire, pour l'ensemble des membres du personnel, qu'après l'accomplissement de ces formalités.

Ce mode opératoire est à renouveler à chaque modification de la charte.

Charte et GHT

L'établissement support devra s'assurer que chaque établissement partie du GHT a mis en place une charte ou un document formalisant les règles d'accès et d'usage du SI.

Il est souhaitable que ce document soit harmonisé au sein du GHT en produisant, par exemple, une charte de GHT dont les dispositions s'appliquent à tous, complétée par des chartes par établissement partie. L'harmonisation des organisations des structures (arborescence, formats, principes de mise à jour et diffusion) doit permettre de produire une version consolidée de la structure au niveau du GHT qui représente un référentiel essentiel à la production des indicateurs médico-économiques et aux processus transverses du GHT.

Diffusion de la charte

La charte doit être diffusée de manière individuelle à chacun des membres du personnel ainsi que de manière collective à l'ensemble des membres du personnel. Pour la diffusion individuelle, cette communication peut par exemple être réalisée via :

- Le bulletin de paye,
- Un courrier électronique,
- L'intranet de la structure avec un affichage automatique dans l'espace personnel du salarié pour s'assurer qu'il y accède au moins une fois.
- Pour la diffusion collective, la charte pourra, par exemple, être :
    - Affichée à un endroit accessible à tous dans les locaux de l'établissement,
    - Mise à disposition sur les pages collectives de l'intranet de l'établissement.

6.3. Les outils pour la mise en œuvre

Un modèle de charte d'accès au SI est proposé.

Pour aller plus loin, l'établissement de santé pourra se référer aux documents suivants :

- PGSSI, guide de gestion des habilitations, 2017
- PGSSI-S, politique générale de sécurité des systèmes d'information de santé, modèle de charte d'accès et d'usage du système d'information, 2017
- ANAP, avis d'expert : comment mettre en place un accès à distance pour les professionnels de santé, 2015
- HAS, guide thématique sur la gestion du système d'information, 2014

7. FICHE 8 — CARTOGRAPHIE APPLICATIVE

7.1. Contexte et périmètre

Contexte et objectifs

Le socle commun du **programme HOP'EN** est constitué de **4 prérequis** indispensables à une gestion sécurisée des soins dans un contexte de décloisonnement des prises en charge, dont la mise en place, par l'ensemble des établissements de santé est attendue d'ici la fin du programme :

- Identités, mouvements (P1) ;
- Sécurité (P2) ;
- Confidentialité (P3) ;
- Échanges et partages (P4).

Il comprend également **7 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.

- Les résultats d'imagerie, de biologie et d'anapath (D1) ;
- Le dossier patient informatisé et interopérable et le DMP (D2) ;
- La prescription électronique alimentant le plan de soins (D3) ;
- La programmation des ressources et l'agenda du patient (D4) ;
- Le pilotage médico-économique (D5) ;
- La communication et les échanges avec les partenaires (D6) ;
- La mise à disposition de services en ligne aux usagers et aux patients (D7).

La **présente fiche doit guider les établissements pour élaborer leur cartographie applicative**.

Le périmètre fonctionnel d'un SIH diffère en fonction de la maturité de l'établissement en termes de systèmes d'information. Cependant, il peut être cartographié sur la base de cinq grands domaines fonctionnels que sont la production de soins cliniques, la production de soins médico-techniques, le pilotage médico-économique, le support et l'infrastructure.

SI et GHT

Le système d'information constitue une fonction mutualisée obligatoire du GHT. La loi du 26 janvier 2016 de modernisation de notre système de santé prévoit dans son article 107 que l'établissement support désigné par la convention constitutive assure, pour le compte des établissements parties au groupement :

« La stratégie, l'optimisation et la gestion commune d'un système d'information hospitalier convergent, en particulier la mise en place d'un dossier patient permettant une prise en charge coordonnée des patients au sein des établissements parties au groupement. Les informations concernant une personne prise en charge par un établissement public de santé partie à un groupement peuvent être partagées, dans les conditions prévues à l'article L. 1110-4. »

En pratique, le SI cible se construit dans une logique de mutualisation des infrastructures et d'homogénéisation des outils voire d'unicité. Il appartient aux établissements de se définir une cible et une trajectoire adaptée. L'objectif est d'homogénéiser de façon progressive le SIH.

Pour ce faire, il est **indispensable de disposer d'une cartographie applicative à jour du SI**. Cette cartographie doit permettre :

- D'évaluer le niveau de couverture par rapport à une cible en matière de SI ;

- D'évaluer le niveau de redondance sur le périmètre applicatif et fonctionnel des applications disponibles ;
- D'objectiver la situation grâce à l'inclusion d'une analyse du niveau de déploiement – développement des usages sur les applicatifs, d'une évaluation de l'obsolescence et échéances contractuelles.

Indicateur concerné

La fiche concerne principalement les indicateurs ci-dessous :

- Indicateur P1.1 — Taux d'applications au cœur du processus de soins, de la gestion administrative du patient et du PMSI connectées à un référentiel unique d'identités des patients
- Indicateur P1.3 — Taux d'applications au cœur du processus de soins, de la gestion administrative du patient et du PMSI connectées à un référentiel unique de séjours et de mouvements des patients

7.2. Méthode proposée

Principes directeurs

L'élaboration d'une cartographie applicative repose sur les principes suivants :

- La **mobilisation d'un référent** en charge de l'élaboration de la cartographie applicative. Il est en charge de mobiliser les acteurs en charge de ces applications au sein de son établissement pour obtenir une description de la cartographie applicative ;
- La **capitalisation** issue des travaux menés dans le cadre de l'élaboration du schéma directeur des SI ;
- Une **méthodologie de réalisation de la cartographie** en se basant par exemple sur celle proposée dans le guide d'auditabilité du SI, destiné aux établissements publics ;
- Une **visualisation rapide de l'état des lieux applicatifs** grâce à un format de restitution adapté ;
- Une **progressivité dans la démarche** : description des applications, description de la couverture fonctionnelle des applications, identification des flux interapplications ;
- Du **pragmatisme** : se concentrer en priorité sur les applications qui constituent 80 % du périmètre applicatif.

Méthode proposée

La méthode proposée pour réaliser la cartographie applicative est la suivante :

Phase 1 — Cadrage et lancement du projet

- ❑ Identifier un chef de projet en charge de la réalisation de la cartographie applicative ;
- ❑ Identifier des référents en charge de la cartographie par le DSI, référents dont le chef de projets sera chargé d'animer les travaux ;
- ❑ Préparer et animer une réunion de lancement avec les référents en charge de l'élaboration de la cartographie. Cette réunion est l'occasion de partager les objectifs, la méthodologie et les modèles de documents à utiliser, le calendrier, la gouvernance projet.

Phase 2 — Réalisation de la cartographie applicative

- ❑ Revue de la documentation disponible issue des travaux réalisés dans le cadre de l'élaboration du Schéma Directeur des Systèmes d'Information ;

- ❑ Identifier les besoins de compléments à rechercher et des modalités de collecte de ses informations ;
- ❑ Analyse documentaire et conduite d'entretiens pour obtenir les informations nécessaires à la description de la cartographie applicative ;
- ❑ Alimenter le support décrivant la couverture applicative : liste des applications par domaine et sous-domaine, nom, éditeur, numéro de version, date d'acquisition et de mise en service, échéance du contrat, principales fonctionnalités et niveau d'usage
- ❑ Préparer les éléments de synthèse décrivant la couverture applicative ;
- ❑ Préparer et animer un temps d'échange avec le DSI et des acteurs clés connaissant les applicatifs de l'établissement pour partager le résultat des travaux et être en mesure de les finaliser sur la base des échanges qui ont eu lieu.

Phase 3 — Consolidation, mise en perspective et prospective

- ❑ Collecter par le chef de projet l'ensemble des travaux en vue de leur analyse et consolidation ;
- ❑ Présenter des résultats des travaux lors d'une réunion à laquelle participent le DSI et les référents qui ont réalisé la démarche

Profils à impliquer

- DSI
- Chef de projet en charge de la description de la cartographie applicative
- Référents en charge de la description de la cartographie applicative
- Profils disposant d'une solide connaissance des applicatifs : acteurs de la DSI et acteurs métiers le cas échéant.

Facteurs clés de succès

- Capitalisation sur les travaux réalisés dans le cadre du Schéma Directeur du Système d'Information (SDSI)
  - Analyse multicritères de la cartographie applicative
  - Couverture totale, partielle, pas de couverture ;
  - Nombre d'applications sur un même domaine et sous-domaine fonctionnel : analyse de la potentielle redondance ;
  - Niveau d'usages — de déploiement des solutions.
- Mise en perspective avec les échéances contractuelles (pas obligatoire dans le cadre de l'élaboration d'une cartographie applicative).
  - Support de collecte et de restitution des informations pragmatique et permettant une restitution des résultats sous un format visuel. L'enjeu est de donner du sens aux informations collectées dans une logique de facilitation de la prise de décision ultérieure ;
- Utilisation d'une méthode pérenne : le travail de description de la cartographie applicative est conséquent. L'enjeu est de disposer d'une base d'informations qu'il sera ensuite aisé de mettre à jour pour minimiser les efforts ultérieurs. Il s'agit de passer d'une approche ponctuelle de description des applications à une approche continue pour disposer d'une vision claire de la situation.

7.3. Les outils pour la mise en œuvre

Dans le cadre du projet de fiabilisation et certification des comptes des établissements publics de santé, la DGOS a publié un guide méthodologique à l'attention des établissements de santé leur permettant de se préparer au volet SI de la certification des comptes. Le guide méthodologique est

disponible via l'instruction n° DGOS/MSIOS/2013/62 du 21 février 2013 relative au guide méthodologique pour l'auditabilité des systèmes d'information dans le cadre de la certification des comptes des établissements publics de santé, accessible sur le site circulaire.legifrance.gouv.fr : http://circulaire.legifrance.gouv.fr/pdf/2013/02/cir_36543.pdf et publiée au BO Santé n° 2013/03 du 15 avril 2013.

Le guide méthodologique pour l'auditabilité des systèmes d'information a été élaboré dans l'objectif de constituer un guide pratique à destination des DSI leur permettant de définir :

- Les bonnes pratiques relatives au contrôle interne du système d'information,
- Les documents et éléments de preuve qui devront être produits et conservés par les établissements en vue de faciliter la certification (cartographie du SI, guide utilisateur des applications…),
- Les niveaux de contrôle minimum requis pour les établissements qui développent et maintiennent les applications de leur SIH,
- Les documents et éléments probants produits et conservés par les établissements (cartographie du SI, guide utilisateur des applications…).

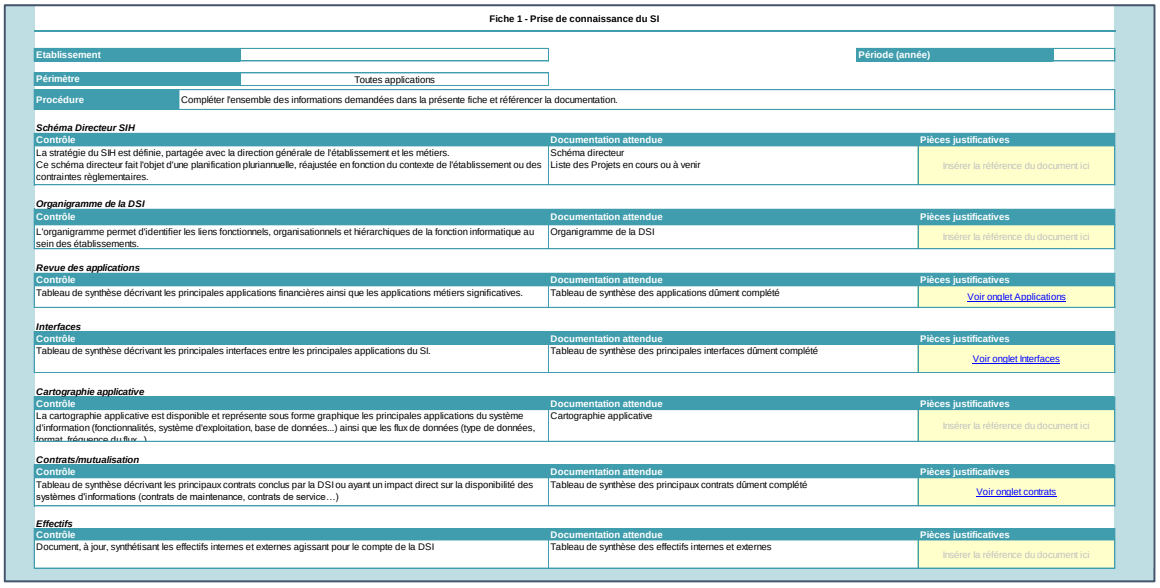
Le guide est composé de trois parties :

- Partie 1 : présentation de la démarche globale de certification des comptes, de l'impact des systèmes d'information sur la démarche et des étapes de la revue du SI ;
- Partie 2 : préparation des établissements à l'audit de leur SI ;
- Partie 3 : fiches pratiques de mise en œuvre.

Afin d'appuyer les DSI sur le volet SI de la certification des comptes, **un outil d'aide au format Excel** leur est proposé. Il sert d'appui au travail préparatoire à la certification en **permettant de décrire de manière exhaustive le SI d'un établissement, son fonctionnement et sa cartographie applicative,** tout en collectant l'ensemble de la documentation et des pièces justificatives nécessaires. Cet outil peut être utilisé par les établissements dans un cadre dépassant celui de la certification des comptes lorsqu'ils souhaitent réaliser — mettre à jour la cartographie applicative de leur SI.

Le fichier Excel est composé de 5 onglets :

- **Le 1er onglet « prise de connaissance » a vocation à présenter de manière synthétique le fonctionnement de la Direction des systèmes d'information et du système d'information lui-même :** pour chaque item, la DSI rassemble la documentation permettant de justifier du fonctionnement actuel et insère la référence des documents dans la colonne de droite de l'onglet.



Fiche 1 - Prise de connaissance du SI

Etablissement		Période (année)	
Périmètre	Toutes applications		
Procédure	Compléter l'ensemble des informations demandées dans la présente fiche et référencer la documentation.		

Schéma Directeur SIH

Contrôle	Documentation attendue	Pièces justificatives
La stratégie du SIH est définie, partagée avec la direction générale de l'établissement et les métiers. Ce schéma directeur fait l'objet d'une planification pluriannuelle, réajustée en fonction du contexte de l'établissement ou des contraintes règlementaires.	Schéma directeur Liste des Projets en cours ou à venir	Insérer la référence du document ici

Organigramme de la DSI

Contrôle	Documentation attendue	Pièces justificatives
L'organigramme permet d'identifier les liens fonctionnels, organisationnels et hiérarchiques de la fonction informatique au sein des établissements.	Organigramme de la DSI	Insérer la référence du document ici

Revue des applications

Contrôle	Documentation attendue	Pièces justificatives
Tableau de synthèse décrivant les principales applications financières ainsi que les applications métiers significatives.	Tableau de synthèse des applications dûment complété	Voir onglet Applications

Interfaces

Contrôle	Documentation attendue	Pièces justificatives
Tableau de synthèse décrivant les principales interfaces entre les principales applications du SI.	Tableau de synthèse des principales interfaces dûment complété	Voir onglet Interfaces

Cartographie applicative

Contrôle	Documentation attendue	Pièces justificatives
La cartographie applicative est disponible et représente sous forme graphique les principales applications du système d'information (fonctionnalités, système d'exploitation, base de données...) ainsi que les flux de données (type de données, format, fréquence du flux...)	Cartographie applicative	Insérer la référence du document ici

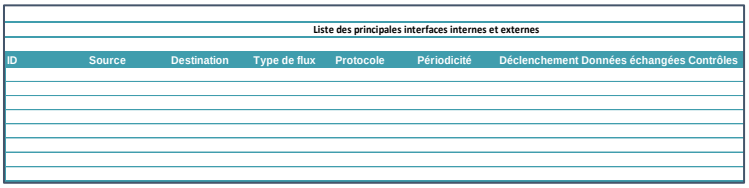
Contrats/mutualisation

Contrôle	Documentation attendue	Pièces justificatives
Tableau de synthèse décrivant les principaux contrats conclus par la DSI ou ayant un impact direct sur la disponibilité des systèmes d'informations (contrats de maintenance, contrats de service…)	Tableau de synthèse des principaux contrats dûment complété	Voir onglet contrats

Effectifs

Contrôle	Documentation attendue	Pièces justificatives
Document, à jour, synthétisant les effectifs internes et externes agissant pour le compte de la DSI	Tableau de synthèse des effectifs internes et externes	Insérer la référence du document ici

- **Le 2e onglet « applications » vise à préciser toutes les applications SI utilisées par l'établissement notamment sur le volet financier** ; il est attendu pour chaque application que la DSI détaille :
  - Nom de l'application
  - Interlocuteur MOA / MOE
  - Fonctionnalités
  - Hébergement
  - Type
  - Date de mise en place
  - Support éditeur
  - Prestataire pour la maintenance
  - Date de fin d'utilisation prévue
  - OS du serveur hébergeant l'application
  - Base de données
  - Projet d'évolution
  - Virtualisé
  - Criticité
- **Le 3e onglet « interfaces » permet de lister l'ensemble des applications internes et externes utilisées par l'établissement notamment sur le volet financier** ; il est attendu pour chaque interface que la DSI détaille les éléments suivants :
  - ID
  - Source
  - Destination
  - Type de flux
  - Protocole
  - Périodicité
  - Déclenchement
  - Données échangées
  - Contrôles



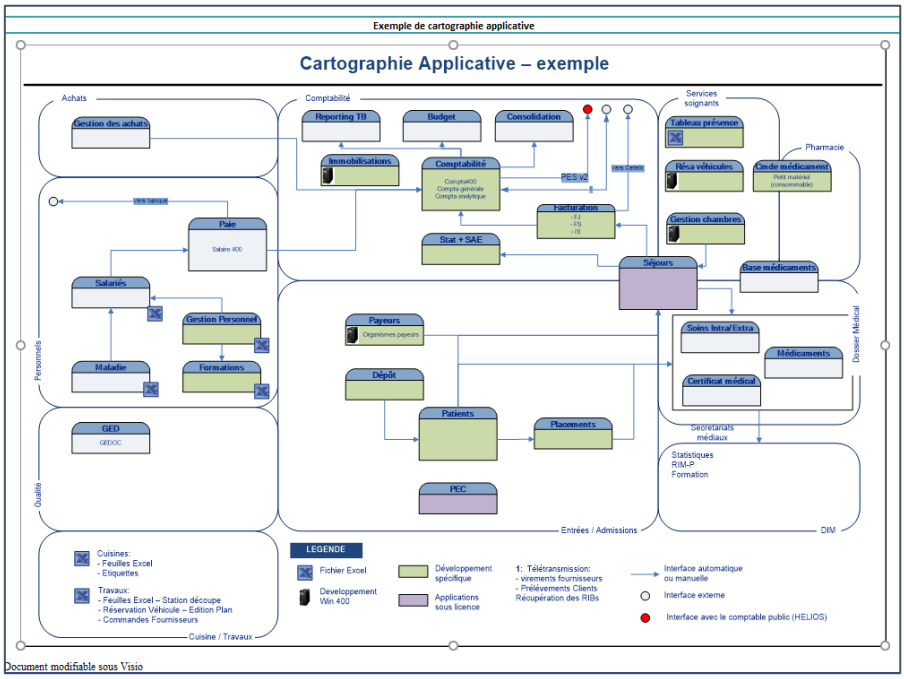
Liste des principales interfaces internes et externes

ID	Source	Destination	Type de flux	Protocole	Périodicité	Déclenchement	Données échangées	Contrôles

- **Le 4e onglet « contrats » permet de lister l'ensemble des contrats internes et externes passés par la DSI de l'établissement** ; les éléments suivants sont attendus pour chaque contrat :
  - Partenaire
  - Objet du contrat
  - Date d'engagement

- Date de fin d'engagement
- Indicateurs de niveau de service

- **Enfin le 5e onglet « cartographie applicative » vise à appuyer les établissements dans la représentation visuelle schématique de leurs applications SI.** Les DSI pourront s'inspirer de l'exemple de cartographie fourni dans l'outil Excel et l'adapter en fonction de la réalité de leurs systèmes d'information en utilisant l'outil Visio :



Pour réaliser sa cartographie applicative, le GHT/ groupe d'établissements pourra notamment s'appuyer sur les documents suivants :

- *DGOS, Guide méthodologique pour l'auditabilité des SI, 2013*
- *DGOS, Guide méthodologique Stratégie, optimisation et gestion commune d'un système d'information convergent d'un GHT, 2016*
- *ANAP, ID-si : outil d'Inventaire et de Décision pour le système d'information, 2016*

8. FICHE 9 — POLITIQUE DE SECURITE ET PLAN D'ACTION SSI

8.1. Contexte et périmètre

Contexte et objectifs

Le socle commun du **programme HOP'EN** est constitué de **4 prérequis** indispensables à une gestion sécurisée des soins dans un contexte de décloisonnement des prises en charge, dont la mise en place, par l'ensemble des établissements de santé est attendue d'ici la fin du programme :

- Identités, mouvements (P1) ;
- Sécurité (P2) ;
- Confidentialité (P3) ;
- Échanges et partages (P4).

Il comprend également **7 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.

- Les résultats d'imagerie, de biologie et d'anapath (D1) ;
- Le dossier patient informatisé et interopérable et le DMP (D2) ;
- La prescription électronique alimentant le plan de soins (D3) ;
- La programmation des ressources et l'agenda du patient (D4) ;
- Le pilotage médico-économique (D5) ;
- La communication et les échanges avec les partenaires (D6) ;
- La mise à disposition de services en ligne aux usagers et aux patients (D7).

Le système d'information vient soutenir la mise en œuvre de la stratégie de l'établissement et couvre un large périmètre englobant notamment l'administratif, le soin, le système d'information hospitalier, le biomédical et tout l'environnement nécessaire au bon fonctionnement de la structure (gestion des bâtiments, contrôle d'accès…) ainsi que les systèmes d'information administratifs.

Une augmentation des incidents de sécurité liés aux systèmes d'information est constatée à l'échelle nationale et internationale et le secteur hospitalier y est particulièrement vulnérable. Des atteintes à la disponibilité, l'intégrité et la confidentialité des informations sont observées et peuvent avoir des impacts sur la prise en charge des patients, l'organisation des services ainsi qu'en termes financiers et de notoriété, engageant parfois la responsabilité de la structure et/ou de son représentant.

Pour accompagner les établissements dans la mise en œuvre d'une politique de sécurité des systèmes d'information, les ministères sociaux ont proposé la mise en œuvre d'un plan d'action SSI dans l'INSTRUCTION N° SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information dans les établissements et services concernés.

La **présente fiche doit guider les établissements pour élaborer leur politique de sécurité et leur plan d'action SSI associé.**

Indicateur concerné

La fiche concerne principalement l'indicateur ci-dessous :

- Indicateur P2.4 - Présence d'une politique de sécurité et plan d'action SSI réalisé, existence d'un responsable sécurité

8.2. Méthode proposée

Objectifs de la politique et du plan d'action SSI

- **Une PSSI est un document porté par la direction de l'établissement et qui regroupe les objectifs stratégiques de la structure en termes de sécurité des systèmes d'information (SSI)** ainsi que les règles et mesures organisationnelles, fonctionnelles et techniques à mettre en œuvre pour y parvenir. Dans son guide d'élaboration de politique de SSI, l'ANSSI indique que :
  - *« Une Politique de Sécurité des Systèmes d'Information reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration...) en matière de sécurité des systèmes d'information (SSI) et de gestion de risques SSI. Elle décrit en effet les éléments stratégiques (enjeux, référentiels, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme. […] La PSSI vise à informer la maîtrise d'ouvrage et la maîtrise d'œuvre des enjeux tout en l'éclairant sur ses choix en termes de gestion des risques et à susciter la confiance des utilisateurs et partenaires envers le système d'information. ».*
- **Le plan d'action SSI vise à opérer une mise à niveau minimale de la sécurité des systèmes d'information dans tous les établissements de santé.** Le plan d'action ne se substitue pas aux obligations de sécurité que doivent mettre en place les établissements, mais il propose un calendrier à 6, 12 et 18 mois de réalisation de mesures prioritaires en termes d'efficacité par rapport, notamment, au risque de piratage informatique. Le niveau 1 de priorité permet de diminuer le risque de manière significative, avec des mesures dont la mise en œuvre ne doit pas poser de difficulté majeure, pour des gains importants en matière de sécurité.

Plan d'action SSI et GHT

Le système d'information constitue une fonction mutualisée obligatoire du GHT. La loi du 26 janvier 2016 de modernisation de notre système de santé prévoit dans son article 107 que l'établissement support désigné par la convention constitutive assure, pour le compte des établissements parties au groupement :

« La stratégie, l'optimisation et la gestion commune d'un système d'information hospitalier convergent, en particulier la mise en place d'un dossier patient permettant une prise en charge coordonnée des patients au sein des établissements parties au groupement. Les informations concernant une personne prise en charge par un établissement public de santé partie à un groupement peuvent être partagées, dans les conditions prévues à l'article L. 1110-4. »

Dans ce cadre, **la sécurité des systèmes d'information peut être assurée à l'échelle du GHT**. Ce sont les directeurs d'établissement qui ont la responsabilité et la charge de la sécurité de leur structure : ils s'appuient pour cela sur un RSSI et un DPO qui sont des maillons importants de la gestion des risques liés au SI. En sus, la chaîne SSI peut être consolidée par un réseau interne de correspondants SSI dans les différentes unités de la structure ou du groupement.

Dans un GHT, il est envisageable de mutualiser la fonction SSI et de mettre en place des correspondants SSI dans chacun des principaux établissements. Quelle que soit l'organisation retenue, il est important que toutes les responsabilités en matière de SSI des différents acteurs soient clairement définies par la direction de la structure / du groupement grâce à des fiches de poste et des ordres de mission.

Acteurs impliqués dans l'élaboration et la mise en œuvre de la PSSI

- La direction générale de l'établissement de santé
- Les directions métiers utilisant le SI
- Les directions supports (RH, juridique, services généraux…)
- Le RSSI et le DPO
- Les professionnels de l'établissement au sens large dans leur utilisation des SI
- Les prestataires ayant accès ou utilisant le SI de l'établissement

Qu'il s'agisse de l'élaboration de la politique de sécurité ou de celle du plan d'action SSI, il est conseillé de nommer au sein de l'établissement un coordonnateur des travaux, afin qu'ils puissent centraliser l'information.

Méthode proposée

La méthode proposée pour élaborer la PSSI d'un établissement de santé comprend 4 étapes :

- **Étape 1 — Cadrage du contexte d'application de la PSSI**
  - Validation du projet avec la direction de la structure
  - Définition de l'objet de la PSSI
  - Définition du champ d'application de la PSSI
  - Précision des enjeux de sécurité
  - Identification des textes applicables
- **Étape 2 – Recensement des différentes catégories de moyens du SI**
  - État des lieux des moyens technique et logistique relatifs au SI
  - État des lieux de l'organisation de la structure
- **Étape 3 – Qualification des principaux risques auxquels est exposé le SI**
  - Identification des principaux risques liés au SI
  - Définition de la stratégie de traitement des risques
- **Étape 4 — Choix des mesures de sécurité nécessaires**
  - Validation des exigences de sécurité applicables
  - Déclinaison des exigences de sécurité en règle

Les actions SSI et GHT

Les fiches actions rédigées par l'ASIP Santé ou encore le guide d'hygiène informatique publié par l'ANSI propose des thématiques à adresser pour améliorer la sécurité des SI. À l'échelle d'un GHT, l'enjeu est de pouvoir dans la situation actuelle avec les SI existants mettre en place une politique de sécurité SI adaptée et de définir une trajectoire dans la cadre de la stratégie de convergence des SI des GHT. Ainsi certaines actions proposées peuvent être mises en place dès à présent, d'autres le seront dans la durée (par exemple : Segmenter le réseau et mettre en place un cloisonnement entre les zones peut être difficile à réaliser sur des infrastructures existantes).

Une fois la PSSI élaborée et validée par la direction de l'établissement de santé, il convient de la mettre en application. Bien que toutes les règles de la PSSI soient applicables à l'établissement, elles ne sont pas toutes mises en œuvre simultanément et le plan d'action SSI vise à définir des règles de priorité et de cadencement de leur mise en place. La méthode retenue pour élaborer son plan d'action SSI repose sur 4 étapes également :

Étape 1 — Identification des personnes en charge de la mise en application de chaque règle de sécurité

Il s'agit d'identifier le / les responsables techniques qui seront en charge de la mise en œuvre de la règle de sécurité.

Étape 2 — Estimation de l'effort nécessaire à la mise en œuvre de chaque règle

Il s'agit de communiquer les règles de sécurité à l'ensemble des contacts identifiés à l'étape précédente pour qu'ils puissent :

- Prendre connaissance des règles qui concernent leur périmètre de responsabilité,
- Déterminer dans quelle mesure chaque règle est déjà mise en œuvre,
- Déterminer l'effort nécessaire, en charge de travail et en coût pour la mise en œuvre de chaque règle sur l'ensemble du périmètre cible qui les concerne,
- Retourner ces informations au coordonnateur de l'élaboration du plan d'action SSI.

Étape 3 — Définition des objectifs, échelonnés dans le temps, de déploiement des règles

Chaque établissement ou groupement d'établissements définit les règles de priorité qui lui sont propres en fonction de ses orientations stratégiques, de l'état des lieux de ses risques en matière SI et également des moyens disponibles et de l'effort nécessaire à la mise en œuvre de chaque règle.

Étape 4 — Validation par la direction de la PSSI et du plan d'action associé et mobilisation des moyens nécessaires à la mise en œuvre planifiée

La validation de la PSSI et du plan d'action SSI par la direction de l'établissement est essentielle à sa diffusion et à sa mise en œuvre au sein de l'établissement. Dans un second temps, les deux documents doivent faire l'objet d'une communication pédagogique plus large auprès des collaborateurs.

Bilan et mise à jour du plan d'action SSI

Il est recommandé de procéder à une revue ponctuelle des actions du plan d'action SSI avec les différents responsables afin d'identifier :

- De dresser un état des lieux de l'avancement du plan ;
- D'identifier les résultats et les difficultés rencontrées.

Le suivi régulier du plan d'action doit également permettre d'anticiper les ajustements du plan d'action qui peuvent notamment être liés à :

- L'évolution des activités de la structure,
- L'élargissement du périmètre auquel s'applique la PSSI,
- L'évolution de la règlementation,
- L'émergence de nouvelles menaces spécifiques ou non aux secteurs sanitaire et médico-social,
- La survenue d'incidents révélant de nouveaux risques,
- Des retours d'expérience sur la mise en œuvre des règles de sécurité, etc.

La méthode et les travaux à réaliser à chaque étape sont précisés dans le « guide d'élaboration et de mise en œuvre d'une PSSI » de la PGSSI-S référencé dans le chapitre « Pour aller plus loin ».

8.3. Les outils pour la mise en œuvre

Pour réaliser sa politique et son plan d'action SSI, l'établissement / le GHT pourra notamment s'appuyer sur les documents suivants :

- PGSSI-S, Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social, 2015
- ASIP Santé, fiches réflexes, 2017 :
  - Réargir face à un défacement
  - Patch management
  - Code malveillant
  - Réagir à un déni de service
  - Vol équipement
  - Se protéger des attaques par hameçonnage
- Guide d'hygiène informatique, ANSI -2017 — https://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/
- Outils de sensibilisation à la cybersécurité – GCS e-santé Pays de la Loire : https://www.esante-paysdelaloire.fr/fr/outils_sensibilisation_securite

9. FICHE 10 — CONFORMITE EN MATIERE DE PROTECTION DES DONNEES PERSONNELLES

9.1. Contexte et périmètre

Contexte et objectifs

Le socle commun du programme HOP'EN est constitué de 4 prérequis indispensables à une gestion sécurisée des soins dans un contexte de décloisonnement des prises en charge, dont la mise en place, par l'ensemble des établissements de santé est attendue d'ici la fin du programme :

- Identités, mouvements (P1) ;
- Sécurité (P2) ;
- Confidentialité (P3) ;
- Échanges et partages (P4).

Il comprend également 7 domaines fonctionnels pour lesquels le programme définit des exigences en matière d'usage du système d'information.

- Les résultats d'imagerie, de biologie et d'anapath (D1) ;
- Le dossier patient informatisé et interopérable et le DMP (D2) ;
- La prescription électronique alimentant le plan de soins (D3) ;
- La programmation des ressources et l'agenda du patient (D4) ;
- Le pilotage médico-économique (D5) ;
- La communication et les échanges avec les partenaires (D6) ;
- La mise à disposition de services en ligne aux usagers et aux patients (D7).

Le présent document a pour objectif d'offrir une vision synthétique sur les points d'attention et la démarche à mettre en œuvre dans le cadre de la mise en conformité des établissements de santé aux obligations réglementaires relatives à la protection des données. Il s'adresse aux acteurs au sein des établissements de santé et des GHT en charge de la mise œuvre des procédures de protection des données personnelles :

- Délégué à la protection des données (DPO) ;
- Responsable et référents sécurité des systèmes d'information (RSSI / rSSI) ;
- Directeur en charge de la qualité et ingénieur qualité ;
- Directeur en charge des relations patients ;
- Directeur des affaires juridiques ;
- Médecin DIM.

Indicateur concerné

La fiche concourt principalement à l'obtention de :

- **L'indicateur P3.2 portant sur l'existence d'un document lié au règlement intérieur formalisant les règles d'accès et d'usage du SI, en particulier pour les applications gérant des données de santé à caractère personnel, diffusé au personnel, aux nouveaux arrivants, prestataires et fournisseurs**
- **L'indicateur P3.6 portant sur l'existence d'une fonction DPO et présence d'un registre des traitements de DCP qualifié avec droits d'accès**

9.2. Présentation

Enjeux

Dans le cadre de ses activités, un établissement de santé est amené à collecter et manipuler des Données personnelles. L'objectif de cette fiche pratique est de fournir aux établissements de santé, un document explicatif des différents points auxquels chacun doit se conformer dès lors qu'il traite des Données personnelles, conformément au RGPD.

Quelles sont les règles à respecter ?

Dès lors qu'il utilise des Données personnelles dans le cadre de ses activités, un établissement de santé doit être attentif au respect des règles prévues par la règlementation en matière de protection des Données personnelles et notamment le Règlement (UE) 2016/679[4] (ci-après le « Règlement Général sur la Protection des Données » ou « RGPD ») et la Loi Informatique et Libertés[5] qui comprend un important volet relatif à la protection des données de santé. Le RGPD contient de nombreuses règles avec lesquelles il est nécessaire de se conformer en cas de Traitement de Données personnelles.

- Par exemple, lorsque l'établissement de santé collecte via un formulaire d'admission des informations sur les patients comme leur nom, leur adresse, leur Numéro d'Inscription au Répertoire National d'identification des personnes physiques (NIR), etc. => il s'agit d'une collecte de Données personnelles.
- Parmi ces règles, il est notamment important de s'assurer que les Données personnelles sont collectées pour un objectif déterminé, que seules les Données personnelles pertinentes et nécessaires sont collectées et qu'elles ne sont pas réutilisées par la suite pour un objectif incompatible avec l'objectif initial (ex : lorsque des Données personnelles sont communiquées à des tiers tels que des compagnies d'assurance, sans le consentement de la personne concernée), que les individus dont l'établissement de santé traite les Données personnelles sont correctement informés de la collecte et de l'utilisation qui va être faite de leurs Données personnelles et qu'ils sont mis en mesure d'exercer leurs droits (ex. droit d'accéder à leurs Données personnelles). Les Données personnelles ne doivent pas être conservées de manière indéfinie et des mesures doivent être mises en place pour assurer leur sécurité. En raison de leur caractère sensible, les Données de Santé[6] bénéficient d'un régime plus protecteur notamment en termes de sécurité.

---

[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des Données personnelles et à la libre circulation de ces données.

[5] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[6] Désignent les Données personnelles relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne. Cette définition permet d'englober certaines données de mesure à partir desquelles il est possible de déduire une information sur l'état de santé de la personne. Pour la CNIL, ces données comprennent :

- « ***Les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services*** *: un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ;*

- ***Les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle****, y compris à partir des données génétiques et d'échantillons biologiques ;*

Quels sont les outils à disposition des établissements de santé pour respecter les règles ?

Cette fiche pratique explique les règles à respecter et la manière dont une revue de conformité doit être réalisée avant la mise en place d'un nouveau Traitement (cf. notamment la section « A quelles règles se conformer en cas de Traitement ?)

Quels sont les acteurs de la conformité ?

- Chaque membre du personnel d'un établissement de santé est potentiellement acteur de la conformité en matière de protection des Données personnelles et doit connaître les règles contenues dans cette fiche pratique.
- Plus particulièrement, les personnes en charge des opérations de Traitement de Données personnelles au sein d'un établissement de santé (ci-après « Personne en Charge ») sont tenues de s'assurer du respect des règles applicables avec l'assistance du Délégué à la Protection des Données le cas échéant, et de documenter la revue de conformité à réaliser pour tout Traitement.
- Le Délégué à la Protection des Données (ci-après « DPO ») est là pour conseiller et assister les employés et en particulier les Personnes en Charge afin de s'assurer du respect des règles[7].

9.3. Comment réaliser une revue de conformité ?

La conformité avec les règles de protection des Données personnelles doit être garantie en ce qui concerne les opérations de Traitement de Données personnelles nouvelles et existantes.

Nouvelles opérations de traitement de données personnelles

Identification des opérations de Traitement de Données personnelles

Dans le cadre des nouveaux projets, il est nécessaire d'identifier l'existence d'un Traitement de Données personnelles qui est caractérisé par les 3 éléments suivants :

- **Des Données personnelles** : toute information se rapportant à une personne physique identifiée ou identifiable (ex : nom, prénom, NIR, pathologie, soins, prescription) ;
- **Un Traitement** : le Traitement peut être automatisé ou non (ex. : base de données électronique, bulletin en format papier) ;
- **Une finalité déterminée** : l'objectif pour lequel le Traitement est réalisé. Afin d'effectuer une revue de conformité, il est important d'identifier pour quelle finalité le Traitement de Données personnelles est réalisé (ex : diagnostic et administration de soins, recrutement du personnel).

Qualification d'un établissement de santé

Pour toute opération de Traitement, l'établissement de santé doit identifier s'il agit en tant que Responsable du Traitement, Responsable conjoint du Traitement ou Sous-traitant.

- ***Les informations concernant 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 santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro)* ».

[7] La désignation d'un DPO est obligatoire dans certains cas et par exemple quand le responsable du Traitement est un organisme public ou en cas de Traitement à grande échelle de données de santé (article 37 du RGPD).

Une revue de conformité complète doit être effectuée uniquement lorsqu'un établissement de santé agit en tant que Responsable du Traitement ou Responsable conjoint du Traitement[8].

Lorsqu'un établissement de santé agit en tant que sous-traitant, la Personne en Charge ne doit pas effectuer une analyse complète de la conformité, mais se limiter à une revue de conformité recouvrant uniquement les exigences applicables aux Sous-traitants.

Focus : en pratique, comment déterminer le rôle des parties prenantes ?

Un établissement de santé doit être considéré comme **responsable du Traitement** lorsqu'il détermine les Finalités (l'utilisation cible des Données personnelles) et les moyens de l'opération de Traitement (ex : choix des outils IT de traitement et de leur utilisation, choix des modalités de Traitement en termes de durée de conservation ou de mesures de sécurité).

Si les Finalités et moyens de l'opération de Traitement sont déterminés conjointement par un ou plusieurs organismes, ils doivent être chacun considérés comme **Responsable conjoint du Traitement**.

Contexte GHT

Un établissement de santé doit être considéré comme **Sous-traitant** lorsqu'il met en œuvre un Traitement de données pour le compte d'un autre organisme (ex. dans le cadre de la convergence SI des GHT). Un établissement de santé peut également bénéficier des services d'un Sous-traitant (ex : prestataire IT réalisant des opérations de maintenance et/ou d'hébergement lié à un logiciel médico-administratif[9]).

Vérification des points de conformité

Lorsqu'un établissement de santé agit en tant que **Responsable du Traitement** (ou Responsable conjoint en charge de la revue de conformité), il doit vérifier que le Traitement est conforme avec les règles de protection des Données personnelles.

Lorsqu'un établissement de santé agit en tant que **sous-traitant**, la Personne en charge doit principalement vérifier les points suivants :

- Des mesures techniques et organisationnelles appropriées sont mises en place (voir ci-après) ;
- Un accord contenant des clauses appropriées à la protection des Données personnelles, est conclu avec le Responsable du Traitement et les mesures nécessaires sont mises en place pour être conforme aux dites clauses (voir ci-après) ;
- Le Responsable du Traitement est informé si un Transfert des Données personnelles vers un Pays tiers est envisagé (voir section ci-après) ;

[8] En cas de responsabilité conjointe, les Responsables conjoints doivent déterminer de manière transparente, leurs responsabilités respectives an matière de protection des Données personnelles, y compris celui en charge de la revue de conformité. Le Responsable conjoint qui n'est pas en charge de cette revue doit néanmoins documenter le fait que la revue a été effectuée par l'autre Responsable conjoint.

[9] Attention, si un établissement de santé veut confier l'hébergement de Données de Santé à un prestataire tiers, celui-ci doit être hébergeur agréé ou certifié (article L. 1111-8 du Code de la santé publique).

- Un registre des activités de Traitement est établi pour ces activités de Traitement (voir ci-après).

Élaboration d'un plan d'action et réalisation des actions nécessaires

Une fois la conformité du Traitement vérifiée, l'établissement de santé doit, sur la base des points de non-conformité identifiés, établir un plan d'actions[10] comprenant toutes les actions correctrices devant être mises en œuvre pour garantir la conformité aux règles de protection des Données personnelles.

Il sera possible de mettre en œuvre l'opération de Traitement uniquement lorsque les actions correctrices auront été mises en œuvre. Dans le cas contraire, les opérations concernées devront être suspendues.

Nécessité de demander une assistance pour la revue de conformité

Différents acteurs de la conformité au sein d'un établissement de santé peuvent intervenir selon le schéma de gouvernance choisi :

- **La Personne en charge** (ex. : médecins, infirmiers, personnel de l'accueil de l'établissement de santé) ;
- **Le Délégué à la protection des Données** ;
- Un **représentant des équipes IT** en charge de fournir une assistance sur les aspects IT ;
- Un **représentant des équipes RH** en charge de fournir une assistance sur les aspects RH (si nécessaire) ;
- Toute autre partie prenante pertinente.

Nécessité de documentation

Conformément au principe de Responsabilité (Accountability) prévu par le RGPD, il est nécessaire d'être en mesure de prouver la conformité aux règles de protection des Données personnelles. Il est par conséquent très important pour la Personne en charge de documenter l'analyse, le plan d'action et la mise en œuvre des actions.

Revue régulière

Une fois le Traitement mis en œuvre, ses conditions de mise en œuvre doivent être régulièrement vérifiées (par exemple une fois par an) afin de constater un éventuel changement qui nécessitera le cas échéant une modification des mesures de conformité.

Opérations de Traitement existantes

Les opérations de Traitement existantes c'est-à-dire les opérations en place avant le 25 mai 2018[11] doivent aussi respecter les règles de protection des Données personnelles. Par conséquent, les étapes mentionnées ci-dessus pour garantir la conformité avec le RGPD doivent également être mises en œuvre.

Afin d'identifier toutes les opérations de Traitement existantes, il est recommandé d'utiliser le registre des activités de Traitement[12] qui doit être tenu par chaque établissement de santé, concernant toutes les activités de Traitement effectuées sous leur responsabilité.

---

[10] Le plan d'action doit préciser : (i) les actions devant être mises en œuvre pour garantir la conformité (ii) la (es) Personne(s) en charge de chaque action et (iii) si possible, un délai maximum pour mettre en œuvre les actions.

[11] Date d'entrée en application du RGPD.

[12] Article 30 du RGPD.

9.4. À quelles règles se conformer en cas de Traitement ?

En cas de Traitement, de nombreuses règles doivent être respectées : les règles concernant le Traitement, les catégories de Données personnelles traitées, les droits des Personnes concernées, le consentement des Personnes concernées, la sécurité et la conservation des Données personnelles, les relations avec les tiers et les formalités.

Traitement de Données personnelles

Licéité, loyauté et transparence du Traitement

Les Données personnelles doivent être traitées **de manière licite, loyale et transparente** au regard des Personnes concernées[13] : il est nécessaire de garantir que les Données personnelles n'ont pas été collectées et traitées suite à des actions frauduleuses, déloyales ou illicites, sans information préalable des Personnes concernées (voir également ci-après sur les droits des Personnes concernées).

De plus, il est nécessaire de vérifier si l'opération de Traitement correspond à **un des fondements suivants**, en prenant en compte la finalité poursuivie[14] :

- Le Traitement est nécessaire **à l'exécution du contrat** auquel la Personne concernée est partie (ex. : contrat de travail).
- Le Traitement est nécessaire au respect d'une **obligation légale** ;
- Le Traitement est nécessaire aux fins des **intérêts légitimes** poursuivis par l'établissement de santé ou par un tiers (gestion des candidatures) ;
- La Personne concernée a **consenti** au Traitement[15].

Limitation de la finalité

Les Données personnelles ne peuvent être traitées que pour des **finalités déterminées, explicites et légitimes et ni être ultérieurement traitées d'une manière incompatible avec ces finalités**[16].

Le principe garantit que les Données personnelles ne seront pas collectées « juste au cas où », mais que ces Données personnelles seront collectées et traitées uniquement pour des finalités déterminées, desquelles les Personnes concernées ont été informées préalablement au Traitement (voir ci-après sur les droits des Personnes concernées).

Les Données personnelles **ne peuvent être traitées pour une autre finalité** autre que celle pour laquelle les Données personnelles ont été collectées uniquement **dans le cas où**[17] :

- Le **consentement préalable** des Personnes concernées a été obtenu ; ou
- Le Traitement ultérieur est fondé sur l'existence d'une **disposition légale** ; ou
- cette nouvelle finalité de Traitement est **présumée compatible avec la finalité initiale** de collecte et de Traitement des Données personnelles.

[13] Article 5.1.a) du RGPD.
[14] Article 6 du RGPD.
[15] NB : le consentement **ne peut pas être utilisé** comme motif au Traitement **s'il y a un lien de subordination** (ex. le consentement d'un employé n'est pas considéré comme librement délivré).
[16] Article 5.1.b) du RGPD.
[17] Article 6.4 du RGPD.

Focus : comment la Personne en charge peut-elle évaluer la compatibilité de ces nouvelles finalités avec les finalités initiales ?

Pour cela peuvent être pris en compte les éléments suivants :

- Tout lien entre la finalité initiale du Traitement et la finalité ultérieure envisagée ;
- Le contexte dans lequel les Données ont été collectées et les attentes raisonnables des Personnes concernées sur l'utilisation ultérieure des Données ;
- La nature de la Donnée personnelle[18] ;
- Des conséquences du Traitement ultérieur sur les Personnes concernées ; et
- les garanties appropriées[19] mises en place.

Données personnelles

Minimisation et exactitude des Données personnelles

Il est nécessaire de garantir que seules les Données personnelles **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités poursuivies, sont collectées et traitées[20]. Des procédures adéquates doivent donc être mises en œuvre pour que les Données personnelles demeurent **exactes et tenues à jour**[21].

Les Catégories particulières de Données et autres Données sensibles

Des Catégories particulières de Données et d'autres Données sensibles sont considérées comme des Données personnelles dont le Traitement présente un risque plus important pour les individus.

✓ **Catégories particulières de Données personnelles**

Les Catégories particulières de Données sont (i) des données révélant **l'origine raciale** ou **ethnique** d'un individu (ii) ses **opinions politiques** (iii) ses **convictions religieuses** ou **philosophiques**, ou son **appartenance syndicale** (iv) ses **données génétiques** (v) ses **données biométriques** (lorsqu'elles sont utilisées aux fins d'identifier une personne physique de manière unique) (vi) les données **concernant sa santé** et (vii) les données **concernant sa vie sexuelle ou son orientation sexuelle**[22].

Le Traitement de ces Données est interdit par principe, sauf circonstances particulières[23]. La Personne en charge doit vérifier si le Traitement de ces Données respecte l'une de ces exceptions :

1. La Personne concernée a donné son **consentement explicite** ;
2. Le Traitement est **nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres** au Responsable du Traitement en matière de droit du travail et de la protection sociale ;

[18] Il convient de prendre en compte en particulier si des Catégories particulières de Données personnelles ou des Données personnelles concernant les condamnations pénales et les infractions sont traitées.
[19] C'est-à-dire des mesures de sécurité techniques et organisationnelles.
[20] Article 5.1.c) du RGPD.
[21] Article 5.1.d) du RGPD.
[22] Article 9.1 du RGPD.
[23] Article 9.2 du RGPD. Le RGPD énumère une liste limitative de circonstances dans lesquelles ces Données personnelles peuvent être traitées.

3. Le Traitement est nécessaire à la sa**uvegarde des intérêts vitaux de la Personne concernée ou d'une autre personne physique** dans le cas où la Personne concernée se trouve dans une incapacité physique ou juridique de donner son consentement ;
4. Le Traitement porte sur des Données personnelles qui sont **manifestement rendues publiques** par la Personne concernée ;
5. Le Traitement est nécessaire à la **constatation, l'exercice ou la défense d'un droit en justice** ;
6. Le Traitement est nécessaire pour des **motifs d'intérêt public important**s ;
7. Le Traitement est nécessaire aux fins **d'appréciation de la capacité de travail de l'employé** ;
8. Le Traitement est nécessaire à des **fins archivistiques dans l'intérêt public**, à des **fins de recherche scientifique ou historique ou à des fins statistiques** (conformément à l'article 89 du RGPD).

Focus concernant les Données de santé à caractère personnelles

La Loi Informatique et Libertés prévoit également parmi les exceptions à l'interdiction, les **traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du Code pénal**.

Autres Données sensibles

Il s'agit des **Données relatives aux condamnations pénales et aux infractions ainsi que le numéro d'identification national** (ex. le numéro de sécurité sociale en France)[24].

Le Traitement de Données relatives aux **condamnations pénales et aux infractions** ou des **mesures de sûreté** ne peut être effectué que sous le contrôle de l'autorité publique ou si le Traitement est autorisé par le droit applicable.

Les droits des personnes concernées

Information des personnes concernées

Le responsable du traitement doit fournir à toutes les personnes concernées (ex. : un patient) **une mention d'information** décrivant le traitement. Cette information doit être **concise, aisément accessible** et rédigée en des **termes clairs et simples**.

Cette mention doit contenir **les informations suivantes** et être fournie avant le traitement, sauf lorsque la Personne concernée a déjà l'information[25] :

- **L'identité et les coordonnées du responsable du traitement** (l'établissement de santé) ;
- Les **coordonnées du délégué à la protection des données, le cas échéant** ;
- Les F**inalités** du traitement ainsi que la base juridique du traitement ;
- Les **intérêts légitimes poursuivis** par le responsable du traitement (lorsque le traitement est basé sur ce fondement) ;
- Les **destinataires** ou les catégories de Destinataires des Données personnelles ;
- Les éventuels **Transferts de Données personnelles** réalisés vers un Pays tiers ou à une organisation internationale et l'existence d'une décision d'adéquation ou la mise en œuvre de garanties appropriées ;

[24] Articles 10 et 87 du RGPD.
[25] Article 13 du RGPD.

- La **durée de conservation** des Données personnelles (ou le critère utilisé pour déterminer cette durée) ;
- L'existence du **droit d'accès ou de rectification ou d'effacement des Données personnelles ou de limitation du Traitement, ou d'opposition au Traitement, de même que le droit à la portabilité** des Données lorsqu'il est applicable ;
- Lorsque le Traitement se fonde sur le consentement de la Personne concernée, **l'existence du droit de retirer le consentement à tout moment** ;
- Le **droit d'introduire une réclamation auprès de l'Autorité de Contrôle (la CNIL en France)** ;
- Lorsque le Traitement se fonde sur une **exigence réglementaire ou contractuelle** (ou sur une exigence conditionnant la conclusion du contrat) et si la communication des Données personnelles est obligatoire ainsi que sur les conséquences de la non-fourniture des Données ;
- L'existence d'une **prise de décision automatisée** (y compris un profilage)[26].

La **liste d'informations à inclure dans la mention est légèrement différente** lorsque les Données personnelles n'ont **pas été directement obtenues** auprès des Personnes concernées (par ex. catégories de Données personnelles collectées et sources des Données personnelles)[27]. De plus, dans ce cas, l'information doit être fournie au moment de l'enregistrement des Données personnelles ou si la communication à un tiers est envisagée, au plus tard au moment de cette communication. Elle peut par exemple être faite par la remise d'une mention ou par voie d'affichage dans les locaux de l'établissement de santé.

Par ailleurs, l'obligation d'informer les Personnes concernées ne s'applique pas lorsque (i) la fourniture de telles informations se révèle impossible ou (ii) exigerait des efforts disproportionnés ou (iii) l'enregistrement ou la communication de ces données est expressément prévue par la loi.

Autres droits des Personnes concernées

- **<u>Droits applicables à toutes les opérations de Traitement</u>**
  Le responsable du Traitement doit garantir la possibilité pour les Personnes concernées d'exercer les droits suivants[28] :
  - Le **droit d'accès** à ses Données personnelles et les informations concernant l'opération de Traitement ;
  - Le **droit de rectification** de Données personnelles inexactes le/la concernant ;
  - Le **droit d'effacement** sous conditions particulières ;
  - Le **droit de limitation**, sous conditions particulières (c'est-à-dire, le droit de demander que les données soient conservées, mais pas traitées) ;
  - Le **droit de s'opposer** au Traitement de ses Données personnelles pour des raisons tenant à sa situation particulière ;
  - Le **droit à la portabilité** de ses Données personnelles vers lui/elle ou vers un autre Responsable de Traitement si (i) le Traitement est fondé sur un consentement ou est nécessaire à l'exécution d'un contrat, et (iii) le Traitement est effectué à l'aide de procédés automatisés.

La Personne concernée doit être informée de l'existence de ces droits et se voir fournir des moyens adéquats à l'exercice de ces droits (c'est-à-dire les coordonnées valables d'une personne responsable

[26] Dans ce cas, il convient également d'informer sur la logique sous-jacente ainsi que l'importance et les conséquences prévues d'une telle décision.
[27] Article 14 du RGPD.
[28] Pour plus d'informations sur les droits des Personnes concernées, veuillez consulter les articles 16 à 23 du RGPD.

afin de lui envoyer facilement et librement une demande, par exemple les coordonnées du Délégué à la Protection des Données).

- **Droit de ne pas faire l'objet d'une décision individuelle automatisée.**

Les Personnes concernées ont le droit de ne pas faire l'objet de décisions fondées uniquement sur un Traitement automatisé (y compris le profilage) produisant des **effets juridiques** concernant la Personne concernée ou **l'affectant de manière significative de façon similaire**.

Par conséquent, **le Responsable du Traitement doit garantir qu'aucune décision** produisant de tes effets ne soit prise que sur la base d'un Traitement automatisé, **sauf si la décision est**[29] :

- Nécessaire à la conclusion ou l'exécution d'un contrat entre l'établissement de santé agissant comme Responsable du Traitement et la Personne concernée ; ou
- Autorisée par le droit applicable ; ou
- Fondée sur le consentement explicite de la Personne concernée.

Le consentement des personnes concernées

Lorsque le consentement des Personnes concernées doit être collecté (ex. comme fondement de licéité du Traitement pour le Traitement de Catégories particulières de Données personnelles), celui-ci doit respecter les conditions suivantes[30] :

- Le consentement doit être une **manifestation de volonté univoque** par laquelle la Personne concernée accepte par une déclaration ou par un acte positif clair ;
- Le consentement doit être **librement donné**, **spécifique et éclairé** :
  - Les **informations nécessaires** doivent être communiquées aux Personnes concernées avant qu'elles consentent ;
  - Le consentement doit être **spécifique à un enjeu** (ex. une finalité du Traitement) et doit être distinct de tout autre sujet ;
  - Le consentement ne peut pas être utilisé en cas de relation de subordination (ex. le consentement d'un employé n'est pas considéré comme librement donné) ;
- Les Personnes concernées doivent **pouvoir retirer leur consentement à tout moment**.

Sécurité et conservation des données personnelles

Mesures de sécurité techniques et organisationnelles

Le responsable du Traitement doit s'assurer que des mesures techniques et organisationnelles appropriées sont mises en place pour garantir un niveau de sécurité adapté au risque en lien avec les Traitements (pseudonymisation, chiffrement, des tests de sécurité, etc.)[31].

En particulier, l'accès aux Données personnelles doit être limité aux seuls Destinataires qui en ont besoin dans le cadre de la réalisation de leurs activités. Il convient donc de s'en assurer (ex. gestion des accès sur la base de profils d'habilitation, des moyens d'authentification, etc.).

---

[29] Lorsque la décision est nécessaire au contrat ou fondée sur le consentement, la Personne en charge doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour la sauvegarde des droits et libertés de la Personne concernée.

[30] Articles 4 (11) et 7 du RGPD.

[31] Article 32 du RGPD. Ces mesures doivent être définies en prenant en compte l'état des connaissances, les coûts de mise en œuvre, la nature, la portée, le contexte et les finalités du Traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, que présente le Traitement pour les droits et libertés des Personnes concernées.

Le cas échéant, l'équipe informatique de l'établissement de santé doit pouvoir être impliquée sur ces questions[32].

Limitation de conservation des Données

Les Données personnelles **ne doivent pas être conservées pendant une durée, excédant celle nécessaire à la finalité pour laquelle les Données sont traitées**. Il est par conséquent nécessaire de **définir et mettre en œuvre** une durée de conservation adéquate, prenant en compte la finalité du Traitement poursuivi et les obligations légales applicables[33]. Par exemple, le dossier médical d'un patient est conservé pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein[34].

Les relations avec les tiers

Relations avec les sous-traitants

Lorsque le Traitement est réalisé par un Sous-traitant pour le compte d'un établissement de santé agissant comme Responsable du Traitement (ex. un prestataire de service fournissant une assistance IT ou un prestataire de paye), l'établissement de santé doit s'assurer que ce Sous-traitant **présente des garanties suffisantes** quant à la mise en œuvre de mesures techniques et organisationnelles appropriées avant de conclure un contrat avec celui-ci. De plus, il doit veiller à ce qu'**un contrat contenant les clauses adéquates relatives à la protection des données soit conclu avec le Sous-traitant**[35].

Relations avec le responsable conjoint du traitement

Lorsque la finalité et les moyens du Traitement sont définis conjointement par plusieurs organismes, ils sont considérés comme des **Responsables conjoints**. Ils doivent alors définir et répartir de manière transparente (au sein d'un contrat) leurs responsabilités de conformité aux règles de protection des données (ex. via un accord de Responsabilité conjointe).

Transfert de données personnelles vers un pays tiers

La Personne en charge doit garantir que les Transferts de Données vers des Pays tiers, c'est-à-dire des pays situés en dehors de l'Espace économique européen[36] sont sécurisés (ex. garanties adéquates comme la conclusion des clauses contractuelles types de la Commission européenne)[37].

9.5. Formalités

Registre des activités de Traitement

Le responsable du Traitement doit tenir un **registre des Traitements** réalisés sous sa responsabilité[38]. Ce registre doit être centralisé par le Délégué à la Protection des Données et être mis à jour à chaque fois que les conditions de Traitement sont modifiées.

---

[32] Un document relatif à la sécurité des données est mis en ligne par la CNIL à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

[33] C'est-à-dire une obligation légale de conserver les informations ou une limitation légale de la durée pour des procédures judiciaires/prescription.

[34] Article R. 1112-7 du Code de la Santé Publique.

[35] Article 28 du RGPD.

[36] États membres de l'UE, la Norvège, l'Islande et le Liechtenstein.

[37] Article 44 à 49 du RGPD.

[38] Article 30 du RGPD.

Afin d'établir les fiches registres par finalité de Traitement, il est nécessaire de procéder par étape :

Étape 1 : Identification des Personnes en charge des Traitements

Les principales Personnes en charge des Traitements peuvent être par exemple le Directeur des Ressources humaines (ou les membres de son équipe) pour les finalités RH et les finalités de gestion du recrutement, le Directeur financier (ou les membres de son équipe) pour la finalité de gestion de la comptabilité et du paiement des frais. De plus, la Personne en charge du Traitement dans le département IT (c'est-à-dire le Directeur de Systèmes d'information (ou les membres de son équipe) doit également être identifiée et contactée afin de :

- Identifier les Traitements mis en œuvre pour des finalités de gestion de l'IT (par exemple, gestion de l'accès aux outils informatiques, gestion de la sécurité informatique y incluant la journalisation des accès, le chiffrement, etc.) et établir les fiches registre des Traitements concernés ;
- Compléter les sections dédiées aux mesures de sécurité de toutes les autres fiches registre.

Étape 2 : Préidentifier les Finalités de Traitement mises en œuvre

Afin de déterminer les fiches registre, il est nécessaire d'identifier :

- les Finalités des activités de Traitement mises en œuvre par l'établissement de santé concerné en tant que responsable du Traitement (ex. la gestion de recrutement, la gestion de la formation, la gestion des diagnostics et l'administration de soins) ;
- les catégories de Traitement mises en œuvre par l'établissement de santé en tant que sous-traitant, éventuellement pour le compte d'un autre établissement de santé (ex. hébergement des données ou autres Finalités dans le cadre de groupements d'établissements de santé).

Tâche #3 : Collecter les informations nécessaires et compléter le registre

Les informations pertinentes requises pour compléter le registre des Traitements (par exemple les Données personnelles traitées, les Destinataires, les Transferts, etc.) doivent être collectées auprès de différentes personnes.

En cas de situation de coresponsabilité, il est recommandé de nommer un des Responsables conjoints, responsable de l'établissement des fiches registres concernées pour son propre compte ou pour le compte de ses Responsables conjoints. Le responsable désigné de l'établissement des fiches registre devra envoyer les fiches registre des Traitements aux autres Responsables conjoints du Traitement.

Chaque fiche registre doit comprendre les rubriques suivantes :

- Le nom du Responsable du Traitement et, le cas échéant, le nom et les coordonnées du Responsable conjoint du Traitement mis en œuvre ;
- Les Finalités du Traitement, l'objectif en vue duquel l'établissement de santé a collecté ces Données personnelles ;
- Les catégories de Personnes concernées (ex. : patient, employé de l'établissement) ;
- Les catégories de Données personnelles (ex. : identité, situation familiale, données bancaires, données de santé) ;
- Les catégories de Destinataires auxquels les Données personnelles ont été ou seront communiquées, y compris les Sous-traitants auxquels recourt l'établissement de santé ;
- Les Transferts de données à caractère personnel vers un Pays tiers ou à une organisation internationale et, dans certains cas très particuliers, les garanties prévues pour ces Transferts ;
- Les délais prévus pour l'effacement des différentes catégories de Données personnelles, c'est-à-dire la durée de conservation, ou à défaut les critères permettant de la déterminer ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles que met en œuvre l'établissement de santé.

La CNIL a mis à disposition un exemple de registre sur son site internet[39].

Le registre devra être mis à jour à chaque modification dans les conditions de Traitement.

Formalités auprès de la CNIL

La Personne en charge doit s'assurer que les formalités adéquates sont réalisées. La loi Informatique et Liberté maintient l'obligation d'effectuer des formalités auprès de la CNIL en cas de Traitement de Données de Santé, soit un engagement de conformité à une méthodologie de référence, soit une demande d'autorisation auprès de la CNIL[40].

L'analyse d'impact relative à la protection des données (AIPD)

La réalisation d'une AIPD est nécessaire en cas de Traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des Personnes concernées[41]. Par conséquent, le Responsable du Traitement doit vérifier si l'AIPD doit être effectuée, sur la base d'une liste de critères publiée par le Groupe de Travail « Article 29 »[42]. La CNIL a publié une liste d'opérations de Traitement pour lesquelles une AIPD est requise[43]. **Par exemple, les Traitements de Données de Santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes requièrent une AIPD.**

Lorsqu'une AIPD est nécessaire, le responsable du Traitement doit réaliser cette AIPD.

Le site de la CNIL a mis à disposition un outil d'AIPD sur son site internet[44].

[39] https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf
[40] Article 54 de la loi Informatique et liberté.
[41] Article 35 du RGPD.
[42] G29, WP 248 rev.01, Lignes directrices sur l'AIPD, adoptées le 4 Avril 2017 et révisées le 4 Octobre 2017.
[43] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf
[44] https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

9.7. Glossaire

Termes	Définition
Autorité de Contrôle	Désigne une autorité publique indépendante qui est en charge de : (i) surveiller les Traitements de Données personnelles au sein de sa juridiction (pays, région ou organisation internationale) (ii), conseiller les organes compétents conformément aux mesures légales et réglementaires concernant le Traitement de Données personnelles, et (iii) traiter les réclamations introduites par les Personnes concernées conformément à la protection de leurs droits à la protection des données[45]. En France, l'Autorité de Contrôle est la CNIL.
Catégories particulières de Données personnelles	Désigne les Données personnelles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le Traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique[46].
Données personnelles	Désigne toute information se rapportant à une personne physique identifiée ou identifiable (« Personne concernée »)[47].
Données sensibles	Désigne toute Donnée personnelle relative aux condamnations pénales et aux infractions de la Personne concernée, ainsi que le numéro d'identification national[48].
Destinataires	Désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de Données personnelles, qu'il s'agisse ou non d'un tiers[49].
EEE ou Espace économique européen	Désigne les pays de l'Union européenne et les pays membres de l'AELE (Association européenne de libre-échange).
Finalité	Désigne le but/l'objectif du Traitement (par exemple, la gestion du personnel, la gestion de la paye, la gestion de la formation, etc.).
L'Analyse d'Impact relative à la Protection des Données	Désigne un processus conçu pour décrire le traitement, évaluer son caractère nécessaire et proportionnel, aider à gérer les risques pour les droits et libertés des personnes physiques résultant du traitement de Données personnelles, en les évaluant et en déterminant les mesures à prendre[50].
Traitement	Désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de Données personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction[51].
Transfert	Désigne tout transfert de Données personnelles. Un transfert peut être réalisé par toute voie de communication, copie, transfert ou transmission de Données personnelles via un réseau, y compris l'accès à distance vers une base de données ou le transfert d'un moyen vers un autre, quel que soit le type de moyen (par exemple d'un disque dur vers un serveur).

[45] Article (4) 21 du RGPD.
[46] Article 9 du RGPD.
[47] Article 4 (1) du RGPD.
[48] Article 10 du RGPD.
[49] Article 4 (9) du RGPD.
[50] Lignes directrices concernant l'Analyse d'Impact relative à la Protection des Données (IAPD) et déterminant si le traitement est « susceptible d'engendrer un risqué élevé » aux fins du Règlement 2016/679 dans sa dernière version révisée et adoptée le 4 octobre 2017.
[51] Article 4 (2) du RGPD.

10. FICHE 11 — PEUPLEMENT DU REPERTOIRE OPERATIONNEL DES RESSOURCES (ROR)

10.1. Contexte et périmètre

Contexte et objectifs

Le socle commun du **programme HOP'EN** est constitué de **4 prérequis** indispensables à une gestion sécurisée des soins dans un contexte de décloisonnement des prises en charge, dont la mise en place, par l'ensemble des établissements de santé est attendue d'ici la fin du programme :

- Identités, mouvements (P1) ;
- Sécurité (P2) ;
- Confidentialité (P3) ;
- Échanges et partages (P4).

Il comprend également **7 domaines fonctionnels** pour lesquels le programme définit des exigences en matière d'usage du système d'information.

- Les résultats d'imagerie, de biologie et d'anapath (D1) ;
- Le dossier patient informatisé et interopérable et le DMP (D2) ;
- La prescription électronique alimentant le plan de soins (D3) ;
- La programmation des ressources et l'agenda du patient (D4) ;
- Le pilotage médico-économique (D5) ;
- La communication et les échanges avec les partenaires (D6) ;
- La mise à disposition de services en ligne aux usagers et aux patients (D7).

Le **répertoire opérationnel des ressources (ROR) est le référentiel de données qui décrit l'offre de santé sur l'ensemble des champs sanitaires et médico-sociaux.** Il a pour finalité de centraliser la description de l'offre de santé des établissements sanitaires, des professionnels de santé libéraux et des établissements et services en charge des personnes âgées en perte d'autonomie et des personnes en situation de handicap. C'est un **outil destiné à aider les professionnels à connaître l'offre de santé disponible afin d'améliorer le parcours du patient.**

Dans le cadre de la Stratégie nationale de Santé et de l'instruction DGOS/PF5/2015 du 7 avril 2015, la DGOS a réaffirmé sa volonté de « déploiement effectif du dispositif ROR sur l'ensemble du territoire national, avec la perspective que toutes les régions soient dotées d'un ROR ».

Pour cela, les établissements de santé sont mobilisés pour décrire leur activité et leurs ressources de manière précise afin de contribuer au remplissage de l'outil ROR : on parle communément de « peuplement du ROR ». Au niveau régional, la démarche de peuplement du ROR est pilotée par l'ARS en lien avec des correspondants ROR dans chaque établissement de santé.

La **présente fiche doit guider les établissements dans leur démarche de description de leurs activités et ressources et de peuplement du ROR.**

Présentation du ROR

Le ROR est un outil régional interopérable avec les solutions ROR des autres régions

Chaque région dispose d'une solution ROR régionale : l'ARS est chargée de piloter le peuplement du ROR à l'échelle de son territoire. Les solutions ROR régionales sont néanmoins **interopérables avec les solutions ROR des autres régions.** Un utilisateur peut ainsi rechercher une offre de santé dans une autre région à partir de son ROR régional.

Le ROR doit fournir une **description exhaustive des ressources de l'offre de santé régionale et extrarégionale** sur les champs du sanitaire, du médico-social et à terme du social. L'offre de ville et l'offre hospitalière sont décrites dans un même outil. Le ROR est le **socle de base de tous les usages et projets régionaux** nécessitant la connaissance de l'offre sanitaire, médico-sociale et à terme sociale.

À quoi sert le ROR ?

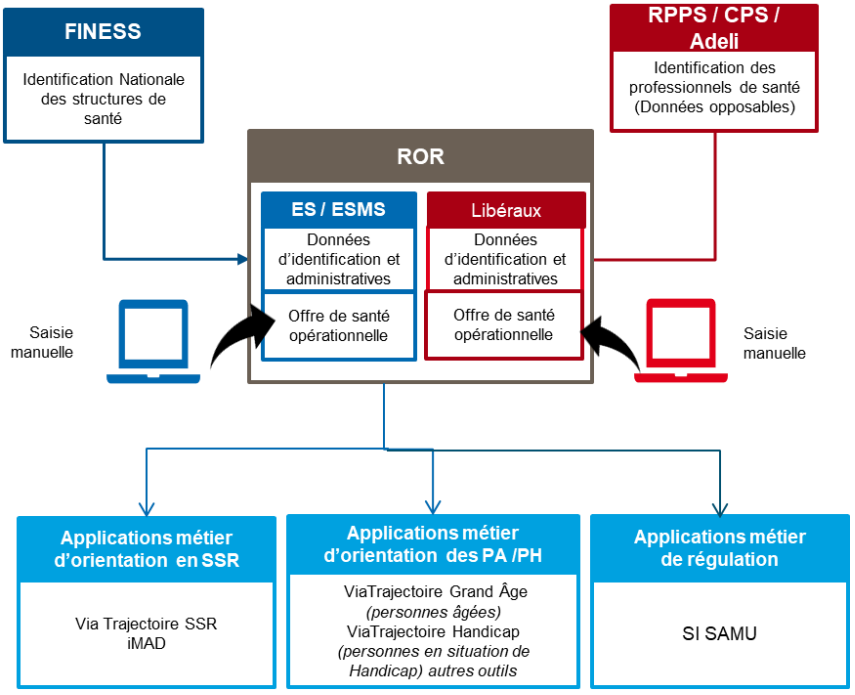
Le répertoire ROR permet de faciliter l'orientation d'un patient dans le cadre de son parcours de soins. En effectuant une recherche dans le ROR, les acteurs de santé peuvent trouver :

- Un correspondant pour donner un avis spécialisé pour établir ou confirmer un diagnostic
- Une équipe pouvant porter un acte diagnostic ou thérapeutique pour le patient
- Une localisation de prise en charge du patient
- Un moyen opérationnel (ex. : IRM)

Le ROR est un outil composé d'un répertoire et de services métiers

Au sein des solutions ROR déployées dans les régions, on distingue :

- **Un répertoire descriptif de l'offre de santé opérationnelle régionale** qui s'alimente :
  - Des référentiels nationaux tels que FINESS (raison sociale, n° FINESS, n° SIREN, statut juridique, catégorie d'établissement, date de création, adresse) et RPPS (identifiant du professionnel, profession, spécialités, savoir-faire, adresse et contact tél./email) ;
  - Des données fournies par les professionnels / établissements de santé et saisies manuellement dans l'outil ROR (description des activités, spécialités, matériel disponible, etc.)
- **Des services métiers nés des besoins régionaux** (ex. : gestions des disponibilités des lits, gestion de la permanence des soins, etc.).
  D'autres outils opérationnels régionaux qui ont besoin de connaître l'offre de santé se sont interfacés avec le répertoire ROR.



Schématisation du fonctionnement du répertoire ROR régional

Le ROR : une définition commune de l'offre de santé

Dans le cadre du programme ROR, les acteurs de santé ont convergé sur une vision commune de l'offre de santé qui est définie selon 4 composants :

- Des **structures** ou organisations qui emploient des professionnels et possèdent des équipements pour réaliser des activités,
- Des **activités** ou prestations délivrées par une structure du sanitaire (activité de soins) ou du médico-social dans le cadre du parcours de santé d'un patient,
- Des **professionnels** exerçant ces activités,
- Des **équipements** techniques utilisés pour réaliser ces activités.

État des lieux du ROR en 2019

- À fin 2018, le peuplement de l'offre MCO à l'échelle nationale est réalisé
- À fin 2018, le peuplement de l'offre PSY / SSR est encore en cours, en voie de finalisation à l'échelle nationale
- Le peuplement de l'offre médico-sociale est un des objectifs de la feuille de route 2019

Indicateur concerné

La fiche concerne principalement l'indicateur ci-dessous :

- Indicateur P4.2 — Peuplement du ROR (champs sanitaires : MCO [dont HAD et USLDD], SSR, PSY)

10.2. Méthode proposée

Principe de la méthode

La description de l'offre de santé s'inscrit dans un cycle itératif avec des campagnes de peuplement successives :

- D'une part, car la démarche de peuplement peut être longue et mobiliser de nombreux professionnels au sein de l'établissement : **il peut être choisi de procéder au peuplement progressif par périmètre** (par services ou autres unités organisationnelles) pour échelonner la charge de travail ;
- D'autre part **l'offre de santé est évolutive** (arrivée/départ de nouveaux professionnels, évolution des nomenclatures dans l'outil ROR, etc.) ce qui nécessite l'actualisation fréquente de l'outil ROR.

Chaque campagne est définie en fonction des objectifs régionaux et des jalons fixés dans le cadre du programme national ROR.

Acteurs impliqués dans le peuplement du ROR

Le peuplement du ROR et la mise à jour des données nécessitent de mettre en place dans l'établissement une organisation spécifique reposant notamment sur les profils suivants :

- **La direction de l'établissement de santé et/ou ses représentants,** qui valident le peuplement, remontent les alertes et difficultés rencontrées et donnent un état d'avancement du peuplement à l'ARS
- **Un correspondant ROR** au sein de l'établissement : il est le point d'entrée unique pour l'équipe projet ROR à l'échelle de l'ARS ; il s'agit le plus souvent d'un profil administratif.

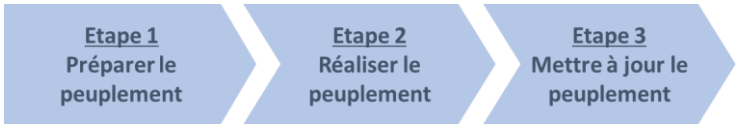
- **Des référents ROR** au sein de l'établissement :
  - **Des référents administratifs :** il s'agit de profils ayant une bonne vision générale de l'organisation interne de l'établissement et des différentes activités de chaque unité fonctionnelle, souvent responsable financier ou contrôleur de gestion
  - **Des référents métiers :** il est conseillé de nommer des cadres de santé comme référents métiers et de démultiplier ces référents pour limiter le nombre de données à saisir pour chacun des référents
- Tout autre acteur en établissement pouvant contribuer au peuplement : président de CME, responsable qualité, etc.

Méthode proposée

L'ARS pilote la mise en œuvre et le peuplement du ROR. Elle accompagne, relayée par les GRADeS en région, les établissements dans leur projet de peuplement grâce à :

- **La formation des référents administratifs** avec un atelier pratique qui permet de familiariser à la saisie de l'organisation de l'établissement dans l'outil ROR ;
- **La formation des référents métiers** avec un atelier pratique qui permet de familiariser à la saisie des données descriptives de l'offre de soins de chaque unité organisationnelle de l'établissement ;
- **L'accompagnement des établissements** par l'équipe régionale ROR (suivi du peuplement, collecte des demandes d'évolution des nomenclatures de description de l'offre de santé, etc.).

La méthode proposée pour contribuer au peuplement du ROR au sein d'un établissement de santé comprend 3 étapes :



Étape 1 — Préparer la campagne de peuplement du ROR

Cette étape consiste à préparer le peuplement du ROR au sein de l'établissement et notamment :

1. Prendre contact avec l'équipe projet ROR de l'ARS / du GCS-GRADeS pour lancer le projet
2. Identifier une équipe projet et des contributeurs au sein de l'établissement
3. Partager les objectifs / enjeux du projet au sein de l'établissement
4. Définir la gouvernance et le pilotage du projet au sein de l'établissement

Prendre contact avec l'équipe projet régionale ARS / GRADeS

- ❑ Informer l'ARS / le GRADeS du lancement d'une campagne de peuplement ROR au sein de l'établissement
- ❑ Se conformer aux objectifs et à la stratégie de peuplement de l'ARS : chaque ARS définit sa propre stratégie en déclinaison des orientations nationales
- ❑ Obtenir des identifiants de connexion sur l'outil ROR pour l'établissement : le GRADeS est chargé de créer un compte par établissement sur l'outil ROR régional et de transmettre ses identifiants de connexion à l'établissement
- ❑ Disposer de la documentation éventuellement mise à disposition sur le peuplement du ROR par l'ARS / les GRADeS

Identifier l'équipe projet au sein de l'établissement

- ❑ Désigner un correspondant ROR, point d'entrée unique de l'équipe projet ARS au sein de l'établissement et préciser ses rôles / responsabilités :
    - Il s'agit habituellement d'un profil administratif et non médical pour le mobiliser plus facilement sur la gestion du projet, l'animation de réunions et les interactions avec la Direction / l'ARS
    - Le correspondant est identifié par le Directeur de l'établissement
- ❑ Identifier le référent administratif (profils responsables financiers ou contrôleur de gestion) et les référents métiers (profils cadres de santé) et préciser leurs rôles / responsabilités :
    - Les référents sont identifiés par le correspondant
    - Le référent administratif est souvent un profil responsable financier ou contrôleur de gestion qui dispose d'une bonne vision de l'organisation interne de l'établissement de santé
    - Les référents métiers sont des profils soignants (cadres de santé) qui connaissent l'activité opérationnelle des services et peuvent la décrire finement
    - Il est recommandé d'identifier le plus de référents métiers possible pour limiter le nombre de données à saisir par chacun des référents

Partager les objectifs / enjeux du projet au sein de l'établissement

- ❑ Organiser une réunion de lancement au sein de l'établissement pour partager les enjeux et les attentes vis-à-vis du projet pour mobiliser et fédérere les professionnels de l'établissement autour du projet
    - Exemples d'enjeux / attentes : améliorer l'attractivité de l'établissement, valoriser au sein de l'établissement la diversité des activités, améliorer le parcours patient, etc.
- ❑ Diffuser si nécessaire en complément une communication sur le lancement du projet auprès du personnel de l'établissement pour informer du lancement du projet et de ses enjeux

Définir la gouvernance et le pilotage du projet au sein de l'établissement

- ❑ Mettre en place un point de suivi opérationnel selon une temporalité adaptée pour faire le point sur l'état d'avancement du peuplement et être en capacité de transmettre l'information au chef de projet ARS tous les trimestres
    - Le suivi peut s'appuyer sur un outil de suivi simple sur le modèle de celui présenté au chapitre 3
- ❑ Identifier le niveau de reporting souhaité au niveau de la Direction de l'établissement et les instances de direction dans lesquelles partager ce reporting sur
    - L'état d'avancement du peuplement
    - Les alertes et difficultés rencontrées

Étape 2 — Réaliser le peuplement (ab initio puis en continu en fonction de l'élargissement du périmètre du ROR et de la mise à jour des informations)

Cette étape consiste à :

1. Décrire l'organisation interne de l'établissement qui porte les activités opérationnelles sur un lieu au sein d'une entité géographique : le référent administratif décrit l'organisation, l'ensemble des pôles de l'établissement, puis dans chaque pôle les services et, enfin, chaque unité opérationnelle au sein des services
2. Décrire les activités opérationnelles / compétences / ressources par unité de l'organisation interne décrite : les référents métiers précisent les activités de soins et les équipements

spécifiques pour chaque unité (liste des spécialités, des professionnels de la spécialité, des équipements spécifiques disponibles…)

3. Saisir les données dans le répertoire ROR : après avoir précisé les activités opérationnelles avec les référents métiers, le référent administratif est chargé de saisir les données dans l'outil ROR ; certaines données pourront avoir été intégrées automatiquement dans l'outil grâce aux répertoires FINESS et RPPS
4. Faire valider les informations saisies par les professionnels de santé adéquats (il peut s'agir des chefs de services ou d'autres profils selon l'organisation de l'établissement) : ils s'assurent que l'information saisie reflète bien l'offre de soin proposée dans les services / unités opérationnelles de l'établissement
5. Faire valider les saisies du ROR par la Direction de l'établissement : avant la mise en en ligne définitive des saisies dans l'outil ROR, l'équipe projet ROR de l'établissement en fait valider le contenu et la diffusion par la Direction ou ses représentants

Descrire l'organisation interne de l'établissement

- ❑ Décrire l'organisation administrative et médicale de l'établissement de santé. Le référent administratif détaille l'arborescence de l'établissement :
  - Entité juridique
  - Entités géographiques
  - Pôles / services (facultatif)
  - Unités fonctionnelles (facultatif)
- ❑ Pour réaliser l'arborescence, le référent administratif s'appuie sur des documents sources comme l'organigramme de l'établissement et le fichier commun de structure
- ❑ La majeure partie des données sur l'entité juridique et l'établissement pourront avoir été intégrées automatiquement dans l'outil ROR grâce aux répertoires FINESS (raison sociale, n° FINESS, n° SIREN, statut juridique, catégorie d'établissement, date de création, adresse) et RPPS (identifiant du professionnel, profession, spécialités, savoir-faire, adresse et contact tél./email)
- ❑ Faire valider la description de l'arborescence de l'établissement par la Direction de l'établissement

Créer des unités élémentaires

- ❑ Une fois la structure de l'établissement définie, les référents doivent s'accorder sur la création des unités élémentaires qui serviront de base à la description de l'offre opérationnelle.
- ❑ L'unité élémentaire (UE) est la plus petite partie de l'organisation interne de l'établissement qui délivre une ou plusieurs activités opérationnelles dans le cadre d'un mode de prise en charge unique.
  - L'identification des UE peut se faire via des entretiens avec les cadres de services et les médecins référents par spécialités animés par les référents métier pour identifier avec précision l'activité opérationnelle de chaque unité décrite dans l'organisation. Le champ d'activité
  - Une adresse
  - Un contact
- ❑ En sus, des équipements / actes et compétences spécifiques peuvent être ajoutés.

Descrire l'offre de soins au sein des unités élémentaires

- ❑ Les informations à recueillir par unité élémentaire sont a minima les suivantes :
  - Au moins une activité

- Au moins un mode de prise en charge
- La classe d'âge
- Le champ d'activité
- Une adresse
- Un contact

❑ D'autres informations peuvent être ajoutées en sus, notamment des équipements, des actes spécifiques et compétences.

Valider les saisies du ROR

❑ Après avoir complété l'outil ROR, le référent administratif, en lien avec les référents métiers, fait valider les saisies de l'offre de soins auprès des médecins référents dans les services et réajuste les informations.

❑ Enfin, le référent administratif fait valider la saisie globale à la Direction de l'établissement avant la mise en ligne définitive des données

Étape 3 — Mettre à jour le peuplement

Pour garantir la fiabilité des données du ROR sur le long terme, il convient de définir une organisation pour améliorer en continu la qualité et la complétude des données du ROR. En effet l'offre de soins de l'établissement peut évoluer rapidement (arrivée/départ de professionnels, réorganisation de services, acquisition de nouveaux équipements, etc.).

Il s'agit de :

1. Formaliser un processus de mise à jour du ROR : identification des acteurs responsables de la mise à jour, de la temporalité des mises à jour, etc.
2. Suivre l'application de ce processus de mise à jour : le référent administratif peut être chargé de s'assurer auprès des référents métiers que l'évolution de l'offre de soins a été intégrée dans l'outil ROR

Définir un processus et suivi de l'alimentation continue du ROR

❑ Définir un processus interne à l'établissement pour ajuster et compléter au fil de l'eau le peuplement du ROR (acteurs, rôles et responsabilités, temporalité, etc.)
- L'actualisation du peuplement est notamment liée à l'évolution des nomenclatures du ROR et à leur diffusion tous les trimestres par l'ASIP Santé

❑ Identifier un responsable du suivi de l'actualisation continue du ROR et suivre l'actualisation afin de pouvoir :
- Réaliser un reporting aux instances et à l'équipe projet ARS
- Prendre des mesures correctives si nécessaire

Exemple d'outil de suivi du peuplement en établissement

Nom et coordonnées de l'établissement									
Préparation du peuplement				**Peuplement**				**Validation**	Délai entre le lancement de la campagne et la validation du peuplement
Date de lancement de la campagne en établissement	Formation des référents en établissement	Date de formation des référents administratifs	Date de formation des référents métiers	Alimentation de l'organisation de l'établissement	Pourcentage réalisé	Alimentation des unités fonctionnelles	Pourcentage réalisé	Date de validation par l'ARS des données saisies	

10.3. Les outils pour la mise en œuvre

Pour réaliser le peuplement du ROR, l'établissement / le GHT pourra également s'appuyer sur les documents suivants :

- Asip Santé, Le ROR au service des parcours usagers, mai 2018
- Asip Santé, Alimentation et mise à jour d'une application à partir du ROR, septembre 2018
- Asip Santé, Déploiement des ROR au 30/09/2018, septembre 2018