RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Provence-Alpes Côte d'Azur

Sécurité sociale L'Assurance Maladie

ieSS Innovation e-Santé Sud

LE PARTENAIRE NUMÉRIQUE DES ACTEURS DE SANTÉ

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

SÉGUR DU NUMÉRIQUE EN SANTÉ

La conformité numérique

Présentation du 25/11/2022

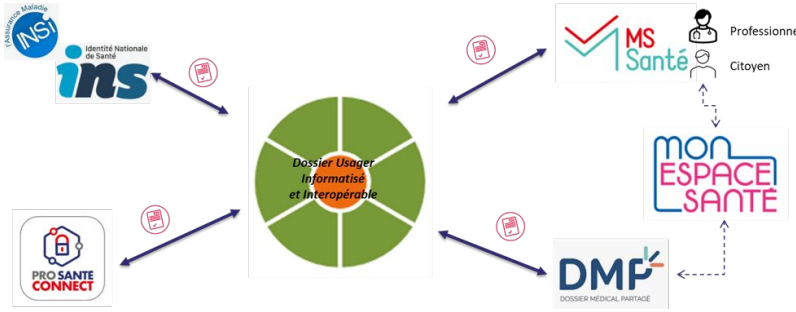
Financé par l'Union européenne NextGenerationEU

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 ?

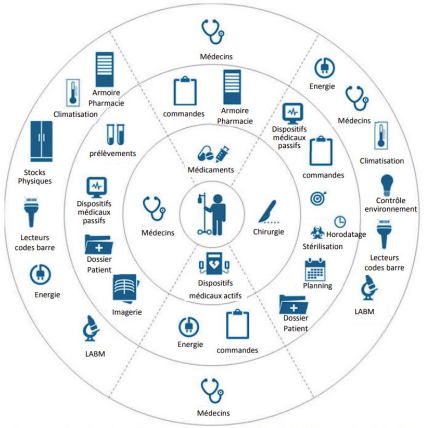
Un environnement numérique grandissant dans nos structures

Le numérique omniprésent à proximité de l'usager



- 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

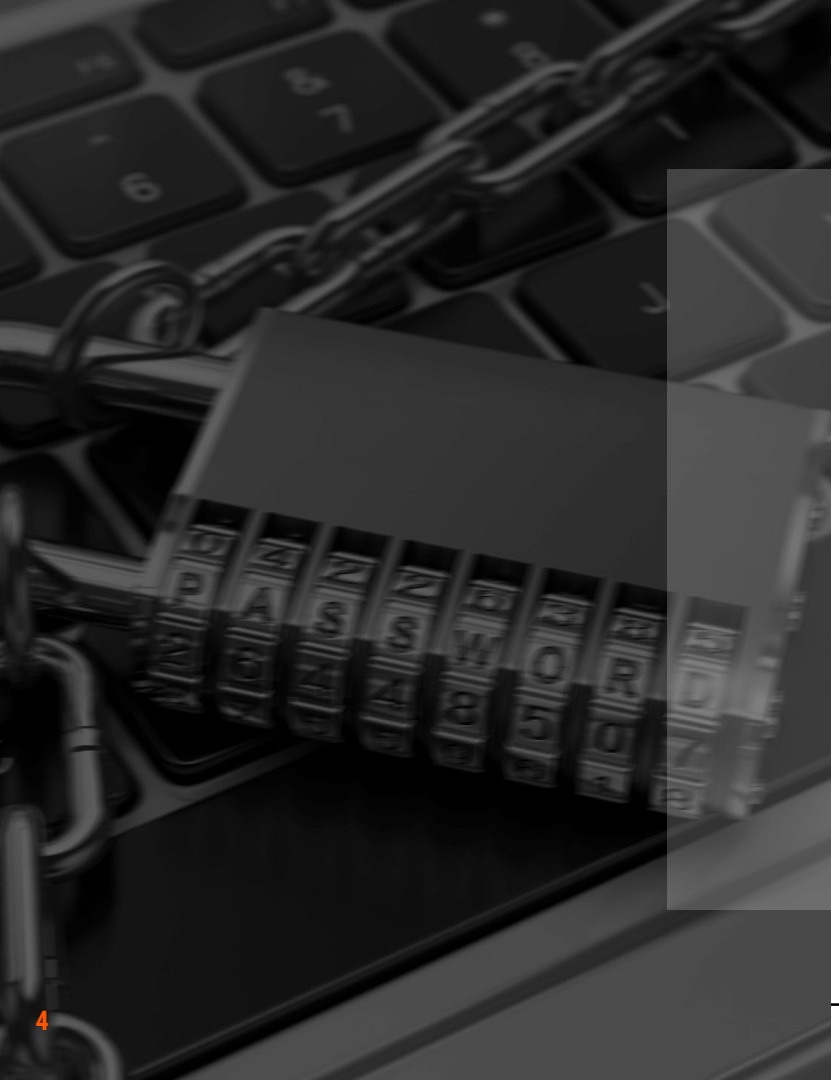
- Une évolution constante des risques concernant les données
- Un enjeu collectif où la sécurité numérique est l'affaire de tous
- Favoriser la création d'un espace numérique de confiance



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

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

Une fonction : gouverner la sécurité numérique de nos structures



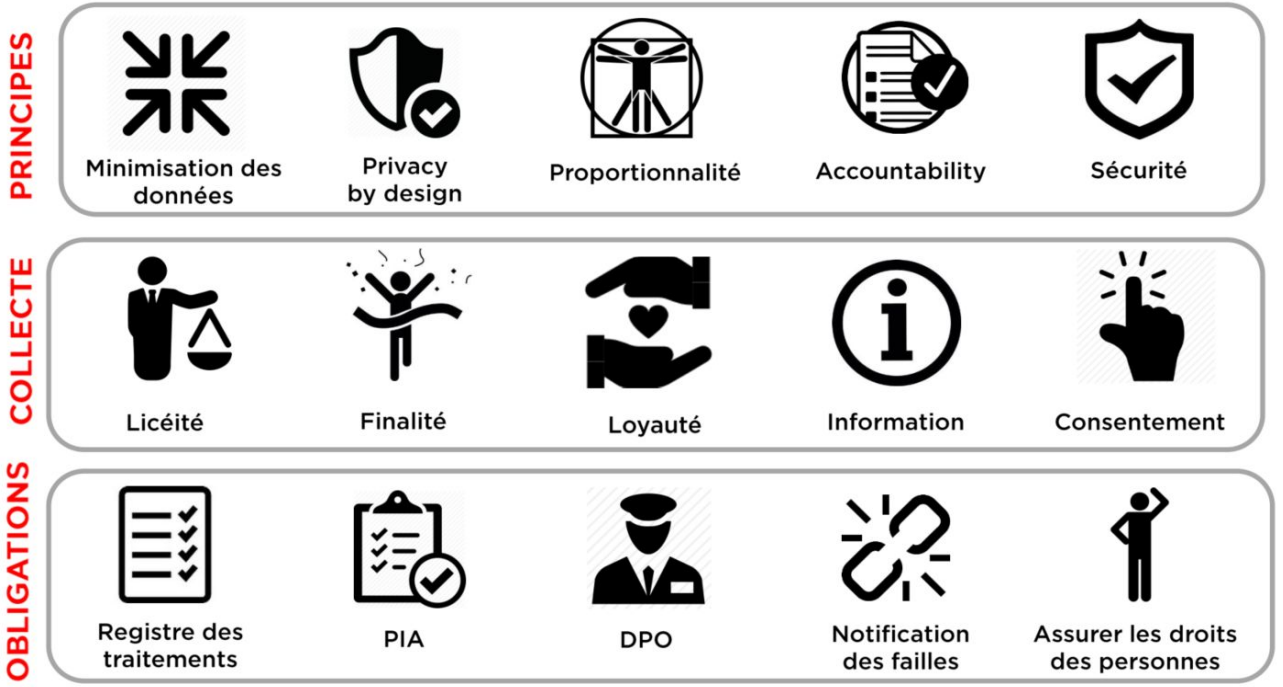
Conformité numérique

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

Financé par l'Union européenne NextGenerationEU

Conformité numérique et gouvernance des données

Rappels des principes et obligations



Financé par l'Union européenne NextGenerationEU

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 Référent DPO			
Nom des outils			
Traitement hors UE			

SI LE TRAITEMENT EST SOUS TRAITE

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)

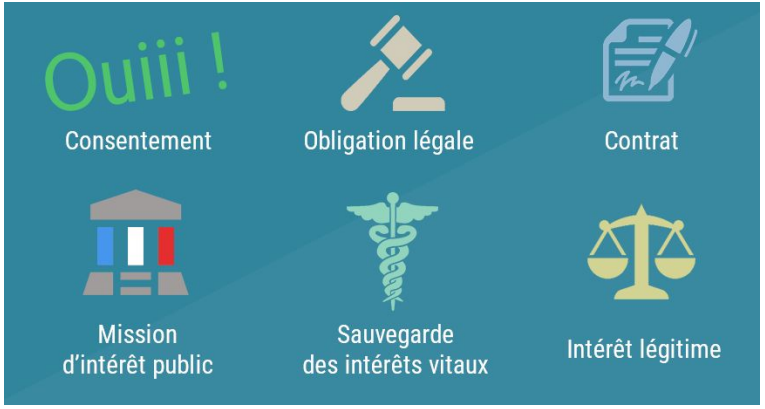
- fondé sur le consentement préalable de la personne physique ;
- fondé sur l'exécution d'un contrat avec la personne physique concernée ;
- fondé sur une obligation légale à laquelle le responsable du traitement est soumis ;
- fondé sur la protection des intérêts vitaux de la personne concernée ;
- 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	État civil, identité, images ? Vie personnelle ? Vie professionnelle ? Economique et financier ? Données de connexion ? Données de localisation ? Internet ? Autres ?
Sensibilité	NON
Durée de conservation	

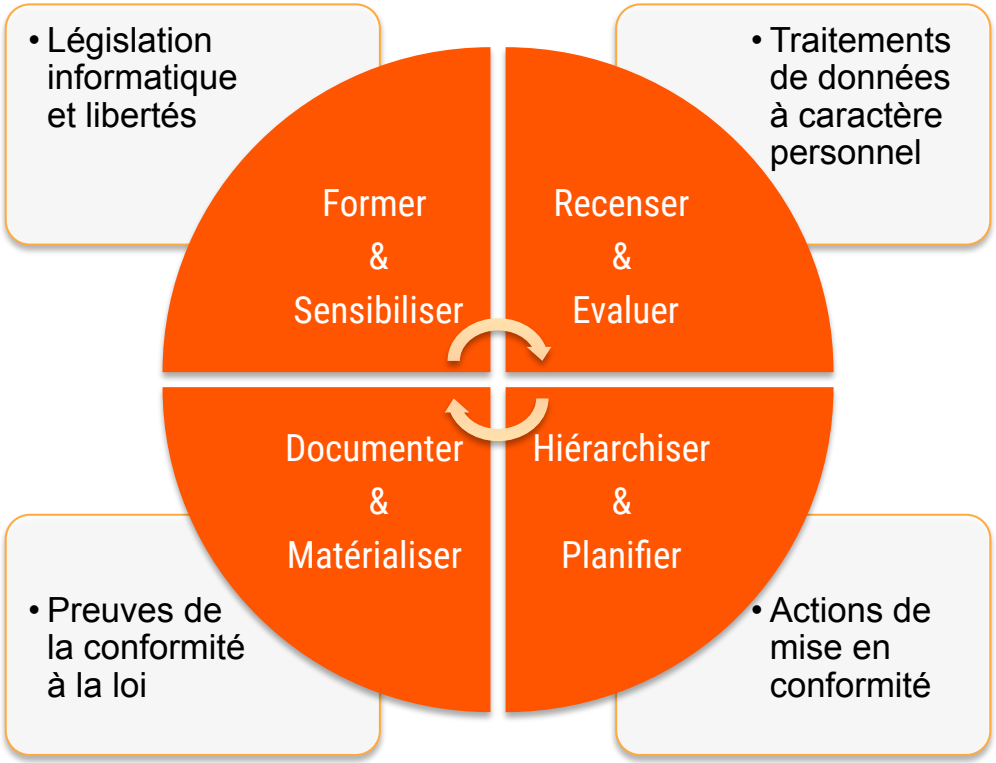
CATEGORIE DES DESTINATAIRES DU TRAITEMENT



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

Financé par l'Union européenne NextGenerationEU

Une mise en œuvre itérative et permanente de la conformité numérique



Financé par l'Union européenne NextGenerationEU

Collecte de données

Recommandations

Les bonnes pratiques à mettre en œuvre :

- Inscrire les traitements au registre obligatoire et vérifier leur légalité
- Limiter les collectes au st *collecte de données?)*
- Informer les répondants *(r les supports de collecte)*
- Ne pas réutiliser les donn utre usage *(détournement)*
- Ne pas diffuser les donné rés dans le traitement initial *(y compris en interne)*
- Supprimer ou archiver les on 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

Financé par l'Union européenne NextGenerationEU

Collecte de données

Conformité de votre site institutionnel

Source et infographie : www.sarbacane.com

Financé par l'Union européenne NextGenerationEU

Source : DIDOMI,

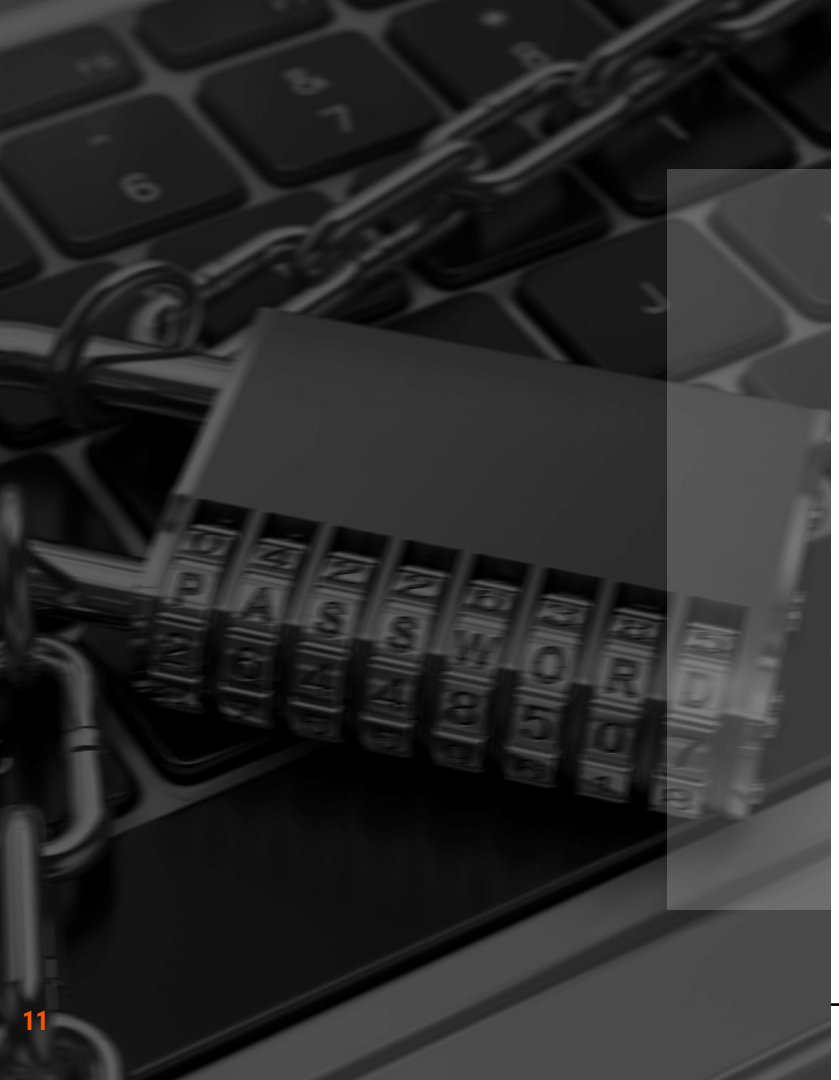
Collecte de données depuis votre site

Le cas des cookies et traceurs de navigation

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

- ☐ **R**évocable
- ☐ **U**nivoque
- ☐ **L**ibre
- ☐ **E**claire
- ☐ **S**pécifique

Financé par l'Union européenne NextGenerationEU



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)

Financé par l'Union européenne NextGenerationEU

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.

Financé par l’Union européenne NextGenerationEU

L'analyse préalable d'impacts requise par la réglementation

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

Sécurité SI

ETUDE D'IMPACT OBLIGATOIRE si le traitement de données figure sur la liste des PIA obligatoires ou si il rempli 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)*	Données sensibles ou hautement personnelles *(santé, géolocalisation …)*	Personnes vulnérables *(patients, personnes âgées, enfants …)*
Décision automatique avec effet légal	Collecte à large échelle	Usage innovant *(utilisation d'une nouvelle technologie)*
Surveillance systématique	Croisement de données	Exclusion du bénéfice d'un droit ou d'un contrat

DPO **RSSI**

Financé par l'Union européenne NextGenerationEU

Règlementation de protection des données

Les implications dans le secteur sanitaire

Sécurité SI

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

|

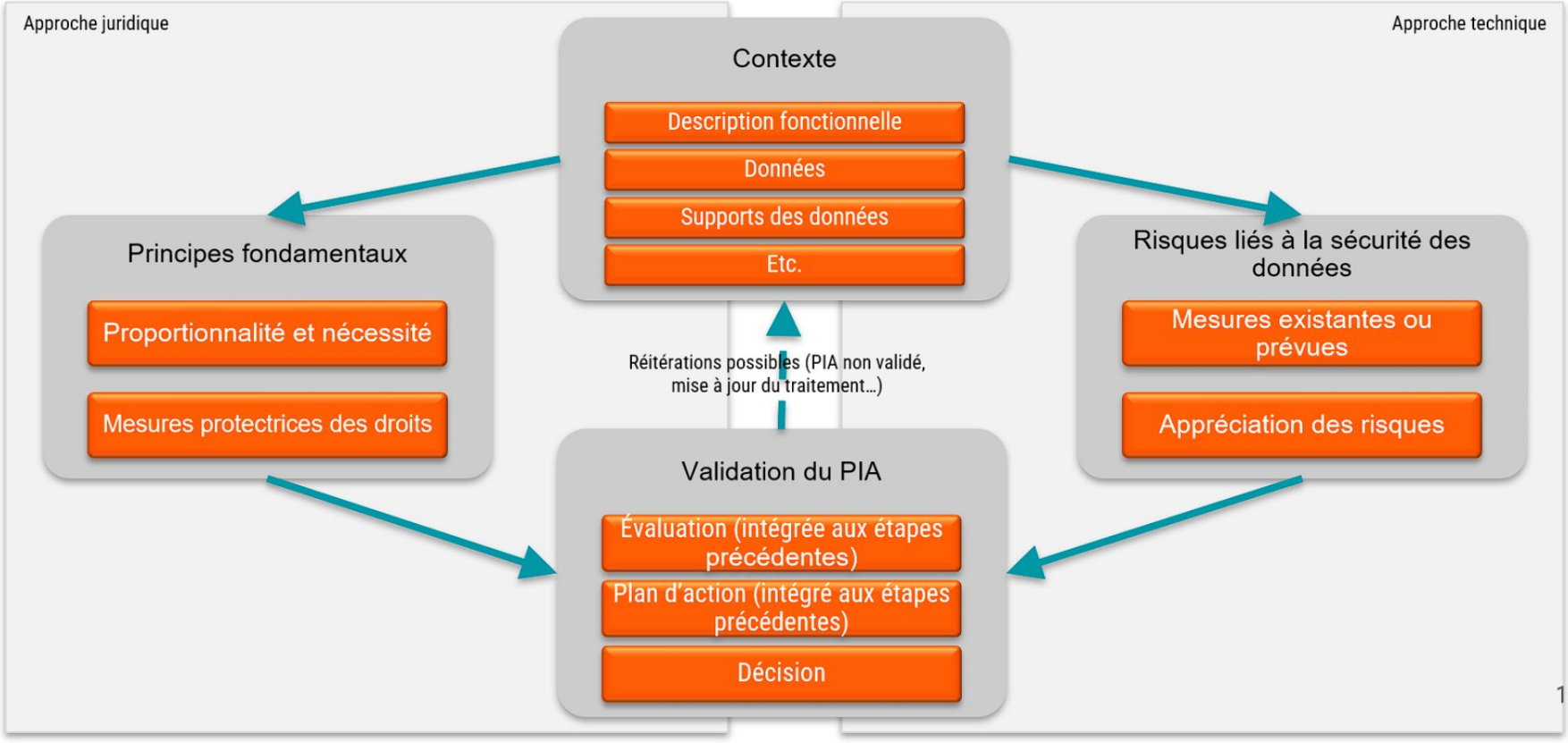
Une prescription pour la majorité des traitements de données de santé

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

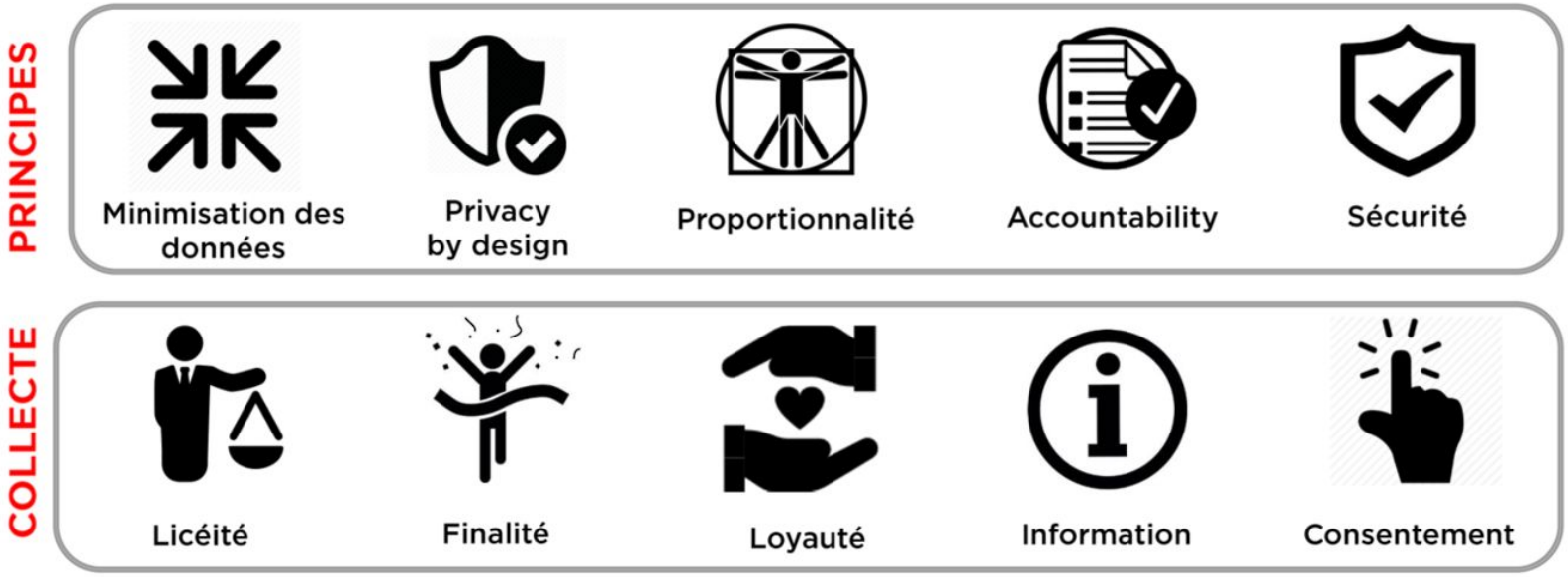
Types d'opérations de traitement	Critères issus des lignes directrices du CEPD qu'ils remplissent	Exemples
Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes.	- collecte de données sensibles - personnes dites « vulnérables »	- traitements « de santé » mis en œuvre par les établissements de santé (hôpital, CHU, cliniques, etc.) : • dossier « patients » ; • algorithmes de prise de décision médicale ; • dispositifs de vigilances sanitaires et de gestion du risque ; • dispositifs de télémédecine ; • 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 (EPHAD).
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.

Financé par l'Union européenne NextGenerationEU

Analyse d'impact obligatoire : quelle méthodologie ?



Analyse d'impact obligatoire :
PHASE 2 : l'évaluation du respect du droit?



Analyse d'impact obligatoire :
Phase 3 : l'évaluation des risques ?

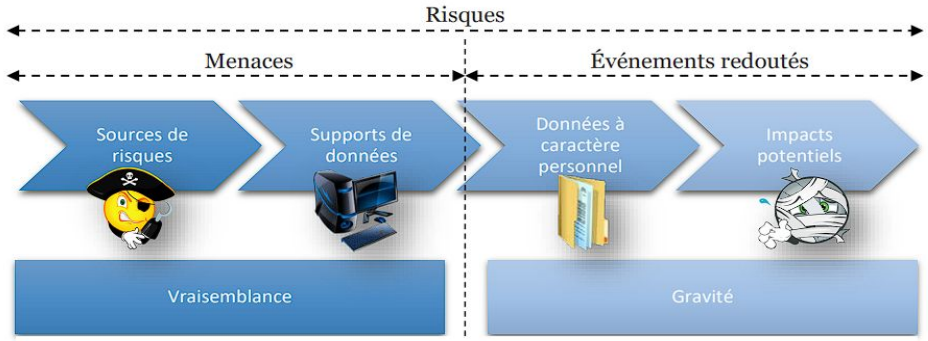


Figure 3 – Éléments composant les risques

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 potentiels[15] ;
- 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.

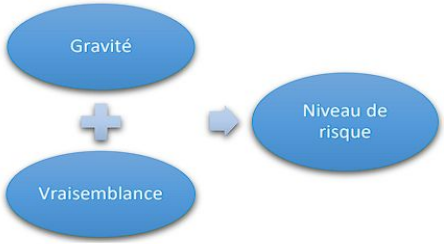


Figure 4 – Éléments permettant d'estimer les risques

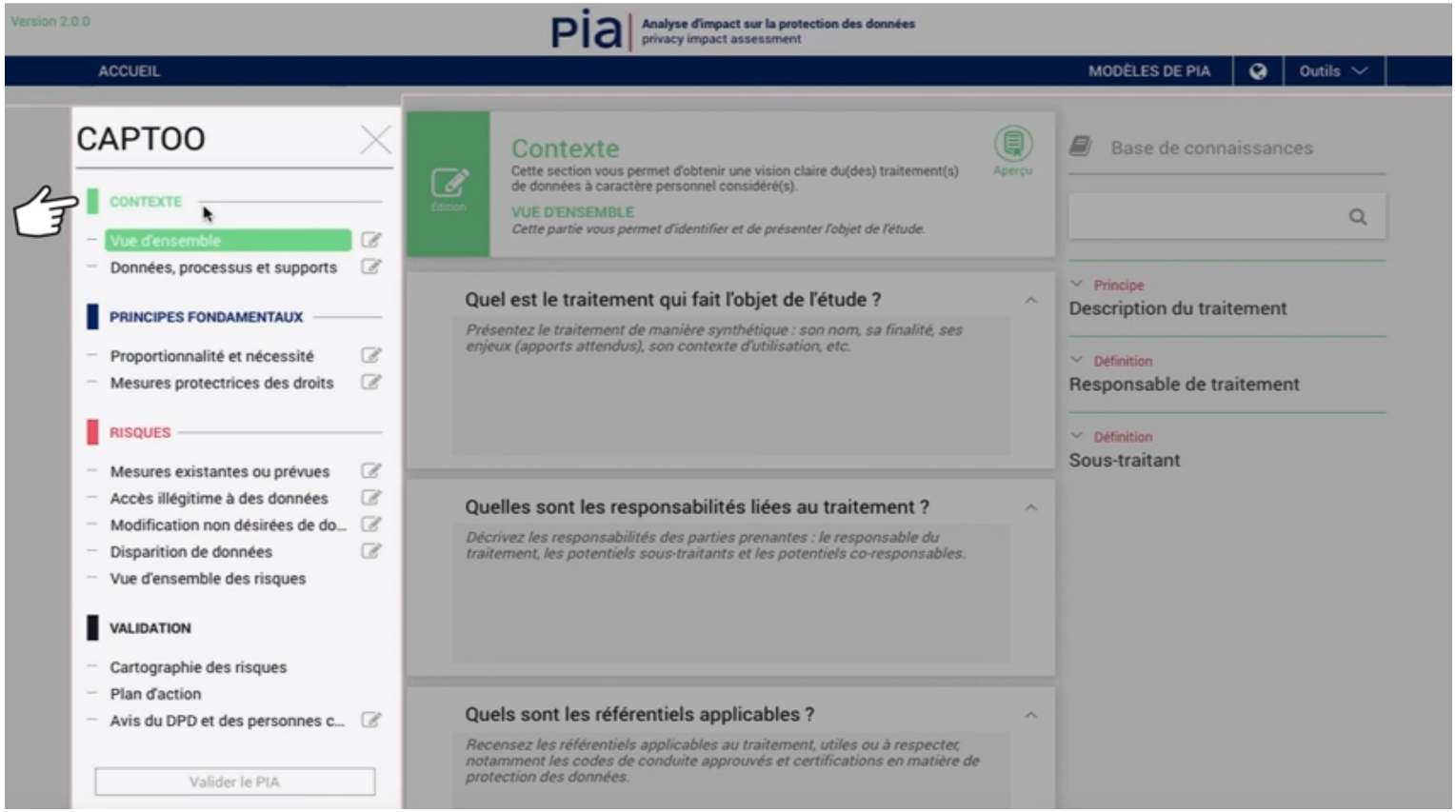
Impacts sur :

- ✔ La disponibilité de la donnée ;
- ✔ L'intégrité de la donnée ;
- ✔ Confidentialité de la donnée

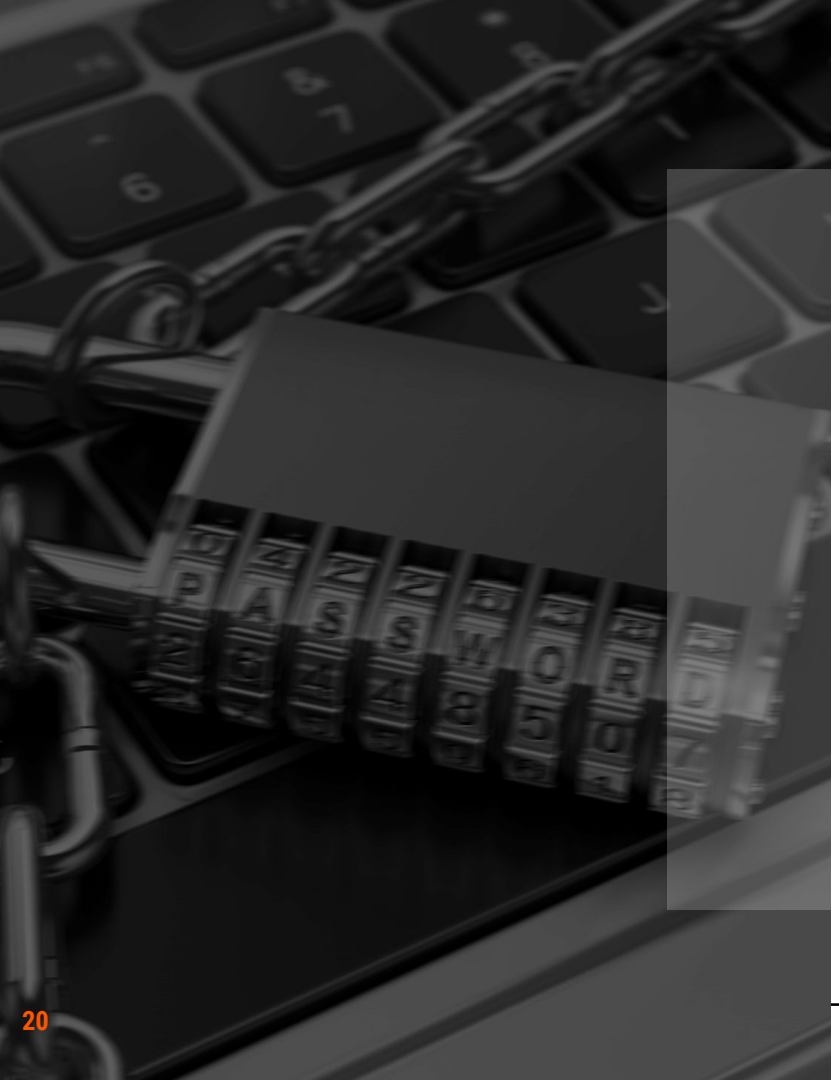
Analyse d'impact obligatoire :
Les outils disponibles ?

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

Outil CNIL PIA : les grandes étapes



Financé par l'Union européenne NextGenerationEU



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

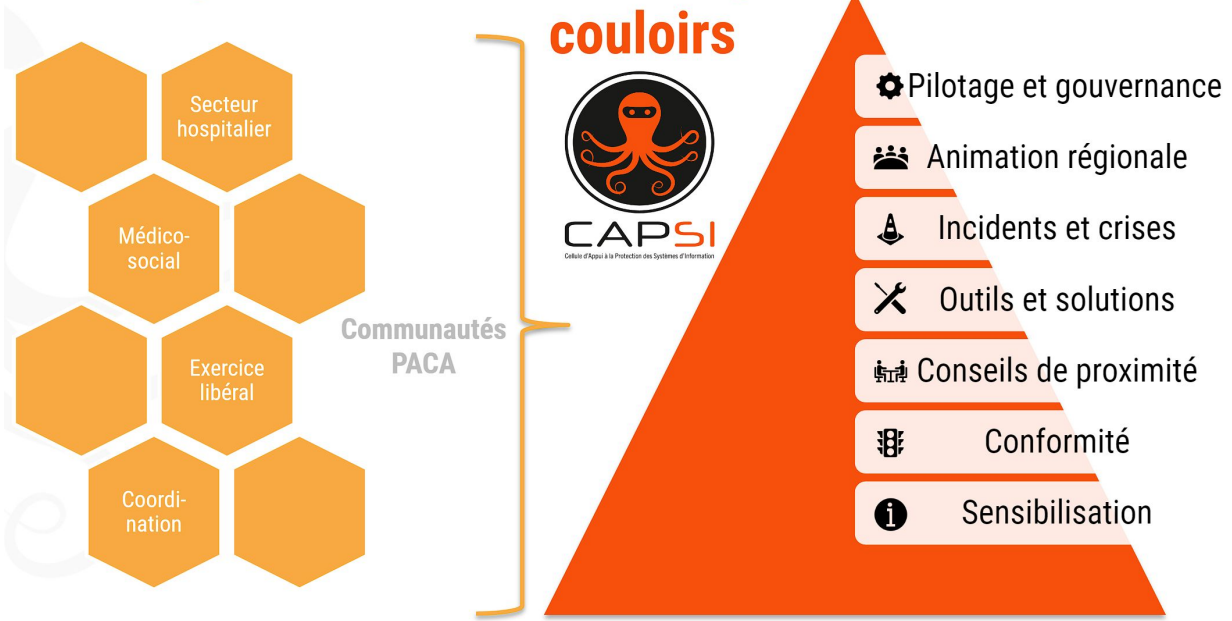
Financé par l'Union européenne NextGenerationEU

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 GRADeS PACA et créée à l'initiative de l'ARS PACA et des communautés régionales

Nos périmètres de services pour l'ensemble des couloirs



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 GRADeS PACA et créée à l'initiative de l'ARS PACA et des communautés régionales

Quelques outils à disposition de tous les couloirs

Plateforme régionale de formation et de sensibilisation à la sécurité numérique

Escape game Crack'n Hack

Offre régionale de sécurité des échanges

Pep'S Proximité Échange Performance Sécurité

Kits de formation Hygiène numérique

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'accompagnent 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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Provence-Alpes Côte d'Azur

Sécurité sociale L'Assurance Maladie

ieSS Innovation e-Santé Sud

LE PARTENAIRE NUMÉRIQUE DES ACTEURS DE SANTÉ

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

Merci pour votre attention !