



SÉCUR DU NUMÉRIQUE EN SANTÉ

La conformité numérique

Présentation du 25/11/2022

Sommaire

1. La conformité numérique : **pourquoi est-elle requise** pour le secteur sanitaire ?
2. La conformité numérique des établissements de santé: **Cadre réglementaire et feuille de route nationale**
3. La conformité numérique dans mon établissement : **comment faire ?**
4. La conformité numérique dans mon établissement : **sur qui m'appuyer en région PACA ?**

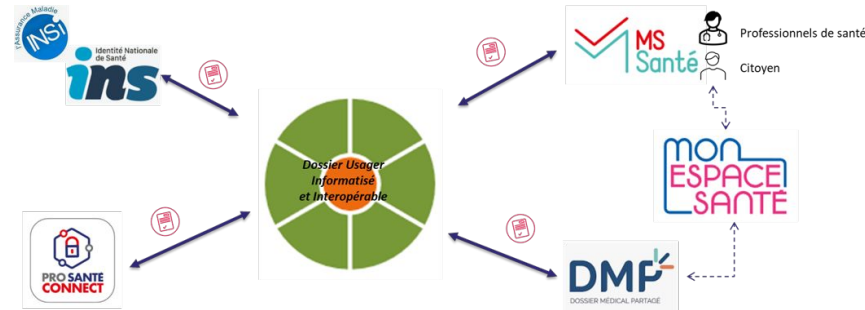
Un environnement numérique grandissant dans nos structures

Le numérique omniprésent à proximité de l'utilisateur

- Un vaste écosystème numérique
 - Des moyens d'interactions numériques nécessaires
 - Assurer la sécurité des parcours et les prises en charge patients
 - Maintenir la confiance des patients dans le système de santé
 - Maintenir la confiance des professionnels dans leurs outils
 - Assurer la continuité des soins et des prises en charge
-
- Une évolution constante des risques concernant les données
 - Un enjeu collectif où la sécurité numérique est l'affaire de tous
 - Favoriser la création d'un espace numérique de confiance

De nouveaux enjeux : la cybersécurité et la **conformité numérique**

Une fonction : gouverner la sécurité numérique de nos structures



Source pour le schéma : https://www.securityevaluators.com/hospitalhack/securing_hospitals.pdf

Conformité numérique

Un bref rappel des principes et obligations en matière de protection des données à caractère personnel collectées ou traitées dans le cadre de vos activités

Conformité numérique et gouvernance des données

Rappels des principes et obligations

PRINCIPES



Minimisation des données



Privacy by design



Proportionnalité



Accountability



Sécurité

COLLECTE



Licéité



Finalité



Loyauté



Information



Consentement

OBLIGATIONS



Registre des traitements



PIA



DPO



Notification des failles



Assurer les droits des personnes

Collecte de données

Le registre des traitements



Registre des
traitements

FICHE DE REGISTRE DE TRAITEMENT	
N° FDR	FDR001
Nom	
Date de création	Date révision
Responsable du traitement	
Responsables conjoints	
DPO ou Réfèrent DPO	
Nom des outils	
Traitement hors UE	
SI LE TRAITEMENT EST SOUS TRAITÉ	
Nom des sous-traitants	
Représentant du ST	
Le contrat précise la finalité du traitement et la catégorie de données	
Le contrat définit les obligations du sous-traitant au regard des droits des personnes	
FINALITES DU TRAITEMENT (Quel est (sont) l'objectif (s) poursuivi (s) ?)	
BASES DE LA LICEITE DU TRAITEMENT (non exclusives)	
<ul style="list-style-type: none"> • fondé sur le consentement préalable de la personne physique ; • fondé sur l'exécution d'un contrat avec la personne physique concernée ; • fondé sur une obligation légale à laquelle le responsable du traitement est soumis ; • fondé sur la protection des intérêts vitaux de la personne concernée ; • fondé sur la réalisation d'une mission d'intérêt public ; • aux fins des intérêts légitimes poursuivis par le responsable du traitement, sauf atteinte aux libertés et droits fondamentaux des personnes. 	
CATEGORIE DE PERSONNES CONCERNEES PAR LE TRAITEMENT	
CATEGORIE DE DONNEES	
DCP	Etat civil, identité, images ? Vie personnelle ? Vie professionnelle ? Economique et financier ? Données de connexion ? Données de localisation ? Internet ? Autres ?
Sensibilité	NON
Durée de conservation	
CATEGORIE DES DESTINATAIRES DU TRAITEMENT	

Ouiiii !

Consentement



Obligation légale



Contrat



Mission
d'intérêt public



Sauvegarde
des intérêts vitaux



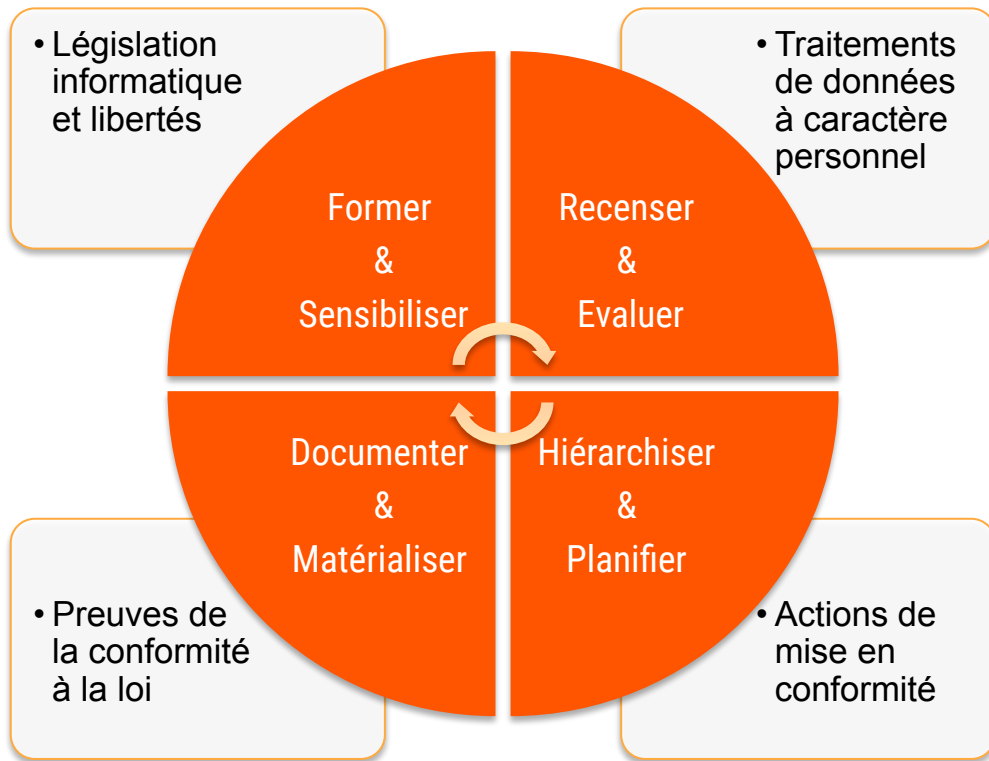
Intérêt légitime

Les bases légales d'un traitement de
données à caractère personnel



CAPSI
Cabinet d'Appui à la Protection des Systèmes d'Information

Une mise en œuvre itérative et permanente de la conformité numérique



Collecte de données

Recommandations

Les bonnes pratiques à mettre en œuvre :



Finalité

- Inscrire les traitements au registre obligatoire et vérifier leur légalité
- Limiter les collectes au strict nécessaire (collecte de données?)
- Informer les répondants (sur les supports de collecte)
- Ne pas réutiliser les données pour un autre usage (détournement)
- Ne pas diffuser les données (y compris en interne)



Sécurité

- Supprimer ou archiver les données non utiles (durée conservation)
- Attention aux zones de commentaires libres dans les outils
- Vigilance au sujet des demandes de droit d'accès (délai de réponse légal contraignant)
- Organiser la protection des données avec mes sous-traitants ou prestataires



Minimisation des données



Registre des traitements



Information

Conformité de votre site institutionnel

CREATION DE COMPTE

CE QU'IL FAUT FAIRE

Usage de cases non pré-cochées ou de déclaration papier

CRÉER UN COMPTE

Valider

☐ Si vous souhaitez recevoir nos propositions commerciales par voie électronique, merci de cocher cette case

☐ Si vous souhaitez recevoir les propositions commerciales de nos partenaires par voie électronique, merci de cocher cette case

Vous pouvez vous désinscrire à tout moment en modifiant vos paramètres sur votre compte et à travers les liens de désinscription.

Le client est informé de ses droits de désinscription et décide séparément de chaque type d'inscription auquel il a accès

CE QU'IL NE FAUT PAS FAIRE

Usage de case pré-cochée, exploitation du silence, de l'inactivité

CRÉER UN COMPTE

Valider

☒ Si vous souhaitez recevoir nos propositions commerciales et celles de nos partenaires par voie électronique, merci de cocher cette case

La case est déjà cochée et concerne toutes les informations commerciales

CRÉER UN COMPTE

Valider

☐ Si vous ne souhaitez pas recevoir des propositions commerciales de nos partenaires par voie électronique, merci de cocher cette case

La case n'est pas cochée, l'inactivité entraîne acceptation des inscriptions

Source et infographie
: www.sarbacane.com

Cookies & traceurs : qu'est-ce qu'un consentement valide ?

Exemple



**Vous contrôlez
les cookies !**

L'entreprise X et ses partenaires digitaux utilisent des cookies sur notre site.

1

Certains sont strictement nécessaires pour le fonctionnement du site mais vous trouverez ci-dessous ceux qui sont optionnels :

- Les cookies de performance;
- Les cookies de personnalisation du site;
- Les cookies pour une publicité ciblée.

2

Quand vous cliquez sur "Accepter les cookies", nous plaçons toutes ces catégories de cookies afin de personnaliser votre visite en ligne.

Si vous préférez paramétrer les cookies vous-même, cliquez sur "Refuser les cookies" ou "Paramètres des cookies".

3

Vous pouvez choisir quels cookies vous souhaitez activer ou non et décider à tout moment de retirer votre consentement.

Pour plus d'information, veuillez consulter notre charte de protection des données.

4

ACCEPTER LES COOKIES

REFUSER LES COOKIES

PARAMÈTRES DES COOKIES



2 Consentement univoque

ne pas utiliser des
bannières
de consentement
"trompeuses"



4 Consentement libre

en cas de refus
l'accès au site ne doit
pas être restreint

Source : DIDOMIL

Collecte de données depuis votre site

Le cas des cookies et traceurs de navigation

En dehors des cookies techniques, le
nécessaire recueil d'un consentement :

- ☐ Révocable
- ☐ Univoque
- ☐ Libre
- ☐ Eclairé
- ☐ Spécifique

Analyse d'impact obligatoire : de quoi s'agit il ?

Focus sur l'analyse d'impact sur la
protection des données (AIPD) ou pour les
anglo-saxons le Privacy Impact
Assessment (PIA)

L'analyse d'Impact définie par la CNIL

Une **analyse d'impact sur la protection des données** est une étude qui doit être menée lorsqu'un traitement de données personnelles est susceptible d'engendrer un **risque élevé pour les droits et libertés** des personnes concernées.



L'analyse préalable d'impacts requise par la réglementation

Les implications dans le secteur de la santé et du médico-social



ETUDE D'IMPACT OBLIGATOIRE si le traitement de données figure sur la liste des PIA obligatoires ou si il remplit deux critères ci dessous

L'analyse d'impact
relative à la protection
des données (Art. 35)

|

**La prescription pour
les traitements les plus
risqués**

Evaluation, Scoring (*y compris
profilage*)

Décision automatique avec effet
légal

Surveillance systématique

Données sensibles ou hautement
personnelles (*santé,
géolocalisation ...*)

Collecte à large échelle

Croisement de données

Personnes vulnérables (*patients,
personnes âgées, enfants ...*)

Usage innovant (*utilisation d'une
nouvelle technologie*)

Exclusion du bénéfice d'un droit
ou d'un contrat

DPO



RSSI

Règlementation de protection des données

Les implications dans le secteur sanitaire

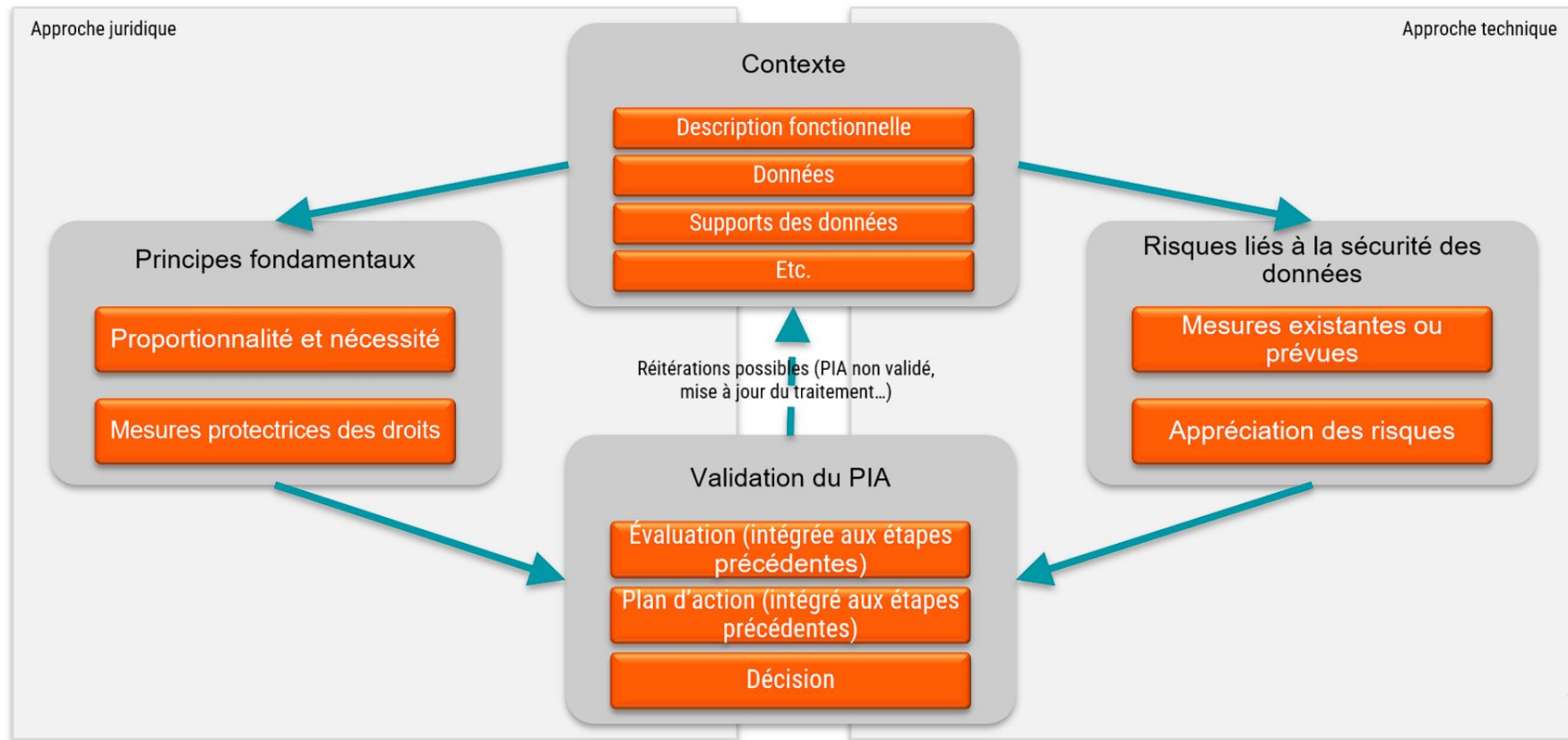
Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise



L'analyse d'impact
relative à la
protection des
données (Art. 35)
|
Une prescription
pour la majorité
des traitements de
données de santé

Types d'opérations de traitement	Critères issus des lignes directrices du CEPD qu'ils remplissent	Exemples
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.	- collecte de données sensibles - personnes dites « vulnérables »	- traitements « de santé » mis en œuvre par les établissements de santé (hôpital, CHU, cliniques, etc.) : <ul style="list-style-type: none"> dossier « patients » ; algorithmes de prise de décision médicale ; dispositifs de vigilances sanitaires et de gestion du risque ; dispositifs de télémedecine ; gestion du laboratoire de biologie médicale et de la pharmacie à usage intérieur, etc. - traitement portant sur les dossiers des résidents pris en charge par un centre communal d'action sociale (CCAS) ou par un établissement d'hébergement pour personnes âgées dépendantes (EHPAD).
Traitements ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire	- personnes dites « vulnérables » - évaluation ou notation - collecte de données sensibles	- dispositif de signalement de mineurs en danger ; - traitement utilisé par une agence sanitaire pour la gestion d'une crise sanitaire ou d'une alerte sanitaire ; - dispositif de signalement de situations de maltraitance sur des personnes vulnérables (personnes âgées, en situation de handicap, etc.).
Traitements ayant pour finalité l'accompagnement social ou médico-social des personnes	- collecte de données sensibles - évaluation ou notation - personnes dites « vulnérables »	- traitement mis en œuvre par un établissement ou une association dans le cadre de la prise en charge de personnes en insertion ou réinsertion sociale et professionnelle ; - traitement mis en œuvre par les maisons départementales des personnes handicapées dans le cadre de l'accueil, l'hébergement, l'accompagnement et le suivi de ces personnes ; - traitement mis en œuvre par un centre communal d'action sociale dans le cadre du suivi de personnes atteintes de pathologies chroniques invalidantes en situation de fragilité sociale.

Analyse d'impact obligatoire : quelle méthodologie ?



Analyse d'impact obligatoire :

PHASE 2 : l'évaluation du respect du droit?

PRINCIPES



Minimisation des données



Privacy by design



Proportionnalité



Accountability



Sécurité

COLLECTE



Licéité



Finalité



Loyauté



Information



Consentement

Analyse d'impact obligatoire :

Phase 3 : l'évaluation des risques ?

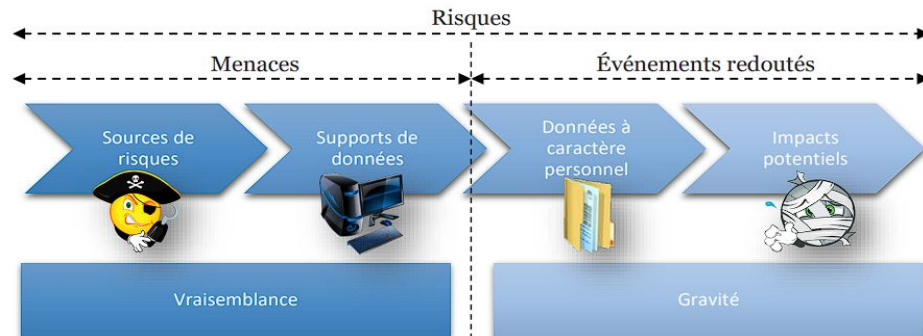


Figure 3 – Éléments composant les risques

Le niveau d'un risque est estimé en termes de gravité et de vraisemblance :

- ❑ la **gravité** représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels¹⁵ ;
- ❑ la **vraisemblance** traduit la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

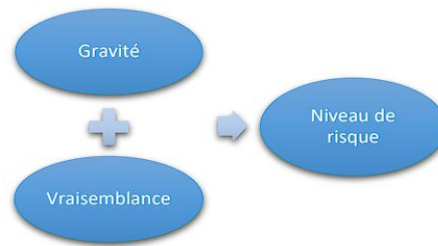


Figure 4 – Éléments permettant d'estimer les risques

Impacts sur :

- ✓ La **disponibilité** de la donnée ;
- ✓ L'**intégrité** de la donnée ;
- ✓ **Confidentialité** de la donnée

Analyse d'impact obligatoire : Les outils disponibles ?

PIA : Outil gratuit de la CNIL utilisable librement pour vos études d'impacts



Outil CNIL PIA : les grandes étapes

Version 2.0.0

Pia Analyse d'impact sur la protection des données
privacy impact assessment

ACCUEIL

MODÈLES DE PIA

Outils

CAPT00

CONTEXTE

- Vue d'ensemble**
- Données, processus et supports

PRINCIPES FONDAMENTAUX

- Proportionnalité et nécessité
- Mesures protectrices des droits

RISQUES

- Mesures existantes ou prévues
- Accès illégitime à des données
- Modification non désirées de do...
- Disparition de données
- Vue d'ensemble des risques

VALIDATION

- Cartographie des risques
- Plan d'action
- Avis du DPD et des personnes c...

Valider le PIA

Contexte

Cette section vous permet d'obtenir une vision claire du(des) traitement(s) de données à caractère personnel considéré(s).

VUE D'ENSEMBLE

Cette partie vous permet d'identifier et de présenter l'objet de l'étude.

Quel est le traitement qui fait l'objet de l'étude ?

Présentez le traitement de manière synthétique : son nom, sa finalité, ses enjeux (apports attendus), son contexte d'utilisation, etc.

Quelles sont les responsabilités liées au traitement ?

Décrivez les responsabilités des parties prenantes : le responsable du traitement, les potentiels sous-traitants et les potentiels co-responsables.

Quels sont les référentiels applicables ?

Recensez les référentiels applicables au traitement, utiles ou à respecter, notamment les codes de conduite approuvés et certifications en matière de protection des données.

Base de connaissances

Principe

Description du traitement

Définition

Responsable de traitement

Définition

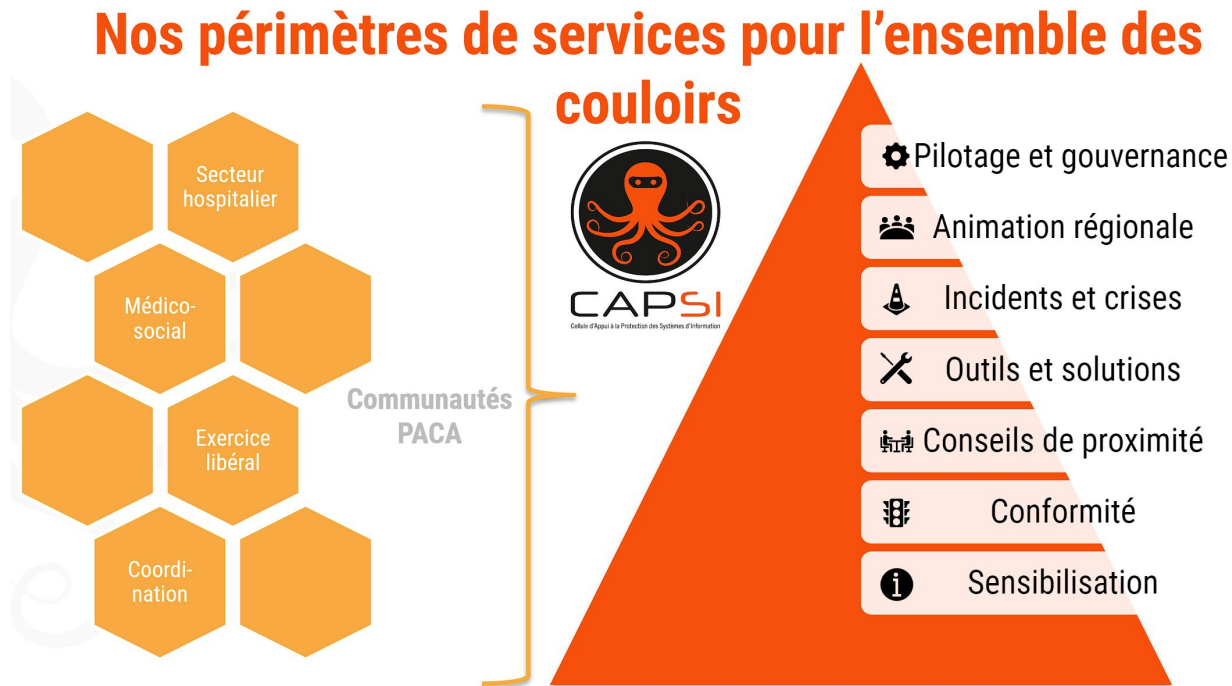
Sous-traitant

La conformité numérique dans mon établissement : sur qui m'appuyer en région PACA ?

Conformité numérique et cybersécurité : quels appuis et outils en PACA ?

Le centre régional PACA de ressources en cybersécurité et conformité numérique : **CAPSI**

Une cellule d'appui à la protection des systèmes d'information portée par le GRDeS PACA et créée à l'initiative de l'ARS PACA et des communautés régionales



Conformité numérique et cybersécurité : quels appuis et outils en PACA ?

Le centre régional PACA de ressources en cybersécurité et conformité numérique : **CAPSI**

Quelques outils à disposition de tous les couloirs

Une cellule d'appui à la protection des systèmes d'information portée par le GRADeS PACA et créée à l'initiative de l'ARS PACA et des communautés régionales

CYBERSÉCURITÉ - Les bonnes pratiques (1 sur 5)



Plateforme régionale de formation et de sensibilisation à la sécurité numérique



Kits de formation Hygiène numérique



Offre régionale de sécurité des échanges



Supports de sensibilisation



Vos Interlocuteurs CPAM/ARS/GRADES pour le Ségur numérique en santé en Région PACA

Une seule adresse pour vous accompagner : pilotage@segur-numerique-paca.fr

- Pour toute question générale relative au pilotage du Ségur du numérique en santé (gouvernance, feuille de route, planning,...)
- Pour l'expertise Technique e-santé et l'accompagnement des professionnels de santé dans la transition numérique
- Pour les demandes d'habilitation au SI Pilotage, la montée en charge de l'alimentation des DMP, la sensibilisation du personnel au sein des établissements



Nous contacter : Innovation e-Santé Sud



capsi@ies-sud.fr



<https://capsi.tech>



Page LinkedIn : <https://www.linkedin.com/showcase/capsi-paca>



Merci pour votre attention !