https://ressources.anap.fr/numerique/publication/2397-atteindre-les-prerequis-hop-en

Atteindre les prérequis HOP'EN

Sommaire

5. Rôles de RSSI et DPO

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.

© ANAP
Ces contenus extraits du centre de ressources de l'ANAP sont diffusés gratuitement.
Toutefois, leur utilisation ou citation est soumise à l'inscription de la mention suivante : "© ANAP"

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 ;

© ANAP
Ces contenus extraits du centre de ressources de l'ANAP sont diffusés gratuitement.
Toutefois, leur utilisation ou citation est soumise à l'inscription de la mention suivante : "© ANAP"

- 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.

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 - Compétences du DPO-DPD
- 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

© ANAP
Ces contenus extraits du centre de ressources de l'ANAP sont diffusés gratuitement.
Toutefois, leur utilisation ou citation est soumise à l'inscription de la mention suivante : "© ANAP"

Ressources associées

KIT DE PRODUCTIONS
Boîte à outils pour l'atteinte des prérequis du programme HOP'EN

MÉTHODE
Plan d'action P3.6 : Existence d'une fonction DPO et présence d'un registre de traitement de DCP
↳ Plan d'action pour l'atteinte des prérequis HOP'EN

MODÈLE DE DOCUMENT
Élaborer une fiche de poste pour un RSSI

MODÈLE DE DOCUMENT
Elaborer une fiche de poste pour un DPO

MÉTHODE
Plan d'action P2.4 : Politique et plan d'action de sécurité du SI - Responsable sécurité
↳ Plan d'action pour l'atteinte des prérequis HOP'EN

Glossaire

ASIP
DCP
DMP
dossier patient
DPD
GHT
imagerie
Indicateur
loi
SI
personne
pilotage
RGPD
SDSI

Télécharger la production

© ANAP
Ces contenus extraits du centre de ressources de l'ANAP sont diffusés gratuitement.
Toutefois, leur utilisation ou citation est soumise à l'inscription de la mention suivante : "© ANAP"