Mars 2023

GUIDE

Guide autodiagnostic « Gestion SI OG »

→ Glossaire, définitions des termes et illustrations dans le but d'aider au renseignement de l'autodiagnostic ANAP

RÉDACTRICES :

Laurie WAGNON
Chargée de mission transformation numérique Nord et Pas-de-Calais
Collectif SI Social et Médico-Social HDF

Cécile HELLEU
Chargée de mission transformation numérique Aisne, Somme, Oise
Collectif SI Social et Médico-Social HDF

RELECTEUR :

Adrien PETIT
DSI de La Vie Active
Expert au Collectif SI Social et Médico-Social HDF

Collectif SI Médico-Social Hauts-de-France

Avec le soutien de

Financement dans le cadre de la réponse de l'Union à la pandémie de COVID-19

SOMMAIRE

SOMMAIRE

INTRODUCTION

Selon l'Appel A Projet ESMS Numérique 2023, l'ARS Hauts-de-France invite les ESMS à renseigner l'autodiagnostic intitulé Gestion SI OG de l'ANAP : « En prérequis à la définition de la stratégie de votre système d'information et à la structuration du projet, l'autodiagnostic de maturité et de sécurité du système de l'Agence Nationale d'Appui à la Performance (ANAP) est mis à votre disposition. Chaque organisme gestionnaire participant à un projet, qu'il soit porteur de projet ou participant à un regroupement est invité à fournir les résultats de cet autodiagnostic […] ».
Les objectifs de cet outil sont multiples :

> Faire le point de manière autonome et rapide sur votre niveau de maturité du système d'information
>
> Evaluer la capacité de votre organisme gestionnaire à déployer un projet SI
>
> Disposer d'une trajectoire sur à 3-5 ans et établir un plan d'action adapté.

Dans le cadre d'un accompagnement des organisations sociales et médico-sociales par le Collectif SI MS HDF, cet outil permet également d'identifier les points de convergence en phase d'émergence de coopération et de montage du projet ESMS Numérique.

Pour faciliter le renseignement de votre autodiagnostic, le Collectif SI MS HDF met à votre disposition un kit composé de 3 outils complémentaires à savoir :

> Un premier tutoriel relatif au chemin d'accès à l'autodiagnostic et aux fonctionnalités sur le site de l'ANAP
>
> Un deuxième tutoriel présentant le contenu de l'autodiagnostic, à savoir les 7 domaines et les sous-parties : lien
>
> Le présent guide d'appui au renseignement de l'autodiagnostic

Ce guide est à destination des directeurs d'ESMS, responsables qualités, chefs de services ou autres non-experts en informatique, chargés de renseigner l'autodiagnostic « Gestion SI OG » de l'ANAP. Il a pour vocation d'expliciter les termes les plus complexes à l'aide de définitions et illustrations.

D1

Dimension 1.

→ Pratiques de management des SI

Collectif SI Médico-Social Hauts-de-France
ADMR FEHAP FHF nexem SYNERPA UNA UNIOPSS
Avec le soutien de
UNION EUROPÉENNE
Financement dans le cadre de la réponse de l'Union à la pandémie de COVID-19
l'Europe s'engage Hauts-de-France avec le FEDER
ars Agence Régionale de Santé Hauts-de-France

A.01. Gouvernance des SI

Système d'information (SI) : Ensemble des moyens (organisation, acteurs, procédure, systèmes informatiques) nécessaires au traitement et à l'exploitation des informations dans le cadre d'objectifs définis au niveau de la stratégie de l'établissement, des métiers, de la réglementation.

Source : https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS_GUIDECYBER_PHASE%201-EXE%20-V2.pdf

Niveau 1.

Feuille de route SI : La Feuille de Route du Système d'Information est un document stratégique de programmation conçu pour préparer l'évolution et l'adaptation du système d'information d'une structure ou d'un groupe, sur une période donnée, qui va généralement de 3 à 5 ans.

Source : Document ANAP « Pourquoi élaborer une feuille de route SI / schéma directeur SI dans une structure médico-sociale ? »

Niveau 3.

Portefeuille de projets SI : La feuille de route SI peut se décliner en un portefeuille de projets suivi de manière régulière (tous les 6 mois). Il s'agit de la mise en œuvre stratégique de la feuille de route.

Source : Document ANAP « Pourquoi élaborer une feuille de route SI / schéma directeur SI dans une structure médico-sociale ? »

Niveau 4.

Schéma directeur de SI (SDSI) : Le schéma directeur du système d'information est un document, plus complexe que la feuille de route, de description de la stratégie autour des SI. Il approfondit la vision des processus métiers à outiller par le SI et détaille d'avantage les projets qui constituent le portefeuille. Mettre en place un SDSI est recommandé pour les organismes ayant plus de 500 salariés.

Source : Webinaire ANAP « RSI MS "Pratiques de management SI" – Approfondissement (théorie) » du 3 mars 2022

A.02.7. Pilotage des projets

Palier initial.

Porteur de projet : Le porteur de projet porte la responsabilité du projet.

Source : Webinaire ANAP « RSI MS "Pratiques de management SI" - Fondamentaux (théorie) » du 27 janvier 2022

Niveau 2.

Chef de projet : Le chef de projet pilote et mène la mission jusqu'à son aboutissement et coordonne les équipes.

Source : Webinaire ANAP « RSI MS "Pratiques de management SI" - Fondamentaux (théorie) » du 27 janvier 2022

A.03. 8. Accompagnement au changement (trouver un sponsor métier)

Palier initial.

Représentants métiers : Ce sont les utilisateurs cible des solutions logicielles, à savoir les éducateurs, psychologues, chefs de service, médecins, secrétaires, etc.

Source : Webinaire ANAP « RSI MS "Pratiques de management SI" - Fondamentaux (théorie) » du 27 janvier 2022

Niveau 2.

Référent métier : Un référent métier assure une fonction de relai et d'alerte entre les utilisateurs d'un système d'information et le chef de projet. Le référent métier doit avoir si possible une appétence pour les outils informatiques ou le déploiement d'un Dossier Usager Informatisé.

Niveau 3.

Sponsor métier : Le sponsor métier désigne un professionnel (chef de service, éducateurs, psychologues, médecins, secrétaires, etc.) qui soutient et dynamise le projet dans le temps. Il est attentif à la bonne avancée du projet, en particulier les progrès mais aussi les blocages ou difficultés qu'il remontra si besoin au chef de projet. Ce rôle peut être assuré par le chef de projet ou le référent métier.

A.04.9. Processus de gestion formalisé

Niveau 1.

Plan de Continuité d'Activité (PCA) : Ensemble de procédures, moyens, équipements et architectures afin de permettre la continuité de l'activité quels que soient les sinistres qui pourraient survenir.

Niveau 2.

Plan de Reprise d'Activité (PRA) : Un Plan de Reprise d'Activité (PRA) est un document qui liste l'ensemble des dispositions et que doit prévoir la structure pour assurer la reprise de l'activité de son système d'information en cas de crise majeure ou importante du centre informatique (panne matérielle, cyberattaque…). Il est complémentaire au Plan de Continuité d'Activité.

Source : Webinaire ANAP « RSI MS "Pratiques de management SI" - Fondamentaux 2ème partie : comment conduire un projet SI mutualisé ? » du 10 mars 2022

Niveau 3.

Processus de gestion des SI formalisé : La formalisation des processus de gestion des SI est l'identification et la modélisation d'un SI à travers ses processus se traduisant en 3 domaines : l'architecture métier, l'architecture fonctionnelle et l'architecture informatique.

Niveau 4.

Processus métiers formalisés : La formalisation des processus métiers est une pratique de description/modélisation, d'analyse et d'optimisation des processus métiers de bout en bout permettant à l'organisation d'atteindre ses objectifs métiers stratégiques. Les processus métiers peuvent être organisés en 3 domaines : pilotage (mesure et suivi de l'activité, rendu-compte…) ; métier (accompagner l'usager et le suivre dans ses projets de vie, coordonner les acteurs internes et externes…) ; support (gestion des RH, gestion budgétaire et comptable…).

Source : Webinaire ANAP « RSI MS "Pratiques de management SI" – Approfondissement (théorie) » du 3 mars 2022

A.05. 10. Financement

Niveau 4.

DSI : La Direction des Systèmes d'Information (DSI) conçoit, déploie et maintien des systèmes d'information permettant d'appuyer les acteurs métiers dans l'exercice efficient de leurs missions. Elle porte ainsi 2 volets d'activité : transformation du SI et création de la valeur ; et maintenance et gestion opérationnelle.

Source : Webinaire ANAP « RSI MS "Pratiques de management SI" - Fondamentaux (théorie) » du 27 janvier 2022

A.06. Place du SI dans la gouvernance de l'organisme

Niveau 3.

Document Unique de Délégation (DUD) : Document qui précise par écrit les compétences et missions confiées par délégation au professionnel chargé de la direction d'un établissement ou service.

A.09. 3. Confidentialité : Respect du réglementaire (ex : RGPD)

Niveau 1.

DPO ou référent RGPD nommé : Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Source : https://www.cnil.fr/fr/definition/delegue-protection-donnees

Niveau 2.

Registre des traitements réalisés : Le registre des activités de traitement permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que vous faites avec les données personnelles.
Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité.

Source : https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

Niveau 3.

Analyses d'impact réalisées : L'analyse d'impact relative à la protection des données (AIPD) est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée. Elle concerne les traitements de données personnelles qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Source : https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd

Niveau 4.

Traçabilité organisée des accès : Afin de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident, il convient d'enregistrer certaines des actions effectuées sur les systèmes informatiques. Pour ce faire, un dispositif de gestion des traces et des incidents doit être mis en place. Celui-ci doit enregistrer les évènements pertinents et garantir que ces enregistrements ne peuvent être altérés.

Source : https://www.cnil.fr/fr/securite-tracer-les-acces-et-gerer-les-incidents

Revue annuelle de la conformité : Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Source : https://www.cnil.fr/fr/documenter-la-conformite

→ A.10. Méthode projet

Niveau 2.

Méthodes agiles : Les méthodes agiles caractérisent un mode de gestion des projets informatiques privilégiant le dialogue entre toutes les parties prenantes, clients, utilisateurs, développeurs et autres professionnels du projet, la souplesse en cours de réalisation, la capacité à modifier les plans et la rapidité de livraison.

A.11. Urbanisation

Urbanisation : C'est une discipline d'ingénierie informatique consistant à faire évoluer son système d'information pour qu'il soutienne et accompagne de manière efficace les missions de cette organisation et leurs transformations.

Source : Webinaire ANAP « Direction ESMS "Les clés de réussite d'une stratégie SI" – Comprendre les notions liées au système d'information » du 15 avril 2021

Niveau 3.

Cartographie technique : Elle décrit l'ensemble des matériels, logiciels et technologies composant le système d'information.

Niveau 4.

Cartographie fonctionnelle : Elle décrit la structuration du système d'information en blocs fonctionnels communicants, c'est-à-dire les fonctions permettant de supporter les processus métiers.

Cartographie applicative : La cartographie applicative vise à établir un catalogue des applicatifs (composants logiciels), des flux échangés entre eux et de leur implantation sur l'architecture technique

D2

Dimension 2.

→ Adéquation fonctionnelle

Collectif SI Médico-Social Hauts-de-France
ADMR FEHAP FHF nexem SYNERPA UNA URIOPSS
Avec le soutien de
UNION EUROPÉENNE
Financement dans le cadre de la réponse de l'Union à la pandémie de COVID-19
l'Europe s'engage Hauts-de-France avec le FEDER
ars Agence Régionale de Santé Hauts-de-France

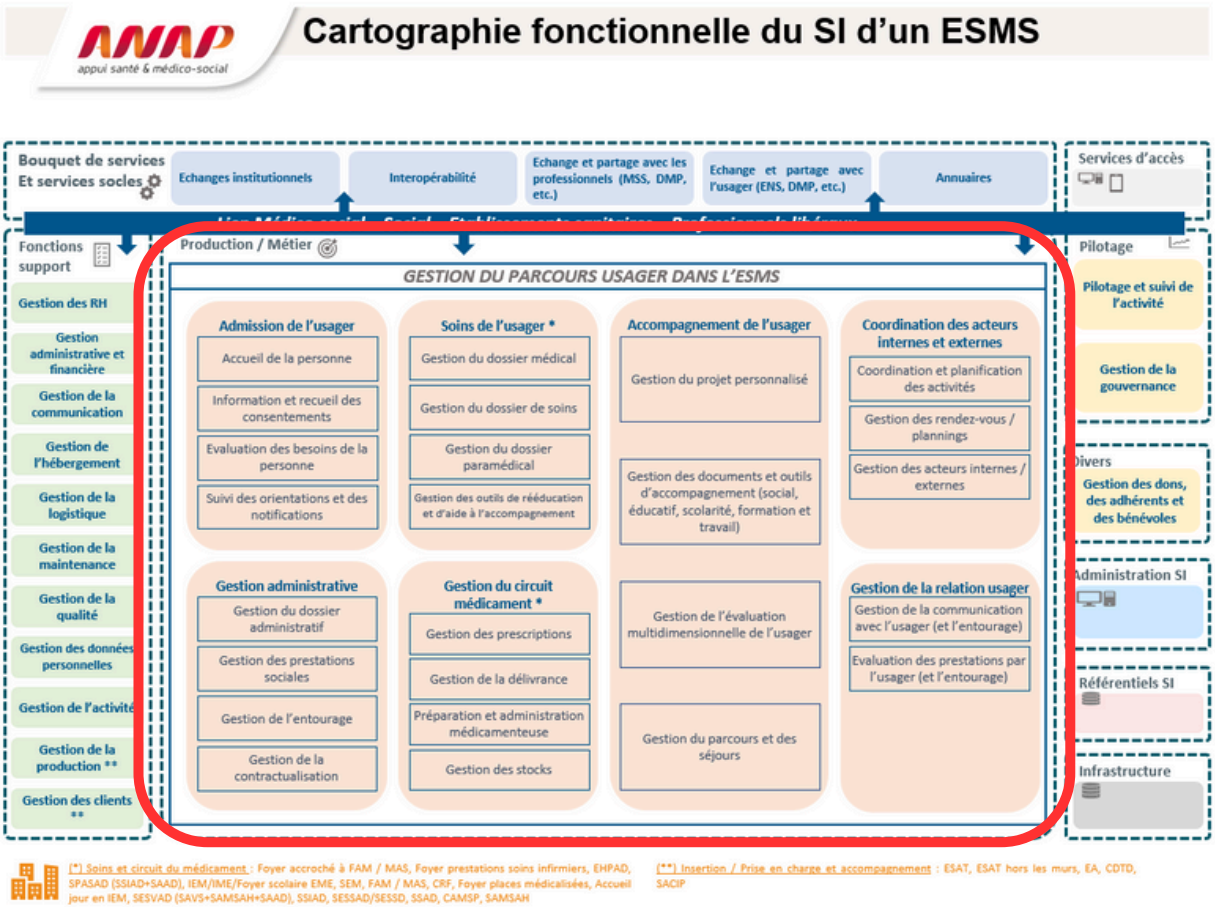
Adéquation fonctionnelle : L'adéquation fonctionnelle permet d'évaluer si la solution présentée est conforme aux attentes implicites et explicites de l'utilisateur.

DUI : Le Dossier de l'Usager Informatisé (DUI) centralise l'ensemble des informations qui concernent les personnes accueillies et accompagnées par un ESMS. Il centralise sur un même support des informations administratives, médicales, paramédicales, socio-éducatives et professionnelles pour une meilleure compréhension de la situation de l'usager et ainsi proposer un accompagnement de qualité.
Outil de suivi et de partage d'informations entre les professionnels (médicaux, paramédicaux, sociaux et médico-sociaux), le DUI est aussi un support d'échange avec les familles et les aidants. Les informations peuvent être complétées par les professionnels des structures ou du soin, la personne elle-même ou son proche.

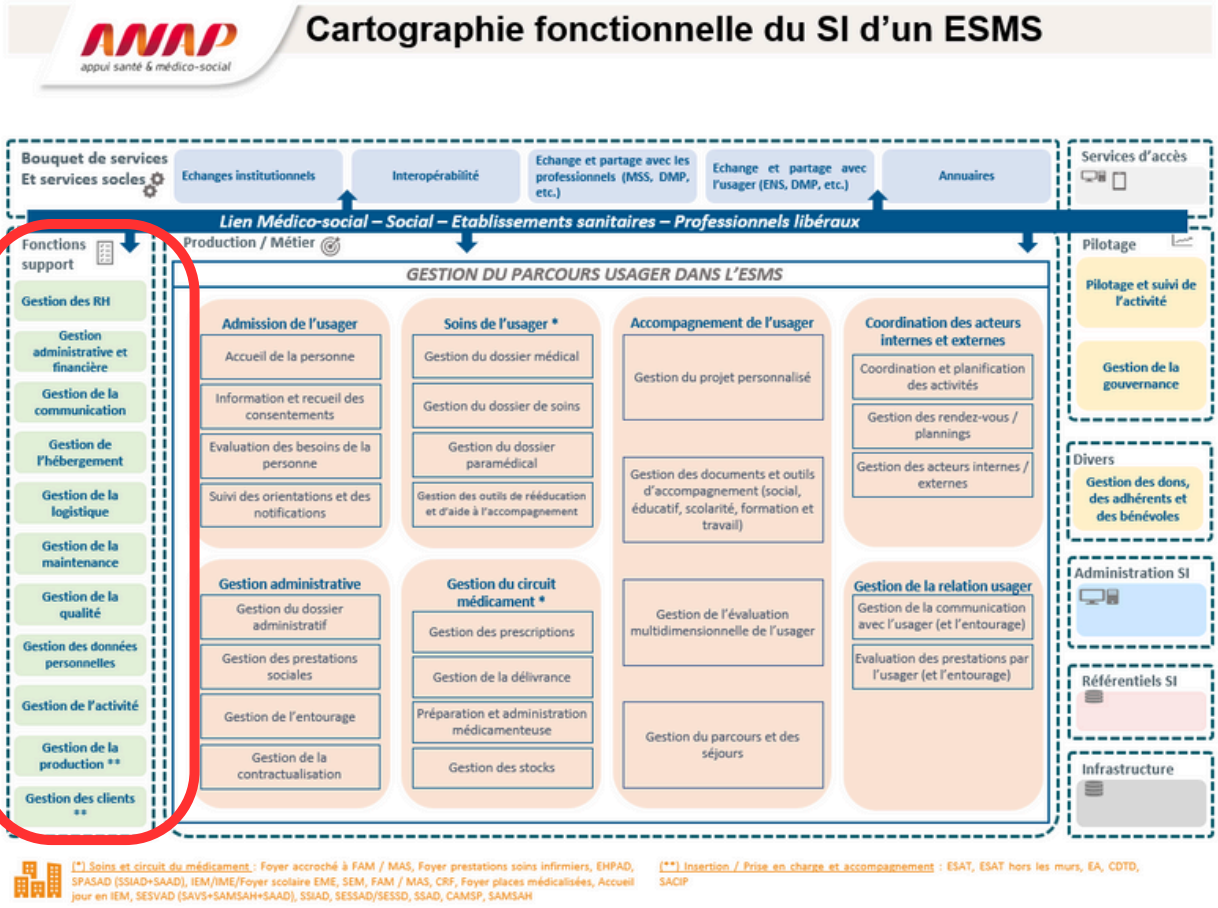
Cartographie fonctionnelle de l'ANAP : C'est un document de l'Agence Nationale de la performance sanitaire et médico-sociale (ANAP) qui présente en un schéma l'ensemble des fonctions à couvrir par le système d'information pour répondre à tous les besoins des professionnels dans une structure médico-sociale.

Source : https://anap.fr/s/article/numerique-publication-2604

B.1. Adéquation fonctionnelle - Dossier usager informatisé



B.2. Adéquation fonctionnelle - Reste du système d'information



B.3. Adéquation fonctionnelle - Interopérabilité

Interopérabilité : C'est la capacité que possède un produit ou un système, dont les interfaces sont généralement connues, à fonctionner et communiquer avec d'autres produits ou systèmes existants ou futur sans restriction d'accès ou de mise en œuvre. C'est-à-dire, disposer d'outils dans un langage commun ou capable de « traduire » l'information.

Source : Webinaire ANAP Directeurs d'ESMS1 Comprendre les notions liées au SI

Services socles : Les 4 service socles prioritaires de la « vague 1 » du Ségur sont les suivants : le Dossier Médical Partagé (DMP), la Messagerie Sécurisée en Santé (MSS), l'Identité Nationale de Santé (INS) et Pro Santé Connect. S'ajoute à cela d'autres services socles tels que la e-prescription et le programme e-parcours. L'ensemble des services socles, encore appelés services numériques, sont directement accessibles à partir des logiciels métiers (DUI) référencés Ségur.

MSS : Les messageries sécurisées de santé (MSS) sont des messageries électroniques réservé aux professionnels habilités (médicaux, sociaux et médico-sociaux), afin de faciliter les échanges de données de santé de manière sécurisée.

Source : https://esante.gouv.fr/produits-services/mssante

INS : L'identité Nationale de Santé (INS) est l'identité clé du système de santé : elle permet d'identifier de manière unique et pérenne les usagers, et participe ainsi à sécuriser les échanges et le partage de données de santé entre acteurs, ainsi qu'à sécuriser le suivi des personnes accompagnées. L'INS est constituée du matricule INS et de 5 traits d'identité.

Source : https://esante.gouv.fr/sites/default/files/media_entity/documents/guide_dui_interoperable_services_et_referentiels_socles.pdf

DMP : Le Dossier Médical Partagé (DMP) est le carnet de santé numérique des usagers. Il permet d'assurer la conservation de données et de documents de santé ou du médico-social de manière sécurisée, et leur partage entre professionnels de santé ou du médico-social habilités.

Source : https://esante.gouv.fr/sites/default/files/media_entity/documents/guide_dui_interoperable_services_et_referentiels_socles.pdf

E-Prescription : La e-prescription est déployée au travers d'un nouveau service proposé aux professionnels de santé sous le nom d'ordonnance numérique. Cette dernière permet de dématérialiser le circuit de la prescription entre les prescripteurs et les pharmaciens ou les professionnels qui réalisent l'acte prescrit afin de favoriser la coordination des soins. Elle permet également aux patients de retrouver leurs ordonnances au format numérique dans Mon espace santé, grâce à l'alimentation automatique du DMP à partir du logiciel métier du prescripteur.

Source : https://www.ameli.fr/pharmacien/exercice-professionnel/delivrance-produits-sante/regles-delivrance-prise-charge/ordonnance-numerique

E-parcours : Le programme « e-parcours » vise à offrir un panel de services numériques de coordination (dossier de coordination, messagerie instantanée, agenda patient, grilles d'évaluation…) au bénéfice des acteurs de la coordination afin d'organiser l'articulation entre médecine de ville, médico-social et hôpital. L'objectif est de développer et de simplifier la coordination entre les professionnels au profit de l'usager, dans une logique de prise en charge décloisonnée.

Source : https://esante.gouv.fr/sites/default/files/media_entity/documents/Atelier%20e-parcours.pdf

ENS : L'Espace Numérique de Santé (ENS) est plus connu sous le nom de « Mon espace santé ».

Mon Espace Santé : Mon espace santé (MES) est un espace numérique de santé pour tous les usagers en France. Il permet à chacun de stocker ses documents et ses données de santé de façon gratuite et sécurisée et de les partager avec des professionnels de santé ou du médico-social. On peut citer 4 fonctionnalités intégrées à Mon espace santé : le dossier médical partagé (DMP), le profil médical, la messagerie sécurisée de santé (MSS) et le catalogue de services.

Source : https://esante.gouv.fr/sites/default/files/media_entity/documents/guide_dui_interoperable_services_et_referentiels_socles.pdf

D3

Dimension 3.

→ Adéquation de l'infrastructure

Collectif SI Médico-Social Hauts-de-France
ADMR FEHAP FHF nexem SYNERPA UNA URIOPSS
Avec le soutien de
UNION EUROPÉENNE
Financement dans le cadre de la réponse de l'Union à la pandémie de COVID-19
l'Europe s'engage Hauts-de-France avec le FEDER
ars Agence Régionale de Santé Hauts-de-France

C.01. Réseaux (LAN/WAN)

Réseaux LAN/WAN : Les réseaux LAN sont des réseaux informatiques reliant des équipements sur une aire géographique réduite. Alors que les réseaux WAN sont des réseaux informatiques reliant des équipements sur des distances importantes (on peut citer par exemple le réseau Internet, qui est le réseau WAN le plus connu).

Source : https://www.ssi.gouv.fr/uploads/2018/11/guide-cartographie-systeme-information-anssi-pa-046.pdf

Niveau 1.

Câblage recetté : On parle d'un câblage recetté lorsque l'ensemble de l'installation du réseau câblé a été vérifié par un technicien spécialisé. Ce dernier vérifie que le système de câblage réponde aux normes en vigueur et fonctionne parfaitement.

Qualité de service garantie : La qualité de service garantie désigne l'obligation contractuelle du prestataire à fournir un service conforme à des exigences en matière de temps de réponse et de bande passante. Les principaux critères permettant d'apprécier la qualité de service sont en général les suivants : débit, latence, gigue, perte de paquet, déséquencement.

Niveau 2.

Logs de connexion internet : Les « fichiers journaux » ou logs sont des enregistrements des activités des utilisateurs, des anomalies et des événements liés à la sécurité d'un environnement informatique (logiciel, système d'exploitation, application, site internet etc.).

Niveau 4.

Test d'intrusion annuel : Un test d'intrusion annuel consiste à vérifier chaque année le niveau de sécurité d'un système, d'un réseau ou encore d'une application de travail sur le web.

C.02. Parc informatique

Niveau 1.

Catalogue de service : Un catalogue de services informatiques est un répertoire de tous les services qu'une équipe informatique propose à ses utilisateurs finaux, avec des informations pertinentes telles que la durée prévue de la prestation de services, les coûts opérationnels associés et les approbations.

OS Pro : Un système d'exploitation (Operating System en anglais ou OS) est un ensemble de programmes qui permettent le fonctionnement et l'utilisation des principales ressources de l'ordinateur (mémoire, disque dur, processeur).

Niveau 2.

Déploiement normalisé/industrialisé : Procédure permettant de déployer un système informatique de manière homogène sur l'ensemble des équipements. Le déploiement normalisé/industrialisé se traduit par l'existence d'une charte d'usage des équipements (dont équipements personnels) et une politique BYOD.

Charte d'usage : Plus connue sous le nom de charte informatique, ou charte d'utilisation des équipements informatiques, la charte d'usage est un document qui définit les conditions d'utilisation des équipements informatiques de l'entreprise (postes de travail, réseau informatique, messagerie, accès à Internet...). Elle vise donc à poser un cadre clair et strict tant pour le salarié que pour l'employeur.

Politique BYOD : L'acronyme « BYOD » est l'abréviation de l'expression anglaise « Bring Your Own Device » (en français : « Apportez Votre Equipement personnel de Communication » ou AVEC), qui désigne l'usage d'équipements informatiques personnels dans un contexte professionnel. Il peut s'agir par exemple d'un employé qui, pour se connecter au réseau de l'entreprise, utilise un équipement personnel comme son ordinateur, sa tablette ou son smartphone.

Source : https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques

Niveau 4.

Gestion centralisée : La gestion centralisée est une méthode de pilotage, depuis un point central, de l'ensemble des ressources matérielles et logicielles (parc informatique) utilisées au sein d'une organisation. Elle concourt à l'élaboration d'orientations stratégiques grâce à une gestion optimisée des différentes activités liées au parc informatique parmi lesquelles : l'acquisition et le renouvellement de l'ensemble des ressources matérielles et logicielles ; la maintenance informatique préventive et corrective ; la gestion des différents prestataires intervenants dans l'organisation et l'entretien du parc informatique ; le déploiement et le maintien de systèmes assurant la sécurité matérielle et logicielle ; la gestion stratégique du budget attribué au parc informatique, etc.

WSUS : Windows Server Update Services (WSUS) est un service permettant de distribuer les mises à jour pour Windows et d'autres applications Microsoft sur les différents ordinateurs fonctionnant sous Windows au sein d'un parc informatique.

Console antivirale : Console centralisée de gestion de l'antivirus de l'organisation (gestion des alertes, ...).

Master Data Management (MDM) : La gestion des données de référence ou gestion des données maîtres (GDR en français) est une branche des technologies de l'information qui définit un ensemble de concepts et de processus visant à définir, stocker, maintenir, distribuer et imposer une vue complète, fiable et à jour des données référentielles au sein d'un système d'information, indépendamment des canaux de communications, du secteur d'activité ou des subdivisions métiers ou géographiques.

Gestion helpdesk : Le centre d'assistance (helpdesk) est l'intermédiaire par lequel les employés accèdent à l'assistance informatique. Ses opérateurs sont les techniciens informatiques et les agents d'helpdesk virtuels qui font du centre d'assistance une ressource centralisée permettant de résoudre les problèmes techniques.

C.03. Ressources serveurs

Niveau 2.

Sauvegarde sécurisée contrôlée : Effectuer des sauvegardes régulières permet de limiter l'impact d'une disparition non désirée de données. Ainsi, plusieurs modalités de sauvegarde doivent être mises en œuvre en fonction du type de données sauvegardées (nature, criticité, volume...). Dans le cadre d'une sauvegarde sécurisée contrôles, l'ESMS a défini une politique de gestion et de suivi des sauvegardes conforme aux recommandations de la CNIL (effectuer des sauvegardes fréquentes, stocker les sauvegardes sur un site extérieur idéalement dans des coffres ignifugés et étanches, etc.)

HDS : La certification HDS (Hébergement de Données de Santé) a pour vocation de renforcer la protection des données de santé à caractère personnel et de construire un environnement de confiance autour de l'eSanté et du suivi des patients. Elle s'appuie sur des référentiels incluant le respect de normes ISO.

Source : https://esante.gouv.fr/produits-services/hds

Niveau 4.

PRA/PCA : Cf. A.04.09 Processus de gestion formalisé

D4

Dimension 4.

→ Qualité de service

Collectif SI Médico-Social Hauts-de-France
ADMR FEHAP FHF nexem SYNERPA UNA UNIOPSS
Avec le soutien de
UNION EUROPÉENNE
Financement dans le cadre de la réponse de l'Union à la pandémie de COVID-19
l'Europe s'engage Hauts-de-France avec le FEDER
ars Agence Régionale de Santé Hauts-de-France

D.01. Gestion de l'environnement de l'utilisateur

Palier initial.

Cloud public : Un cloud public est une infrastructure informatique dans laquelle un fournisseur de services met des ressources à la disposition du public via internet. Les ressources varient selon le fournisseur mais peuvent inclure des capacités de stockage, des applications ou des machines virtuelles.

Niveau 4.

Revue annuelle des droits : Réaliser une revue annuelle des habilitations, des droits d'accès est une précaution élémentaire afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.

Source : https://www.cnil.fr/fr/securite-gerer-les-habilitations

D.02. Gestion des niveaux de service et des prestataires

Niveau 2.

SLA : Le SLA, Service Level Agreement en anglais, consiste en un accord entre un fournisseur et un utilisateur final. Cet accord établit et définit clairement le niveau de service que l'utilisateur final attend du fournisseur de services. Pour cela, il contient les paramètres de mesure de ce service et les solutions ou pénalités, en cas de non-respect des niveaux de services convenus. Traduit par Engagement des niveaux de service en français, c'est un élément crucial lorsqu'un organisme choisit d'externaliser l'un de ses services auprès d'un prestataire extérieur.

D5

Dimension 5.

→ Sécurité des SI

Collectif SI Médico-Social Hauts-de-France
ADMR FEHAP FHF nexem SYNERPA UNA UNIOPSS
Avec le soutien de
UNION EUROPÉENNE
Financement dans le cadre de la réponse de l'Union à la pandémie de COVID-19
l'Europe s'engage Hauts-de-France
ars Agence Régionale de Santé Hauts-de-France

E.01.2. Sécurité (organisationnelle et stratégique) (utilisateur = Professionnels et usagers)

Niveau 1.

Charte SI : Pour respecter le RGPD, toutes les organisations qui traitent des données personnelles doivent mettre en place une charte informatique. Cette charte fixe les règles d'utilisations des outils informatiques d'une entreprise, mis à la disposition de ses employés. La charte informatique définit aussi les risques encourus dans le cas du non-respect de ces règles et des obligations liées au RGPD. Pouvant être intégrée au règlement intérieur de l'entreprise ou au contrat de travail des salariés, la charte informatique et sa mise en application sont recommandées par la CNIL.

Niveau 3.

RSSI : La mission première du Responsable de la Sécurité des Systèmes d'Information (RSSI) est de s'assurer et garantir la bonne application de la politique de sécurité du SI. Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il préconise toute décision d'intervention sur les systèmes d'information, dans leur globalité, de son périmètre pour préserver l'intégrité et la continuité du SI.

Source : https://www.cigref.fr/wp/wp-content/uploads/2021/12/Cigref-Nomenclature-RH-des-profils-metiers-du-SI-version-intermediaire-2021.pdf

Niveau 4.

Référentiel PGSSI-S : La PGSSI-S (Politique Générale de Sécurité des Systèmes d'Information de Santé) regroupe des référentiels thématiques (identification électronique des acteurs, force probante des documents de santé, imputabilité des actions…) et des guides pratiques, qui rappellent aux différents acteurs des systèmes d'information de santé les bonnes pratiques pour être en conformité avec la réglementation en vigueur.

Source : https://esante.gouv.fr/sites/default/files/media_entity/documents/180528_PGSSI-S_0.pdf

E.02.1. Identité de l'utilisateur (identité de l'usager, identité du professionnel)

Niveau 1.

Procédures d'identification des utilisateurs formalisées : Il est nécessaire que les droits et les accès au système d'information soient mis à jour en fonction des évolutions des effectifs d'une entité (arrivées, départs, mobilité interne. Les procédures d'arrivée et de départ doivent donc être définies, et mise à jour en fonction du contexte : création et suppression des comptes informatiques et boîtes aux lettres associées ; droits et accès à attribuer et retirer à une personne dont la fonction change ; gestion des documents et informations sensibles (transfert de mots de passe, changement des mots de passe ou des codes sur les systèmes existants) ; etc.

Source : https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

Niveau 2.

Disparition des comptes génériques d'accès au SI : L'accès au système d'information doit s'effectuer à l'aide de comptes utilisateurs nominatifs, et non génériques, afin de pouvoir de tracer les actions faites dans le SI et, ainsi, de responsabiliser l'ensemble des intervenants. En effet, les comptes génériques (ex : compte pour l'infirmerie, compte pour l'ensemble de l'équipe éducative…) ne permettent pas d'identifier précisément une personne. Cette règle doit également s'appliquer aux comptes des administrateurs systèmes et réseaux et des autres agents chargés de l'exploitation du système d'information.

Politique d'annuaire et de gestion des authentifications : Politique de recensement des logins et mot de passe au sein d'une seule et même base de données en lien avec la matrice d'habilitations (cf. définition matrice d'habilitations).

Niveau 3.

Politique de mot de passe conforme ANSSI : L'Agence National de la Sécurité des Systèmes d'Information (ANSSI) recommande un minimum de 9 caractères pour les services peu critiques (dont la compromission ne donnerait accès à aucune information personnelle, financière et n'impacterait pas le fonctionnement de l'organisation) et un minimum de 14 caractères pour les services critiques (dont la compromission donnerait l'accès à des données de santé de l'usager). Un mot de passe robuste comporte des capitales, des minuscules, des chiffres et des caractères spéciaux. Il ne doit comporter aucun élément personnel tel qu'une date de naissance ou un prénom.

Source : https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS_GUIDECYBER_PHASE%201-EXE%20-V2.pdf

RPPS+ : Le portail RPPS+ permet l'enregistrement des professionnels du médico-social ayant besoin d'accéder à des services numériques en santé. Les professionnels enregistrés dans le RPPS, répertoire sectoriel de référence des personnes physiques, peuvent ainsi : disposer d'une e-CPS pour accéder aux services numériques locaux (DUI), régionaux (plateforme régionale, e-parcours) et nationaux (DMP), notamment en mobilité ; disposer d'une messagerie sécurisée MSSanté nominative pour échanger des données de santé.

Source : https://esante.gouv.fr/actualites/ouverture-du-portail-rpps-lensemble-des-etablissements-et-services-medico-sociaux

→ E.03. Sécu Physique (patrimoine baie – équipements matériels)

Baie : Une baie de type informatique est une armoire technique qui abrite les équipements d'un réseau informatique et téléphonique. Elle est équipée en général de panneaux de brassage, de switchs (commutateur réseau), de routeurs, d'un ou plusieurs serveurs, de divers modems....

Niveau 2.

Equipements critiques : Ce sont les équipements qui doivent être en état de marche pour que l'ESMS puisse fonctionner (routeur, serveur, switchs, ...).

Baie fermée : Il est très fortement recommandé que les baies disposent d'une porte qui ferme ou soient situées dans une pièce fermée à clé pour restreindre l'accès aux équipements qu'elles contiennent et contrôler le flux d'air.

Salle serveur sécurisée : La salle serveur, ou salle informatique, est un lieu central dans l'activité d'une organisation. Aussi, toutes les précautions doivent être prises afin d'éviter des dommages numériques ou physiques qui pourraient mettre en péril l'activité de l'organisation : accès limités aux personnels habilités et sécurisation des locaux (vérification des habilitations, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs, etc.)

Niveau 3.

Habilitations formalisées : L'accès aux données personnelles traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées. De cette analyse, dépend « le profil d'habilitation » de l'agent ou du salarié concerné. Des procédures ont ainsi été mise en place afin par exemple, que pour chaque mouvement ou nouvelle affectation d'un salarié à un poste, le supérieur hiérarchique concerné identifie le ou les fichiers auxquels celui-ci a besoin d'accéder et procède à la mise à jour de ses droits d'accès.

Source : https://www.cnil.fr/fr/10-conseils-pour-la-securite-de-votre-systeme-dinformation

Registre d'accès aux équipements critiques : Afin de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident, il convient d'enregistrer certaines des actions effectuées sur les systèmes informatiques. Pour ce faire, un dispositif de gestion des traces et des incidents doit être mis en place. Celui-ci doit enregistrer les évènements pertinents et garantir que ces enregistrements ne peuvent être altérés.

Source : https://www.cnil.fr/fr/securite-tracer-les-acces-et-gerer-les-incidents

E.04. Sécurité Système & réseau Hardware (système & réseau)

Hardware : Le hardware est la partie physique de l'ordinateur, c'est-à-dire les pièces et les équipements qui le font fonctionner. Le terme désigne également l'ensemble des équipements attachés aux ordinateurs (ou autre produit) qui nécessitent une gestion informatique. Les processeurs sont l'un des hardwares les plus populaires.

Source : https://www.futura-sciences.com/tech/definitions/informatique-hardware-570/

Niveau 1.

Mise à jour système : La mise à jour système consiste à télécharger la version la plus récente système d'exploitation afin de bénéficier des dernières modifications et mesures de sécurité.

Accès système et réseau systématiquement authentifié : Procédure d'authentification des utilisateurs pour l'accès au système informatique et au réseau.

Séparation des comptes systèmes (y compris administration) & utilisateurs : Les comptes systèmes peuvent modifier tous les paramètres du système informatique, installer des applications, etc. Ces taches ne sont pas permises via un compte utilisateurs. Ainsi pour des raisons de sécurité, il faut séparer les comptes systèmes des comptes utilisateurs.

Niveau 2.

Solution de supervision déployée et managée : C'est un outil qui permet de suivre en temps réel l'état de fonctionnement du système d'information.

Supervision des accès externes (sur services publiés) : Elle permet de suivre en temps réel la disponibilité des applications, des services en ligne ou hébergés, utilisés par l'organisation.

Revue périodique des comptes informatiques et des droits d'accès : cf. définition revue annuelle des droits

Niveau 3.

Scan de vulnérabilité : C'est un programme conçu pour identifier des failles dans une application, un système d'exploitation ou un réseau. Il permet de détecter rapidement les vulnérabilités et les menaces de cybersécurité, d'identifier les dispositifs non autorisés et de trouver des indices indiquant qu'un système a été compromis. Ils peuvent également identifier le système d'exploitation utilisé, la dernière mise à jour des logiciels et la dernière application de correctifs de sécurité.

Niveau 4.

Solution d'analyse comportementale déployée et managée : L'utilisation d'une solution d'analyse comportementale permet de suivre et marquer les comportements suspects ou malveillants des utilisateurs.

Test d'intrusion annuel : cf. définition réseaux LAN/WAN

→ E.05. Sécurité applicative

Matrice d'habilitations : La matrice d'habilitations doit permettre d'identifier les profils utilisateurs à créer et les droits d'accès au SI qui y sont liés.

Source : Guide ANAP : « Déployer un dossier de l'usager - Méthode pour le chef de projet en contexte multi-ESMS/OG »

Interfaces : Le terme interface désigne un programme permettant un échange de données. Il y 3 types d'interfaces : interface entre deux logiciels (programme qui reformate les données pour assurer la compatibilité entre deux logiciels par exemple) ; interface entre deux équipements informatiques (programme qui permet à ces deux matériels de communiquer, comme un pilote d'imprimante, par exemple) ; ou encore interface « homme-machine » permettant l'interaction entre un système informatique et son utilisateur.

Authentification individuelle systématique : cf. définition disparition des comptes génériques d'accès au SI

Disparition des comptes génériques d'accès au SI : L'accès au système d'information doit s'effectuer à l'aide de comptes utilisateurs nominatifs, et non génériques, afin de pouvoir de tracer les actions faites dans le SI et, ainsi, de responsabiliser l'ensemble des intervenants. En effet, les comptes génériques (ex : compte pour l'infirmerie, compte pour l'ensemble de l'équipe éducative…) ne permettent pas d'identifier précisément une personne. Cette règle doit également s'appliquer aux comptes des administrateurs systèmes et réseaux et des autres agents chargés de l'exploitation du système d'information.

Revue périodique des matrices d'habilitations applicatives : Il s'agit de la mise en place d'une révision, à un rythme défini, des matrices d'habilitations.

→ E.06. Identité de la personne accompagnée (identité de l'usager)

Niveau 1.

Référentiel d'Identitovigilance : Le référentiel national d'identitovigilance (RNIV) a pour objet de fixer les exigences et recommandations à respecter en termes d'identification des usagers pris en charge sur le plan sanitaire ou médico-social par les différents professionnels impliqués (structures de ville, établissements de santé, secteur médico-social, acteurs sociaux) afin de maîtriser les risques dans ce domaine.

Source : https://esante.gouv.fr/sites/default/files/media_entity/documents/RNIV%201%20Principes%20communs_1.pdf

D6

Dimension 6.

→ Ethique, Développement durable

Collectif SI Médico-Social Hauts-de-France
ADMR FEHAP FHF nexem SYNERPA UNA
Avec le soutien de
UNION EUROPÉENNE
Financement dans le cadre de la réponse de l'Union à la pandémie de COVID-19
l'Europe s'engage Hauts-de-France
ars Agence Régionale de Santé Hauts-de-France

F.01. Ethique du numérique

Ethique du numérique : Il s'agit d'installer le développement d'un numérique en santé dans un cadre éthique, respectueux des droits de l'ensemble des acteurs de l'écosystème (usagers du système de santé et professionnels), de façon à garantir la confiance, l'adhésion, et par voie de conséquence, les usages.

Source : https://esante.gouv.fr/esante.gouv.fr/virage-numerique/ethique-et-numerique-en-sante/pourquoi-ethique-et-numerique

F.02. Démarche RSE sur le numérique

RSE : La responsabilité sociétale des entreprises (RSE) également appelée responsabilité sociale des entreprises est définie par la commission européenne comme l'intégration volontaire par les [organisations] de préoccupations sociales et environnementales à leurs activités [...] et leurs relations avec les parties prenantes. En d'autres termes, la RSE c'est la contribution des [organisations] aux enjeux du développement durable.

Source : https://www.economie.gouv.fr/entreprises/responsabilite-societale-entreprises-rse

Niveau 1.

DEEE : Un DEEE, ou D3E, est un déchet d'équipement électrique et électronique. On peut parfois également entendre parler de déchet électrique, de matériel électrique usagé, d'équipement électrique hors service. C'est un équipement fonctionnant sur secteur ou bien avec des piles ou batteries, devenu hors d'usage. [...] La réglementation impose de mettre en place la collecte des DEEE et leur recyclage.

Source : https://www.ecosystem.eco/fr/article/deee

Niveau 2.

Green IT : La Green IT, ou Eco TIC en français (pour Techniques de l'Information et de la Communication), est un ensemble de techniques ou de pratiques visant à réduire l'empreinte sociale, économique et environnementale du numérique.

D7

Dimension 7.

→ Performance, usage et satisfaction

Collectif SI Médico-Social Hauts-de-France
ADMR FEHAP FHF nexem SYNERPA UNA UNIOPSS
Avec le soutien de
UNION EUROPÉENNE
Financement dans le cadre de la réponse de l'Union à la pandémie de COVID-19
l'Europe s'engage Hauts-de-France avec le FEDER
ars Agence Régionale de Santé Hauts-de-France

G.05. Innovation Numérique/SI

Niveau 3.

Structures 3.0 : « Structures 3.0 : favoriser l'innovation numérique dans le secteur social et médico-social » est un AAP de l'ANS. La première édition a eu lieu en 2020, avec 140 candidats et 10 lauréats. 2 nouvelles éditions de l'appel à projets ont eu lieu en 2021 et 2022 et d'autres sont prévues jusqu'en 2025 dans le cadre du Ségur du numérique en santé.

GLOSSAIRE

ANAP = Agence Nationale de la Performance sanitaire et médico-sociale

ANSSI = Agence Nationale de la Sécurité des Systèmes d'Information

BOYD = Bring Your Own Device (en français : « Apportez Votre Equipement personnel de Communication » ou AVEC)

CPOM = Contrats Pluriannuels d'Objectifs et de Moyens

DAF = Direction Administrative et Financière

DEEE = Déchets d'Equipements Electriques et Electroniques

DMP = Dossier Médical Partagé

DPO = Data Protection Officer (en français : « Délégué à la Protection des Données » ou DPD)

DUD = Document Unique de Délégation

DUI = Dossier Usager Informatisé

DSI = Direction des Systèmes d'Information

ESMS = Etablissements et Services Médico-Sociaux

HDS = Hébergement de Données de Santé

INS = Identité Nationale de Santé

MDM = Master Data Management (en français : « Gestion des Données de Référence » ou GRD)

MSS = Messagerie Sécurisée de Santé

OG = Organisme Gestionnaire

PCA = Plan de Continuité d'Activité

PGSSI-S = Politique Générale de Sécurité des Systèmes d'Information de Santé

PRA = Plan de Reprise d'Activité

RGPD = Règlement Général sur la Protection des Données

RPPS = Répertoire Partagé des Professionnels intervenant dans le système de santé

RSE = Responsabilité Sociétale des Entreprises

RSI = Responsable des Systèmes d'Information

RSSI = Responsable de la Sécurité des Systèmes d'Information

SDSI = Schéma Directeur du Système d'Information

SI = Système d'Information

SLA = Service Level Agreement (en français : « Accord sur un niveau de Service »)

WSUS = Windows Server Update Services