e-santé Occitanie
Connecter pour mieux soigner

Première rencontre du club des DRSI

4 Mai 2021

Les thèmes de notre rencontre

RGPD

Règlement Général de Protection des données

Le 25 mai 2018, le règlement européen est entré en application. De nombreuses formalités auprès de la CNIL disparaissent. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité. [Source : CNIL]

Identitovigilance

INS : Identité Nationale de Santé

Identité Nationale de Santé
ins
Bien identifié·e, bien soigné·e.

RGPD

Cadre réglementaire et démarche de mise en conformité RGPD

Nadège MACE – Institut des Jeunes Aveugles

31 - Haute-Garonne, 81 - Tarn, 82 - Tarn-et-Garonne

02

Retour d'expérience sur une démarche de mise en conformité au RGPD dans des structures médicosociales

Olivier MUSSEAU – GCSMS ISI

34 – Hérault

03

Aspects techniques du RGPD / prospective : l'exemple de la block chain

Stéphane SAINT-ALME – Association le Clos du Nid

48 - Lozère

04

Captation d'images et études comportementales

Hervé BAROU-CROUTZAT – ADAPEI des Hautes Pyrénées

65 - Hautes-Pyrénées

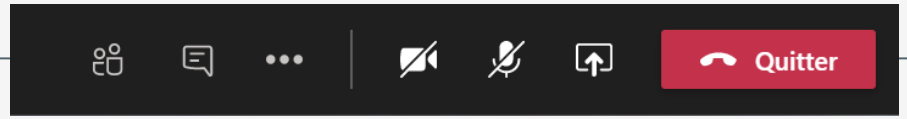
Identitovigilance

Identitovigilance et INS : fondamentaux et aspects techniques

Christine LECLERCQ, Isabelle STACH et Loïc PANISSE

GRADeS Occitanie

Les règles du jeu de cet atelier à distance…



- **LORSQUE VOUS N'INTERVENEZ PAS, COUPEZ MICRO ET CAMERA.** Cela évitera les bruits parasites et les confusions pour ceux qui souhaitent s'exprimer.
- **VOUS POUVEZ POSER VOS QUESTIONS DANS LE TCHAT AU FUR ET A MESURE DE LA PRESENTATION**. Les questions seront traitées après chaque présentation.
- **LORSQUE VOUS VOULEZ PRENDRE LA PAROLE, SIGNALEZ-LE** en levant la main et en rallumant votre caméra. Confirmez en levant la main que vous souhaitez prendre la parole.

Main levée, caméra allumée

> Vous souhaitez réagir

- Une fois la parole donnée, **N'OUBLIEZ PAS D'OUVRIR VOTRE MICRO.**
- **PRESENTEZ-VOUS** afin que ceux qui sont par téléphone puissent vous identifier également.

Groupe de travail DRSI

4 mai 2021

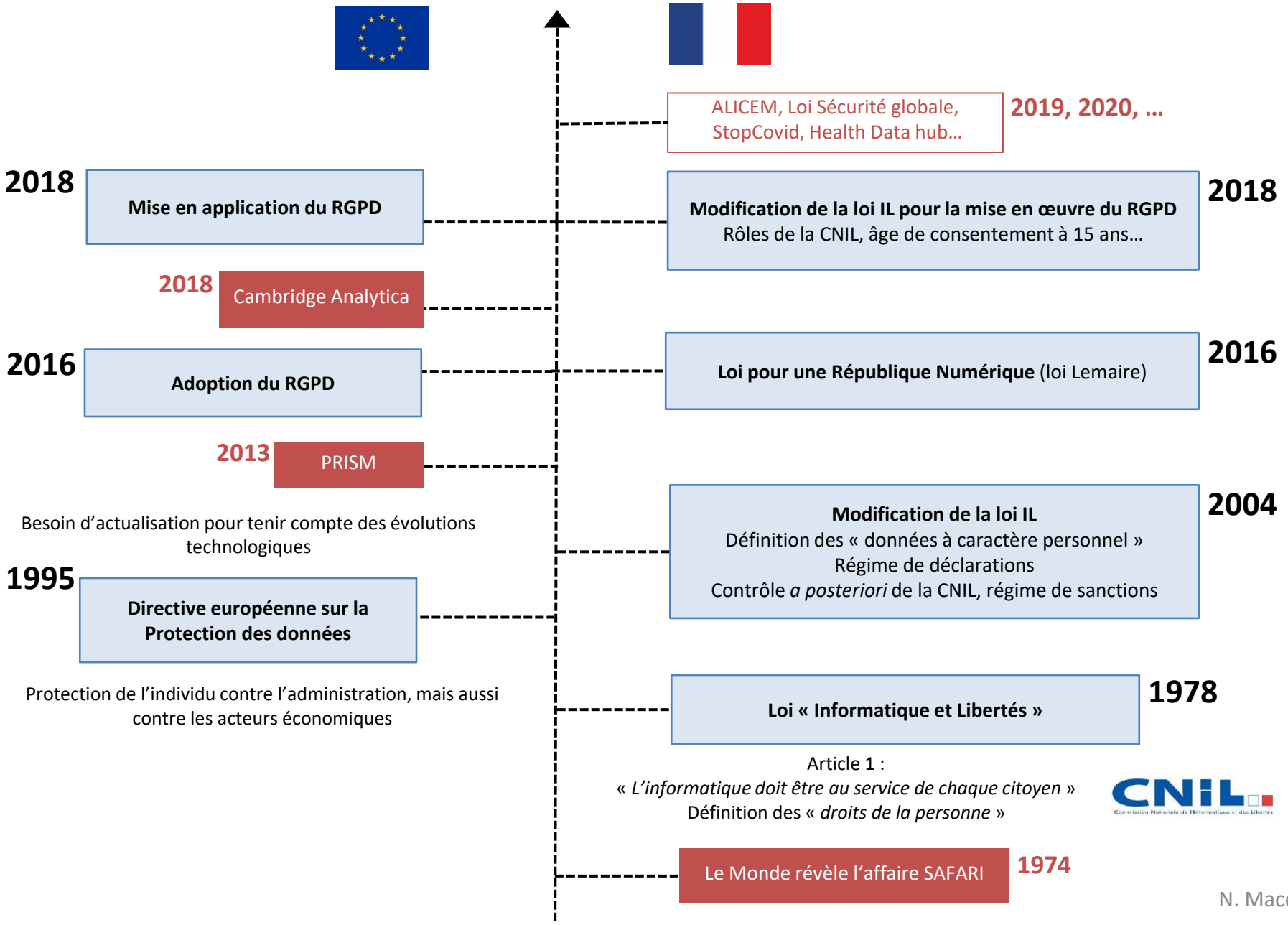
Cadre réglementaire et démarche de mise en conformité RGPD

Entrée en vigueur le 24 mai 2016

Mise en application le 25 mai 2018

- Nadège Macé -

Un peu de contexte



Les objectifs

Réagir face aux violations répétées des GAFA

Renforcer le droit des personnes

Responsabiliser les responsables de traitement

Uniformiser les règles dans les pays européens

Faciliter la libre circulation des données

Renforcer les sanctions

RGPD : Qu'est ce qu'une donnée à caractère personnel ?

Article 4 RGPD :
« *Toute information relative à une personne physique identifiée, ou qui peut être identifiée, de manière directe ou indirecte, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* »

Nom, prénom, photo

Numéro de téléphone, adresse IP, numéro de SS, adresse mail, numéro de châssis de voiture, enregistrement vocal…

Même si son identification n'est possible que par des recoupements hypothétiques avec d'autres informations détenues par des tiers avec lesquels vous n'avez aucune relation.

Les données personnelles sensibles sont un ensemble spécifique de « catégories spéciales » qui doivent être traitées avec encore plus de prudence et qui portent sur :

- L'origine raciale ou ethnique
- Les opinions politiques, l'adhésion à un syndicat
- Les croyances religieuses ou philosophiques
- Les données de santé, les données génétiques, les données biométriques...

Gestion des données personnelles : les risques

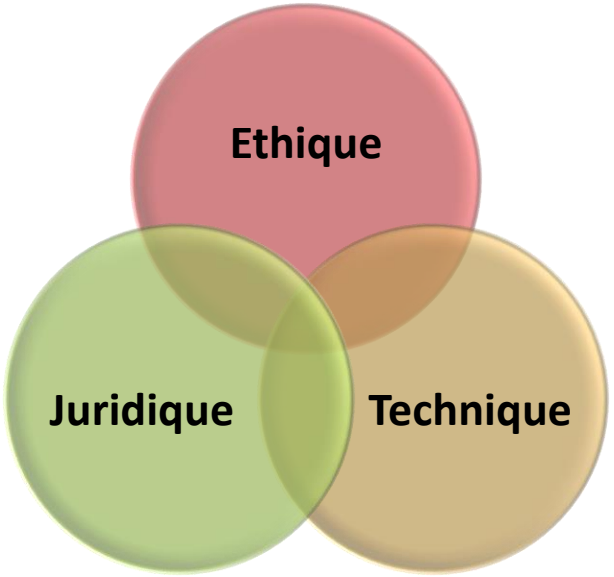
Spécificités du secteur

Impact possible d'une indisponibilité ou d'un manque d'intégrité des données sur la prise en charge des personnes accompagnées

Spécificité des règles de partage et d'échange des données à caractère personnel et des données sociales et de santé, en matière de confidentialité et de traçabilité.

Une personne n'est pas dissociable de ses données.

Le respect qui lui est dû passe aussi par celui des informations qui le concernent



Les supports

Règlement RGPD (11 chapitres, 99 articles) : *Lien*

**Comparatif RGPD/IL : ** https://www.gdpr-expert.eu

MOOC de la CNIL : https://atelier-rgpd.cnil.fr/

Mars 2021 - **Référentiel pour la prise en charge médico-sociale des personnes âgées, en situation de handicap ou en difficulté** : *Lien*

Guide de la sécurité des données personnelles : *Lien*

RGPD : les grands principes (1/2)

	ORGANISER	DOCUMENTER	CONTRÔLER
RESPONSABILISATION Le responsable de traitement prend des mesures efficaces pour se conformer et apporter la preuve que les mesures sont appropriées	✓ Nommer un DPD	✓ REGISTRE des traitements	✓ Réaliser des analyses d'impact
	✓ PROCEDURE de contact du DPD	✓ REGISTRE des violations / incidents (dont SI)	
	✓ PROCEDURE de notification des violations de données	✓ REGISTRE des sous-traitants (hébergeurs, éditeurs côté SI…) et clarification des responsabilités de chacun	
FINALITE, PROPORTIONNALITE ET PERTINENCE Les données collectées et enregistrées sont pertinentes et strictement nécessaires à l'objectif poursuivi. Les objectifs de la collecte sont clairs et compatibles avec les missions de l'organisme et explicitement exposés aux personnes concernées avant toute collecte. Détermine les durées de conservation.	✓ Animer la démarche, sensibiliser, communiquer sur les bonnes pratiques	✓ Pour chacun des traitements, clarifier les « 8 règles d'or » • Licéité du traitement • Finalité du traitement • Minimisation des données • Obligation de sécurité • Protection des données sensibles • Conservation limitée • Transparence • Droit des personnes	

RGPD : les grands principes (2/2)

	ORGANISER	DOCUMENTER	CONTRÔLER
SECURITE Le responsable de traitement doit prendre toutes les mesures nécessaires pour garantir la sécurité des données ainsi que leur confidentialité en évitant leur divulgation à des tiers non autorisés	✓ Sécuriser les réseaux, les sauvegardes, les postes de travail, les locaux, les transmissions… ✓ Politique de sécurité SI (cf PGSSI) ✓ +PCA/PRA	✓ Cartographies fonctionnelle, applicative, technique (préciser les interconnexions et les flux…) ✓ Lister les droits d'accès / habilitations (DIU, bureautique, serveurs…) Identifier les flux d'information en interne et vers l'extérieur. Considérer les données numériques et sur papier	✓ Auditer, contrôler ✓ Tester le mode dégradé
CONSERVATION Les données personnelles sont conservées uniquement le temps nécessaire à l'accomplissement de l'objectif poursuivi.	✓ Identifier les durées de conservation, archiver, détruire		
DROITS et CONSENTEMENT Réviser les procédures visant au respect des droits : Information, accès, rectification, effacement, portabilité. Les procédures de demande de consentement doivent être formulées en des termes simples, clairs et accessibles.	✓ Informer les usagers / salariés /… ✓ Recueillir le consentement des usagers / salariés / … le cas échéant		

Les règles d’or de la CNIL

- Quelles sont les bases légales pour le recueil et l’exploitation des données ?
- Quelles sont les finalités précises ?
- Quelles sont les données concernées, et y’a-t-il parmi celles-là des données sensibles ?
- Quelles mesures de protection sont apportées ?
- Quelle est la durée de conservation (réglementaire le cas échéant) ?
- Quelle procédure d’archivage / destruction ?
- Les personnes sont-elles informées ?
- Le consentement a-t-il été recueilli le cas échéant ?

https://atelier-rgpd.cnil.fr/apprenant/default.php

Des questions ?

03

REX sur une démarche de mise en conformité au RGPD

Club DRSI le 04.05.2021

Au menu du jour…

LE PLAN D'ACTION THÉORIQUE

LE VRAI BILAN À 3 ANS

ECHANGES ENRICHISSANTS ☺

1 MAINTENIR UNE ORGANISATION INTERNE LIÉE À LA PROTECTION DES DONNÉES

2 MAINTENIR UN INVENTAIRE DES TRAITEMENTS

3 VÉRIFIER LA CONFORMITÉ DES TRAITEMENTS

4 MAINTENIR DES DOCUMENTS SUPPORT

5 COMMUNIQUER, SENSIBILISER ET FORMER

6 GÉRER LES RÉCLAMATIONS ET LES CONTENTIEUX

7 GÉRER LES RISQUES DES TIERS

8 GÉRER LES RISQUES DE SÉCURITÉ DE L'INFORMATION

9 GÉRER LES VIOLATIONS DE DONNÉES

10 SUPERVISER ET CONTRÔLER LACONFORMITÉ

« La mise en place d'un système de management de la protection des données à caractère personnel est la clé de voute de la conformité. »

Olivier MUSSEAU – DPO interne, mutualisé, certifié (mais pas que…)

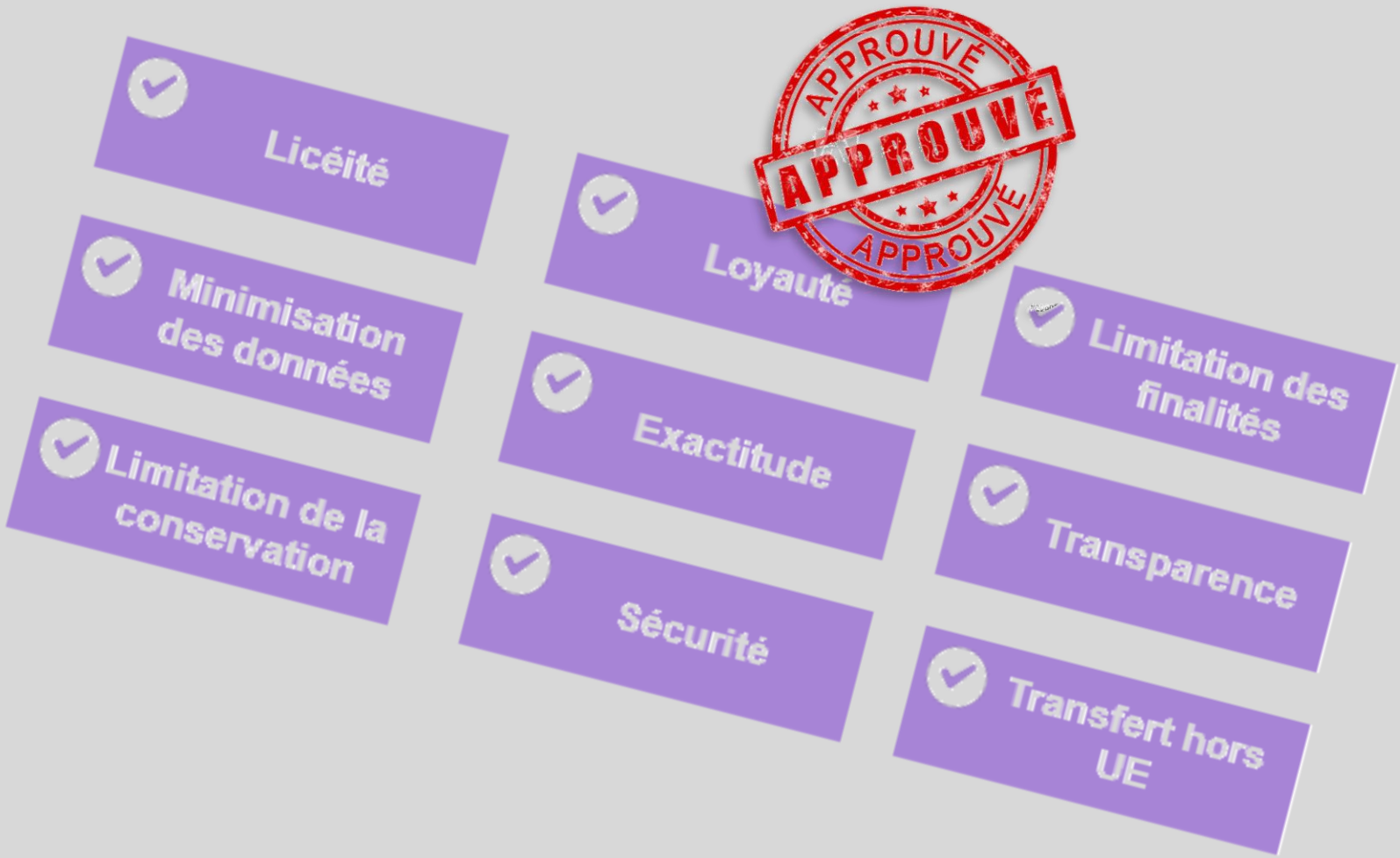
1 MAINTENIR UNE ORGANISATION INTERNE LIÉE À LA PROTECTION DES DONNÉES

- Désigner un DPO (et il n'y a aucun débat possible!)
- Cadrer l'action du DPO : lettre de mission + fiche de poste
- Rédiger une charte interne RGPD
- Constituer le réseau des RIL (Référent Informatique et Liberté = relai local)
- Réaliser un audit, un diagnostic de l'existant avant de débuter la démarche
- Le DPO doit réaliser une veille légale et se former
- Intégrer la protection des données dans la vie des structures : projet d'établissement, documents institutionnels, réponse à un AAP…

2 MAINTENIR UN INVENTAIRE DES TRAITEMENTS

- Réaliser une cartographie exhaustive des traitements à date = la 1ère chose à faire !
- Prévoir ensuite un process qui garantit la mise à jour continue de cette cartographie
- La mission est confiée aux RIL, avec le soutien et la dynamisation du DPO
- L'inventaire alimente le registre des traitements, CQFD ☺
- Ne pas aller plus loin que le rapport d'étonnement à cette étape

3 VÉRIFIER LA CONFORMITÉ DES TRAITEMENTS



4 MAINTENIR DES DOCUMENTS SUPPORT

- Et oui, il appartient au RT de démontrer sa conformité au RGPD…
- Tous les registres doivent être tenus à jour
- Conserver une trace écrite de toutes les actions qui vont dans le sens de la conformité : réunions, formations, campagnes d'info, documents produits…
- Gérer les consentements : don et retrait
- Rédiger les mentions d'information type

5 COMMUNIQUER, SENSIBILISER ET FORMER

- Le RGPD concerne tous les acteurs de la structure !
- Débuter par les sponsors de la démarche : codir, board, cadres…
- Élaborer des supports de référence simples : affiches, flyers, intranet…
- Accompagner les collaborateurs au travers de formations
- Saupoudrer du RGPD dans le quotidien afin de créer une culture de la protection des données

6 GÉRER LES RÉCLAMATIONS ET LES CONTENTIEUX

- Globalement, cela revient la plupart du temps à gérer les exercices de droit des personnes concernées
- La gestion est facilitée par l'existence de procédures et de documents modèles
- En cas de saisine auprès de la CNIL, le DPO sera le médiateur privilégié et désigné
- Les contentieux avec les tiers existent aussi !

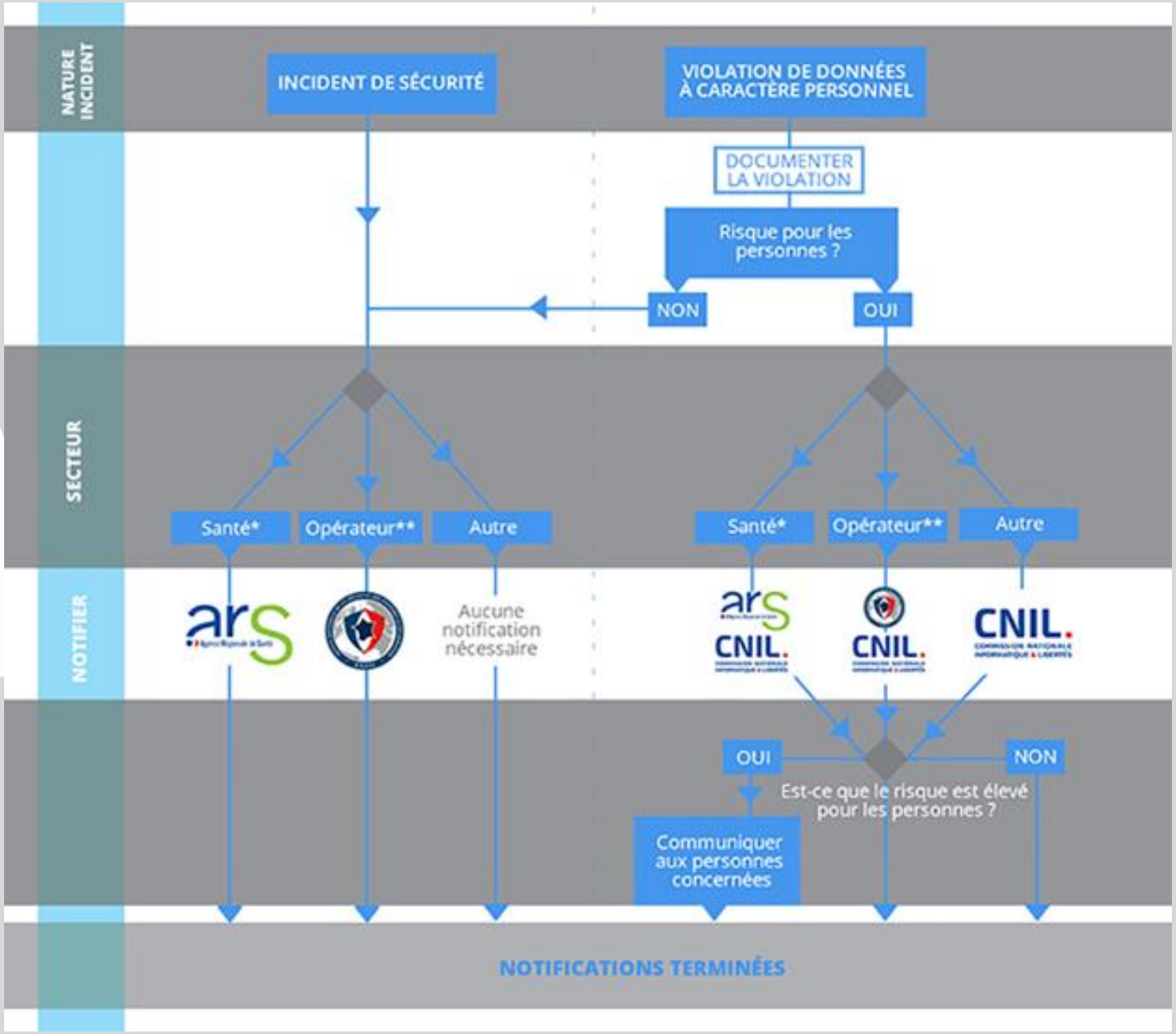
7 GÉRER LES RISQUES DES TIERS

- Tiers = sous-traitant
- Tiers = responsable conjoint
- Tiers = destinataire externe
- Tiers = … il faut donc les recenser dans un registre ad hoc !
- Ne pas confondre avec les tiers autorisés.
- Ne pas confondre avec les PC (Personnes Concernées)
- Réaliser une évaluation des risques auxquels les tiers sont susceptibles d'exposer la structure
- Mise à jour des contrats commerciaux actuels : avenants RGPD

8 GÉRER LES RISQUES DE SÉCURITÉ DE L'INFORMATION

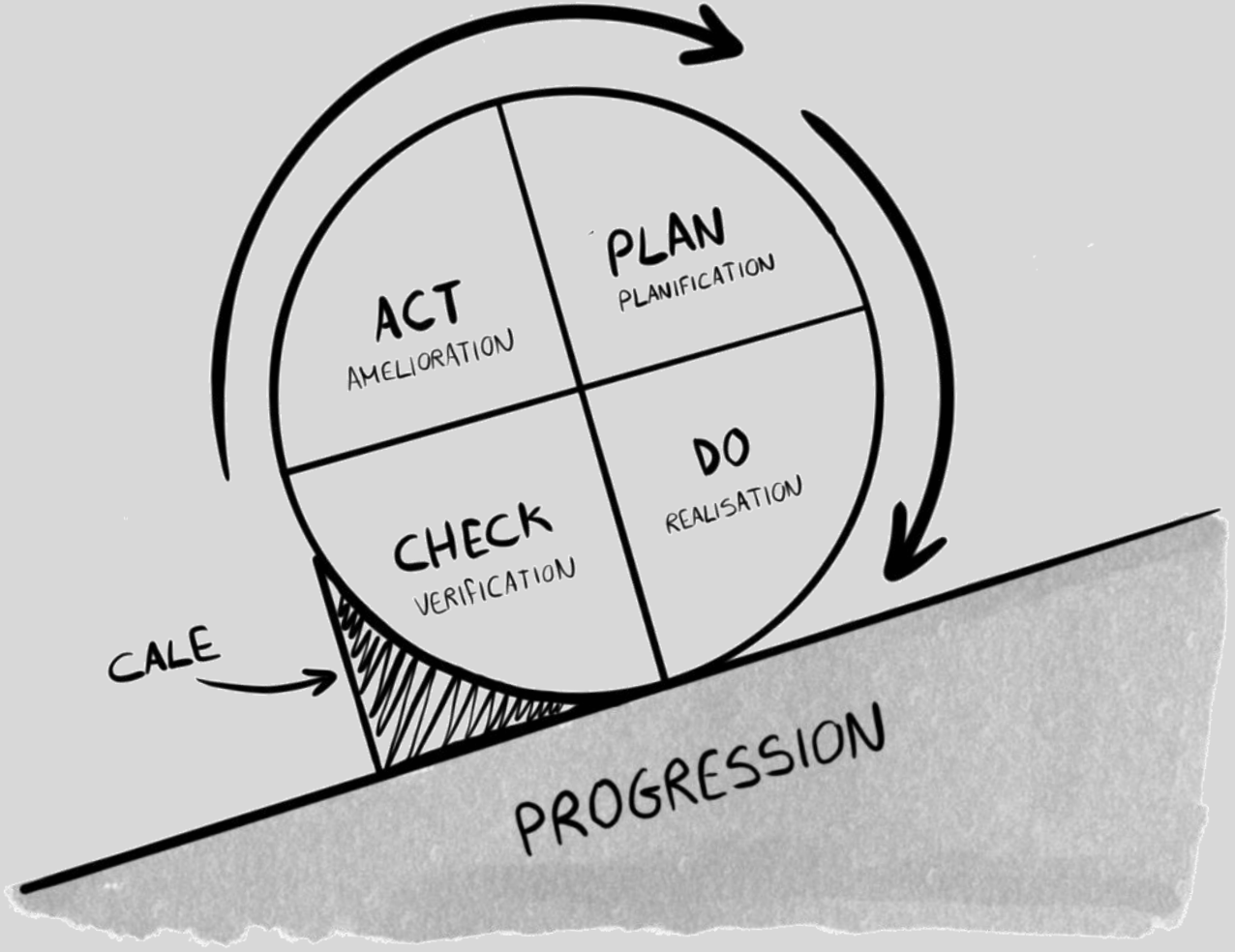
- Postulat de base : le RT doit prendre les mesures nécessaires pour garantir la confidentialité et l'intégrité des données qu'il a collectées
- Intégrer les concepts de *privacy by design* et *privacy by default*
- Réaliser une AIPD à chaque fois que le traitement le nécessite
- Mise en œuvre des sécurités physiques, logiques, logicielles, etc…

9 GÉRER LES VIOLATIONS DE DONNÉES



10 SUPERVISER ET CONTRÔLER LACONFORMITÉ

« Et si la conformité au RGPD se trouvait au centre d'une démarche globale d'amélioration continue ? »



Le vrai bilan à 3 ans

- Pour l'instant, je n'ai pas trouvé l'utilité d'une solution logicielle de gestion de la conformité.
- L'année 2020 a mis la démarche entre parenthèses à cause de la crise sanitaire. Globalement, et comme elle n'est pas prioritaire dans les ESMS, le moindre évènement la met en pause.
- La phase de cartographie est plus longue que prévu… (Réel = 4 X estimation)
- Les RIL font toujours partie des forces vives des organisations, donc des personnes les plus engagées dans les projets, donc les plus sollicitées, donc au final les moins disponibles…
- Le secteur social est plus mobilisé que le médicosocial.
- La démarche a été bien accueillie par les sponsors, pas de frein particulier.
- Des précisions, des recommandations sur l'interprétation du RGPD sortent tous les jours : veille juridique indispensable qui prend du temps.
- Le DPO ne doit pas rester isolé : intégration de réseaux, de clubs…

Le vrai bilan à 3 ans

- La charte RGPD n'est pas rédigée, il y a trop de superpositions avec la charte info et le RI…
- Beaucoup de sollicitations de la part des structures sur les mentions légales à inclure.
- La formation et la sensibilisation doivent être des ritournelles récurrentes : il faut tenir compte du turnover et de l'amnésie des salariés…
- La gestion des tiers est très compliquée, on dialogue avec des personnes qui sont au niveau 0 du RGPD.
- Dans le secteur, presque tous les traitements nécessitent une AIPD ☹
- Zéro attaque, mais des dizaines de pertes/vols d'équipement…
- Déclarer une violation de données à la CNIL et à l'ARS n'est pas un acte neutre de sens ni de conséquences. Généralement, les hautes sphères se mobilisent.
- La mise en place de l'organisation interne dédiée à la protection des données personnelles ne pose aucune difficulté.

Le vrai bilan à 3 ans

- L'analyse de la conformité des traitements est la phase le plus révélatrice des effets de bords positifs de la démarche : détection des doublons, mise en exergue des process ancestraux donc inutiles, ménage dans les archives, remise à plat des droits d'accès…
- Documenter la démarche de conformité nécessite une attention de tous les instants.
- Le travail sur les mentions d'information est très pédagogique, il embarque tout le monde.
- Le consentement n'est plus la solution miracle.
- Avec le temps, le RGPD suscite moins de curiosité, il y a moins de monde aux formations ou aux animations.
- Très peu de demandes d'exercice de droit, souvent liées à des situations conflictuelles décorrélées du RGPD.
- La démarche est un formidable levier pour faire monter la sécurité des organisations en gamme !
- *privacy by design* et *privacy by default* un peu à la traine…
- DPO jamais en porte à faux ! (guideline ET constat)

Echanges enrichissants ☺

RGPD & Blockchain

GT-DRSI ESMS Numériques

Définition & caractéristiques de la Blockchain

La technologie de la confiance numérique

La **blockchain** est une technologie de stockage et de transmission d'informations, **transparente**, **sécurisée**, et fonctionnant **sans organe central de contrôle**.
Par extension, une blockchain constitue une base de données qui **contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création.**
Cette base de données est **sécurisée** et **distribuée** : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun **de vérifier la validité de la chaîne.**

Sécurisée

Les algorithmes de cryptage utilisés dans la blockchain en font l'une des technologies les plus sûres connues de l'Homme à ce jour.

Décentralisée

La blockchain n'est contrôlée par aucun organe central et est répliquée sur des milliers de nœuds qui en ont tous une copie exacte

Immuable

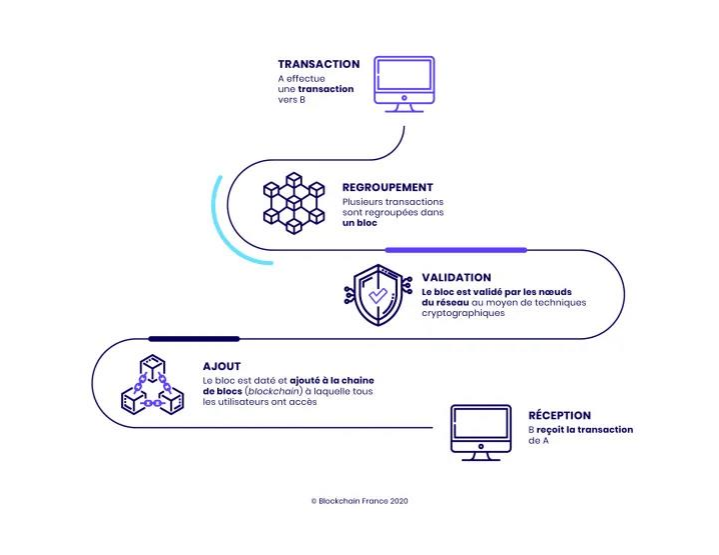
Rien de ce qui a été écrit dans la blockchain ne peut être supprimé ou modifié.

Transparente

Auditable, elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne

Comment fonctionne la Blockchain ?

BLOC 1	BLOC 2	BLOC 3	BLOC 4	BLOC 5
Donnée 10 Donnée 11 Donnée 12 Donnée 13	Donnée 20 Donnée 21 Donnée 22 Donnée 23	Donnée 30 Donnée 31 Donnée 32 Donnée 33	Donnée 40 Donnée 41 Donnée 42 Donnée 43	Donnée 50 Donnée 51 Donnée 52 Donnée 53



[Démo blockchain]

Les potentiels de la Blockchain

Embleema lance le premier carnet de santé en Blockchain et ouvre la voie à la rémunération des données de santé

Rédigé par Communiqué de Embleema le 17 Juillet 2018

Embleema lance la première Blockchain santé destinée aux études en vie réelle, pour connecter patients, communautés médicales et scientifiques. Elle entend devenir la nouvelle référence en termes de sécurité, de transparence, et de qualité en recherche clinique, bouleversant un marché de 140 milliards de dollars.

Accueil > Économie > Conjoncture

La Chine en passe de lancer sa cryptomonnaie nationale

Par la voix de la Banque populaire de Chine, le pays a déclaré que sa monnaie numérique nationale était «opérationnelle».

Par **Harold Grand**
Publié le 12/08/2019 à 18:14, mis à jour le 12/08/2019 à 18:14

AXA se lance sur la Blockchain avec fizzy

AXA est le premier grand groupe d'assurance à proposer une offre utilisant la technologie blockchain. Découvrez fizzy, une plateforme d'assurance paramétrique 100% automatisée, 100% sécurisée, permettant de couvrir les retards d'avion.

ACTUALITÉS
13 SEPT. 2017

ACCUEIL › ÉCONOMIE

Euro numérique : Comprendre le projet de nouvelle monnaie européenne en sept questions

ARGENT Face à la montée des monnaies virtuelles comme le BitCoin ou Libra de Facebook, la Banque centrale européenne veut mettre en place sa propre monnaie numérique

Blockchain en santé : le registre patient distribué

(source BlockchainPartner)

Enjeux du registre

Sécurité des données
- Protection contre le vol de données,
- Protection de la vie privée,
- Protection de l'intégrité des données.

Interopérabilité
- Problème d'interopérabilité des SI entre les institutions de santé : coûteux, pas conçus pour interagir, ...
- Rapidité de la transmission des informations

Moderniser

Interopérabilité
- Une blockchain où tous les participants du système de santé : hôpitaux, patients, établissements de santé résoudrait les problèmes d'interopérabilité (standardisation des données, ...

Analyses des données
- Du fait de l'accessibilité et de la transparence de la Blockchain, l'analyse Big Data des données serait facilitée pour la recherche, les pouvoirs publiques, … afin d'en déterminer des traitements, des politiques de prévention.

Respect de la vie privée et reprise de contrôle sur les données
- Les données standardisées stockées sur la BC resteraient limitées à certains types de données (cf section suivante)
- Le patient reste maître de ses données via sa clé privée (droits d'accès, monétisation, …)

Assurances et Smart-Contract
- Remboursement de santé automatique via smart-contract si les données de santé répondent aux conditions requises.
- Lutte contre la fraude à l'assurance maladie

Collecte des données
- Par les professionnels de santé
- Via les objets connectés sur la base de l'accord du patient

Défis à relever

Défis techniques
- Développement de la blockchain : comment inciter les participants à la validation des blocs ?
- Nécessité de coupler une architecture traditionnelle avec la Blockchain.
- Sécurité des informations non stockées dans la Blockchain
- Engorgement du réseau créé par les micro-transactions

Défis pratiques
- Comment accéder aux données du patient si celui-ci est inconscient, en crise, … compte tenu qu'il est nécessaire de disposer de sa clé privée (désignation de personnes de confiance, …)

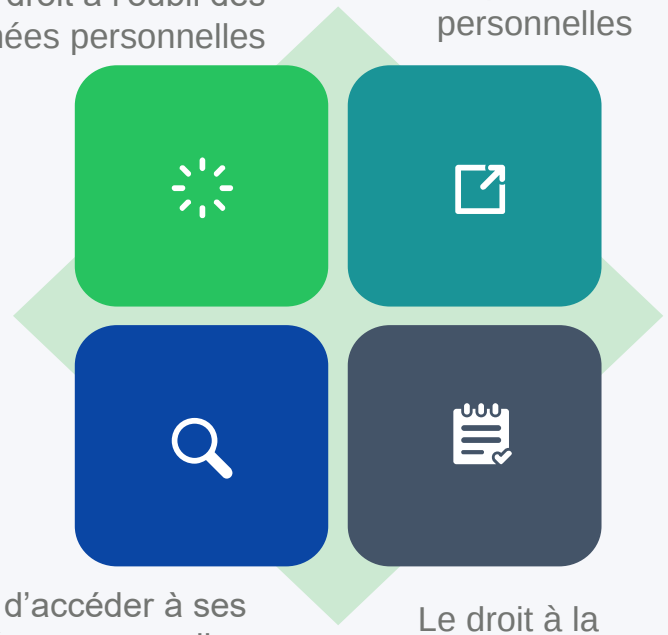
Défis culturels et réglementaires
- Le secteur de la santé souffrant d'un certain retard en matière de numérique, les projets rupturistes comme la Blockchain se heurteront à des freins culturels importants
- Le secteur de la santé est très réglementé, avec des variations fortes d'un pays à l'autre (gestion des identités à l'échelle européenne)
- Le RGPD

Le paradoxe Blockchain / RGPD en Santé (1/3)

Les caractéristiques en jeu

Le droit à l'oubli des données personnelles

La portabilité des données personnelles



Le droit d'accéder à ses données personnelles

Le droit à la modification des données personnelles

RGPD

Sécurisée

Les algorithmes de cryptage utilisés dans la blockchain en font l'une des technologies les plus sûres connues de l'Homme à ce jour.

Décentralisée

La blockchain n'est contrôlée par aucun organe central et est répliquée sur des milliers de nœuds qui en ont tous une copie exacte

Immuable

Rien de ce qui a été écrit dans la blockchain ne peut être supprimé ou modifié.

Transparente

Auditable, elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne

Blockchain

Le paradoxe Blockchain / RGPD en Santé (2/3)

Similarités et différences

Similarités

Le RGPD et la Blockchain sont tous deux orientés vers la transparence en matière de donnée.

Le RGPD et la Blockchain visent à renforcer les droits individuels.

Le RGPD et la Blockchain ont pour objectif de renforcer la sécurité des données personnelles.

Différences

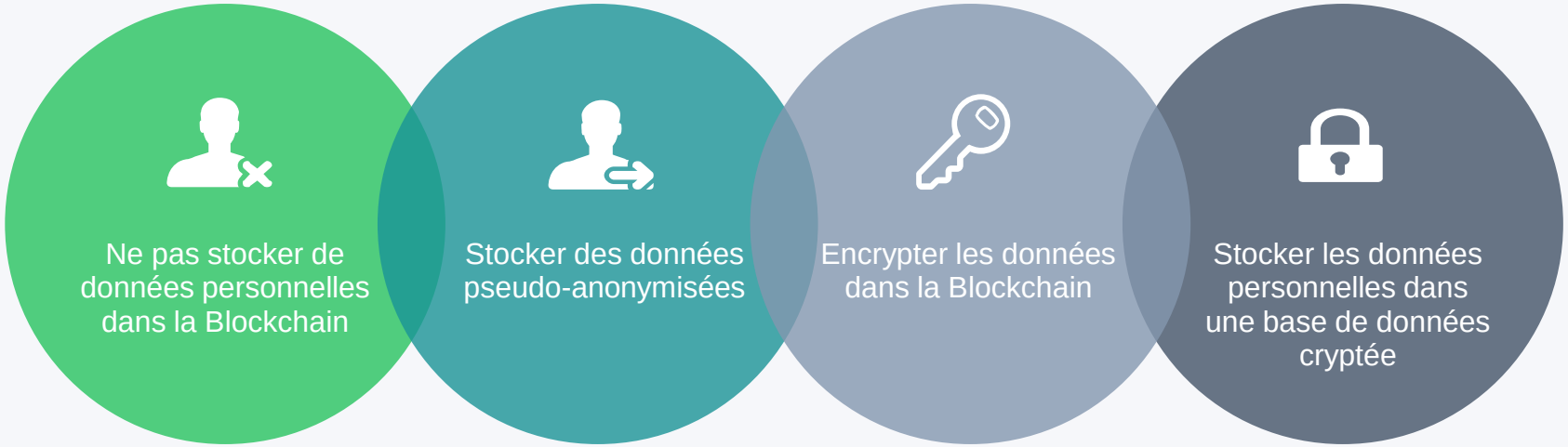
La Blockchain est immuable alors que le RGPD donne aux utilisateurs le droit d'effacer ou de modifier leurs données personnelles.

Le RGPD est conçu de manière à être géré par un système centralisé plutôt que décentralisé comme le DLT.

Le RGPD nécessite l'identité de l'utilisateur alors que la Blockchain est fondée sur l'anonymat.

Le paradoxe Blockchain / RGPD en Santé (3/3)

Les solutions



Cette solution diminue fortement l'intérêt de la Blockchain pour des applications publiques telles que le DMP, ...

Seules les données qui ne peuvent pas être liées à une personne en particulier peuvent être stockée (régime alimentaire, centres d'intérêt, ...)

Pour satisfaire les principes du RGPD, la clé de cryptage doit
- être « brûlée » en cas d'exercice du droit à l'oubli,
- être confiée à l'utilisateur qui ne dispose pas toujours des moyens d'éviter une compromission

- Un hash de la base peut être intégré à la Blockchain pour prouver qu'elle n'a pas été modifiée.
- Les clés de cryptage / décryptage de la base peuvent être intégrées à la BC
- Les enregistrements de la base sont modifiés au gré de l'exercice des droits RGPD

Des questions ?

Retour d'Expérience

Captation d'image et études comportementales

I. Contexte de survenue de l'événement

- Accueil en FAM de résidents présentant des troubles du comportement récurrents nécessitant des adaptations de l'accompagnement (soins, interventions psychologue…),

- Une culture RGPD présente mais à développer au sein de notre association et plus généralement auprès de tous les professionnels de terrain dans le Médico-Social,

- Une politique RGPD en cours (Cabinet HAAS, DPO, Registre CNIL, Fiches Traitements ….),

- Documentation qualité en cours de construction sur cette thématique.

II. Description chronologique de l'événement

- Demande du psychologue d'utiliser un caméscope pour filmer des situations de travail

- Précisions concernant les situations de travail évoquées :
  - « Filmer la passation de certaines évaluations afin de les visionner dans un second temps et en extraire des préconisations.
  - « Travailler sur des évènements spécifiques, pas toujours observables par l'ensemble de l'équipe (Ex : situation se présentant tard le soir, le week-end, etc….) ».
  - « Vidéos destinées à un usage interne. »

- Demande du directeur de se rapprocher de la qualiticienne pour explorer la situation au regard du droit à l'image

III. Analyse de l'événement du point de vue

A – Réglementaire

Prise en compte des référentiels existants concernant la gestion des données et le droit à l'image :

- Article 9 du RGPD - Traitement portant sur des catégories particulières de données à caractère personnel,

- Référentiel de la CNIL applicable aux acteurs du secteur social et médicosocial (Délibération n° 2016-094 du 14 avril 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre dans le cadre de l'accueil, l'hébergement, l'accompagnement et le suivi des personnes handicapées et des personnes âgées.),

- Contrat conclu entre l'ADAPEI des Hautes Pyrénées et la personne accompagnée.

Des recommandations concernant le droit à l'image insuffisantes à encadrer les pratiques liées à l'utilisation de caméras (ou téléphones) en vue de filmer des situations liées à l'accompagnement médico-social.

Analyse de l'événement du point de vue

B- Humains

- Des personnels peu au faite des recommandations et textes de loi
- Peu d'acculturation dans le domaine de l'utilisation des images à usage médical.

C- Organisationnel

- Absence de procédure permettant d'asseoir les bonnes pratiques dans ce genre de situation

- Les formulaires de recueil de consentement d'utilisation des images différents en fonction de l'usage et/ou des établissements

IV. Mise en œuvre

- Elaboration d'une procédure « **Captation vidéo aux fins d'observation comportementale** »,
- Création d'un formulaire **« droit à l'image : autorisation de captation vidéo »**,
- Elaboration d'un formulaire unique **« autorisation droit à l'image »** reprenant la totalité des situations envisageables,
- Diffusion des documents via la GED « **Ageval** »,
- Etude en cours pour la mise en place prochainement d'un stockage chez un hébergeur **agréé données de santé.**

Des questions ?

03

e-santé Occitanie
Connecter pour mieux soigner

Identitovigilance et INS

Fondamentaux et aspects techniques

01

Les grands principes
Les enjeux

Organisation au sein de e-santé

Contexte

- Mise en place du Référentiel National d'Identito Vigilance (RNIV)
- Obligation réglementaire d'utiliser l'identité nationale de santé (INS) pour référencer les données de santé dans les secteurs sanitaire et médico-social, entrée en vigueur le 1er janvier 2021

→ il existe donc 2 volets liés : opérationnel et technique

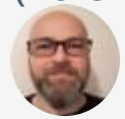
ivo3 identitovigilance
e•sante Occitanie

Qui contacter au sujet de l'IdentitoVigilance ?

Le point d'entrée à privilégier est la Cellule **IVO3** (IdentitoVigilance : Organisation Opérationnelle en Occitanie) qui propose un accompagnement à la mise en place des bonnes pratiques

identitovigilance@esante-occitanie.fr

Elle est constituée d'un référent médical (Dr Christine LECLERCQ) et d'un référent administratif (Loïc PANISSE)



Après analyse de la demande, son statut permettra de transmettre la question vers Isabelle STACH (DUSI), s'il s'agit d'une problématique plutôt technique.

Apport d'IVO3 au sein d'e-santé

En coordination avec le service juridique et les responsables RGPD

- Réponses aux questions internes / **FAQ**
- Orientation lors de la mise en place des nouveaux SI, ou les évolutions des anciens
- Alerte éditeurs en vue d'une autorisation CNDA (INS)

ivo3 identitovigilance
e•sante Occitanie

Mise à disposition d'une bibliothèque documentaire

A consulter sur **l'espace-utilisateurs IVO3**, sur le site e-santé Occitanie, ou sur demande :

- Liens vers les sites nationaux dans leur partie dédiée à l'IV (ANS, DGOS, ANAP, ARS, ...)
- Supports documentaires nationaux (textes et référentiels), y compris soumis à consultation
- Documents régionaux (référentiel, modèle de charte, auto-évaluation, guide d'audit...)
- Kit de communication (flyers, fiche de présentation, et prochainement MOOC)

Les vigilance sanitaires

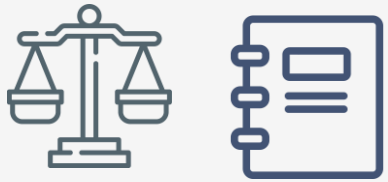
Définition

Les vigilances sont organisées autour de processus continus de recueil, d'analyse et de diffusion standardisés de données portant sur des événements sanitaires et/ou indésirables. Elles ont une finalité d'alerte, de gestion et de prévention des risques (sur la base de signalements).

Le champ actuel de ces vigilances

Au niveau réglementaire, l'ANSM (Agence Nationale de Sécurité du Médicament et des produits de santé) a en charge huit vigilances différentes. Elles sont définies dans le code de la santé publique et à l'heure actuelle leur liste est la suivante :

- Pharmacovigilance
- Pharmacodépendance
- Hémovigilance
- Matériovigilance
- Réactovigilance
- Biovigilance
- Cosmétovigilance
- Vigilance des produits de tatouages



La prochaine vigilance prévue

L'Identitovigilance

Les enjeux de l'identitovigilance

Importance de l'Identitovigilance

La sécurisation du parcours de santé d'un usager nécessite sa bonne identification, élément incontournable devant la multiplicité des étapes de prise en charge disponibles, pouvant potentiellement accroître le risque de survenue d'évènements indésirables graves

L'identitovigilance doit être la première étape d'une démarche qui se prolongera tout au long de la gestion de son dossier par les différents intervenants médicaux, paramédicaux, médico-techniques, médico-sociaux ou sociaux

Au même titre que les autres vigilances, elle devrait devenir réglementaire

Les risques

La confusion entre dossiers médicaux peut-être génératrice d'évènements indésirables potentiellement dangereux, voire mortels :

- Existence d'allergies à certains médicaments
- Erreurs de prescriptions médicamenteuses
- Chirurgie non appropriée (mauvais côté, mauvaise indication d'intervention…)
- Examens biologiques et/ou radiologiques faits et/ou ne se référant pas au bon patient
- …

Le vocabulaire de l'identitovigilance

Les traits

Ce sont les attributs qui permettent de reconnaitre une personne

Ces traits peuvent être :

- **Stricts (ou obligatoires)** = constants / invariables dans le temps (comme une date de naissance)
- **Complémentaires** = soumis à variations (comme une adresse), mais pouvant aider dans l'identification

Les traits obligatoires (à renseigner / nécessaires pour une bonne identification) font partie des traits stricts

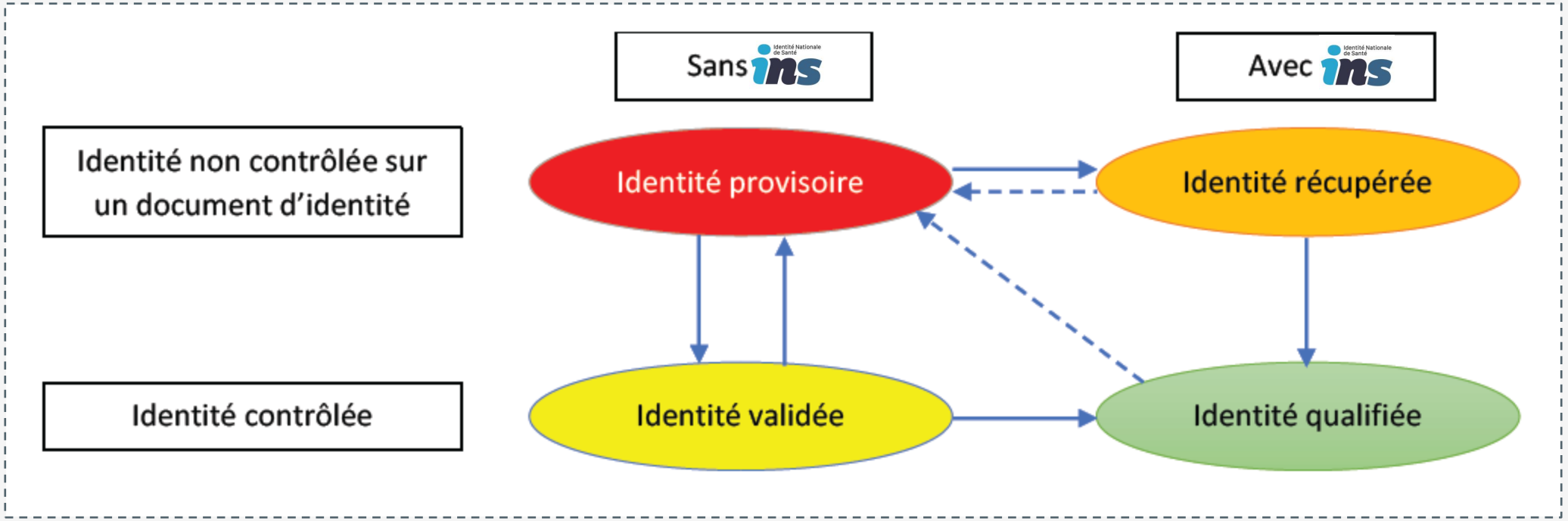
Les situations

Il s'agit des états critiques dans lesquels les identités peuvent se retrouver

- **Doublon** = un même patient a plusieurs dossiers différents, sous plusieurs numéros d'identification locale différents

- **Collision** = dans un même dossier (sous le même identifiant) les informations médicales de plusieurs patients différents sont enregistrées
- **Identités erronées ou incomplètes** = nombreuses situations possibles allant de l'usurpation d'identité aux inexactitudes dans la saisie des identités

Les statuts de l'identité



La sécurisation des identités

Introduction de l'INS

L'Identité Nationale de Santé ou INS permet de référencer les **données de santé** et regroupe :

- le Numéro d'Inscription au RNIPP : Répertoire National d'Identification des Personnes Physiques (NIR ← INSEE) ou le Numéro d'Identifiant en Attente (NIA / assurés nés à l'étranger, en attente d'une identification NIR)
- associé aux traits obligatoires d'identité

Les traits obligatoires

Ils permettent de s'assurer que l'identité de la personne est cohérente avec le patient qui se présente pour un soin ⇨ ***le bon dossier pour le bon patient***

Ils sont constitués de traits stricts :

- Nom de naissance
- Prénom de naissance
- **Liste des prénoms de naissance**
- Date de naissance
- Sexe
- Lieu de naissance (nom de la ville + **code géographique INSEE**)

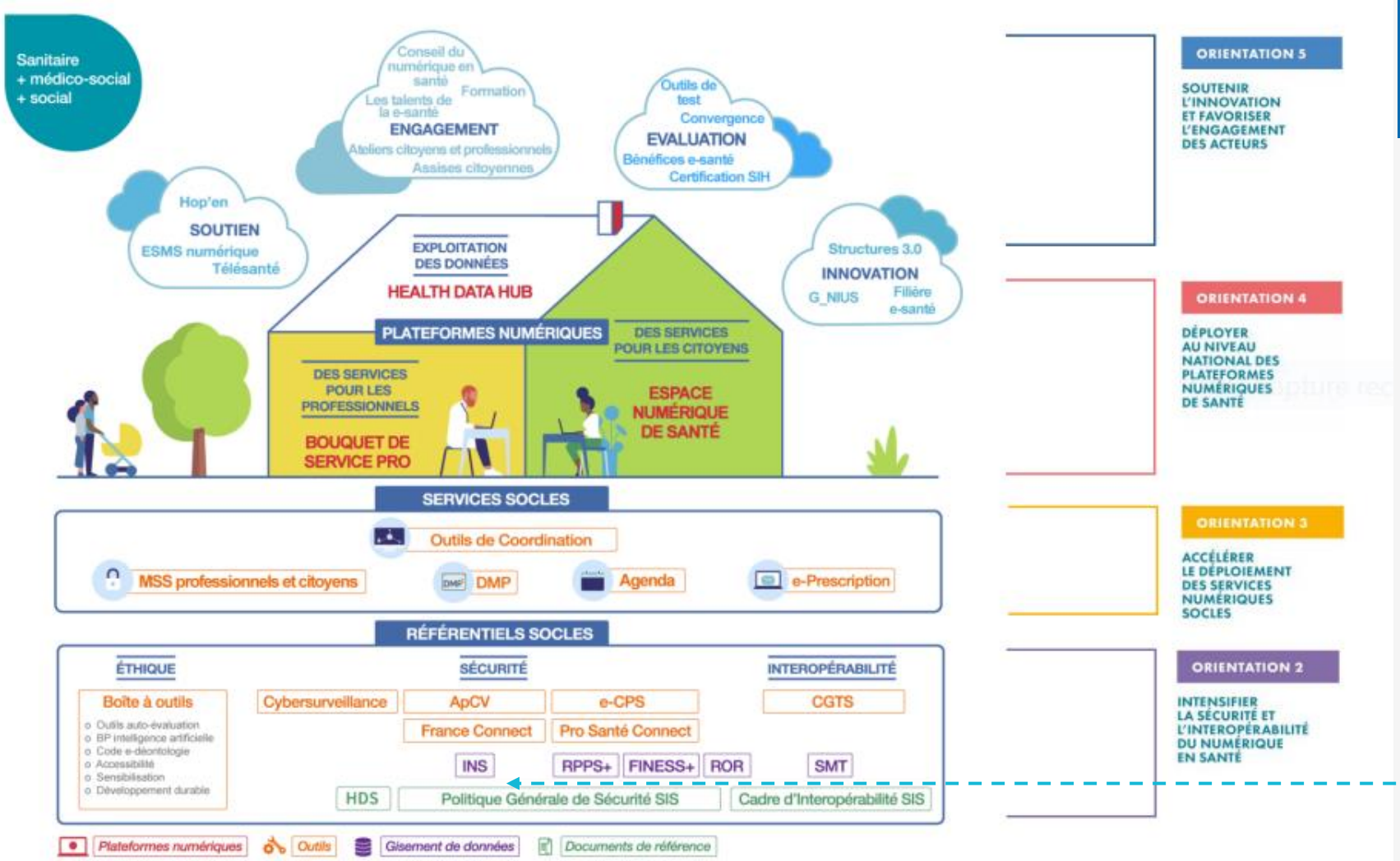
?

Questions

02

l’Identité Nationale de Santé (INS)

Feuille de route du numérique en santé 2019-2022



AGENCE DU NUMÉRIQUE EN SANTÉ

ivo3 identitovigilance
e-santé Occitanie

Identité Nationale de Santé
ins

L'Identité Nationale de Santé

Pour qui ?

Toute personne née sur le sol français et/ou bénéficiaire de l'assurance maladie dispose d'un INS.
Cet identifiant est unique et propre à chaque usager.

Pourquoi ?

- SÉCURISER LE RÉFÉRENCEMENT DES DONNÉES DE SANTÉ
- FAVORISER L'ÉCHANGE ET LE PARTAGE
- AMÉLIORER LA QUALITÉ ET LA SÉCURITÉ DE LA PRISE EN CHARGE

Qui peut utiliser l'INS ?

L'utilisation de l'INS est restreinte à un cercle de confiance de professionnels de la santé et du médico-social impliqués dans la prise en charge du patient

Secteurs concernés :

- Sanitaire
- Médico-social
- *Social (mais non prioritaire)*

Quand ?

À PARTIR DU 1ER JANVIER 2021,
obligation d'utiliser l'identifiant national de santé (INS)
(Décret n°2019-1036 du 8 octobre 2019)

Cette obligation est contraignante mais non dérogeable

INS

En pratique

L'INS ET LES TRAITS D'IDENTITÉ DOIVENT ÊTRE QUALIFIÉS :

- **Vérification de l'identité** selon les procédures d'identitovigilance mises en place
- **Utilisation du téléservice INSi** pour s'assurer de la conformité avec les bases nationales de référence

Un téléservice proposant deux opérations

1ÈRE OPÉRATION

Récupération de l'INS et des traits d'identité de l'état civil

- Dans le cadre d'une prise en charge d'un patient
- Appel par le professionnel :
  - à partir de la carte Vitale
  - à défaut, à partir des traits d'identité du patient

2ÈME OPÉRATION

Vérification de la cohérence de l'INS et des traits d'identité transmis par un autre professionnel.

- Dans le cadre d'un échange ou d'un partage de données de santé entre professionnels

Calendrier 2021

Le calendrier sera affiné au cours de l'année 2021

2021

Janv. | Fév. | Mars | Avril | Mai | Juin | Juil. | Août | Sept | Oct. | Nov. | Déc.

01/01/2021

Poursuite des webinaires structures et éditeurs

*Parution note d'information DGOS et abrogation instruction 2013**

Publication DTNS v2.0

Poursuite de l'accompagnement pro-actif des éditeurs par l'ANS et le GIE SV

30 /03 : réunion interrégionale INS

*Publication de l'arrêté opposabilité***

Possibilité de s'identifier électroniquement au TLS INSi comme personne morale

Lancement de la supervision fonctionnelle

Possibilité de s'identifier électroniquement au TLS INSi par Pro Sante Connect (CIBA)

Lancement de la vérification de la conformité des logiciels (phase pilote)

Lancement de la vérification de la conformité des logiciels (ouvert à tous)

Travaux sur l'opposabilité du guide d'implémentation et la mise en œuvre de procédures de vérification de l'application des référentiels

Accompagnement opérationnel (sanitaire et médico-social) / Instruction des problématiques / Généralisation

*Parution de la note d'information N° DGOS/PF2/PF5/2020/202 du 18 novembre 2020 relative à la publication du référentiel national d'identitovigilance des acteurs de santé. Abrogation de l'Instruction DGOS/MSIOS n° 2013-281 du 7 juin 2013 relative à l'utilisation du nom de famille (ou nom de naissance) pour l'identification des patients dans les systèmes d'information des structures de soins

**comprenant le référentiel INS v2.0, le guide d'implémentation v1.0 et le RNIV v1.0 (tous les volets)

Etat de déploiement INS (mars 2021)

Editeurs

81 logiciels autorisés par le CNDA, soit **64** éditeurs

16 éditeurs en cours de test auprès du CNDA

5 éditeurs du médico-social autorisés

Structures / PS

43 solutions déployées, notamment au sein de plusieurs sites pilotes…

(AP- HM / CH Aubagne, CHR Orléans, CH Cahors, GHT Novo, CLCC H. Becquerel)

…et de **2** EHPAD pilotes de Berger Levrault, avec un **REX** prévu début avril

Un **REX** des structures pilotes en cours de rédaction

Corpus documentaire

[Guide d'accompagnement ANS]

Organisation et identitovigilance

Référentiel national d'identitovigilance (RNIV)

Ce document vous permet de prendre connaissances **des règles d'identitovigilance opposables** à tout acteur de santé et à respecter au niveau local

A destination des structures / professionnels de santé (PS)

Comprendre l'INS

Ce document vous permettra de **découvrir / approfondir vos connaissances** sur le projet INS

A destination des structures / professionnels de santé (PS)

Système d'information

Guide d'intégration INSi

Ce document vous permet de consulter les **modalités d'intégration du téléservice INSi** (pour récupérer et vérifier l'INS)

Guide d'implémentation identité INS

Ce document vous permet de consulter **les règles de gestion et les préconisations** pour implémenter au mieux l'identité INS dans l'ensemble des logiciels concernés.

Change Proposal IHE – PAM et annexe du CI-SIS

Ces documents vous permettent de **mettre à jour** vos logiciels **conformément aux évolutions des standards d'interopérabilité**

A destination des éditeurs de logiciels

Juridique / sécurité

Référentiel INS

Ce document vous permet de prendre connaissance de **l'ensemble des mesures de sécurité** qui encadrent le référencement des données de santé avec l'identité INS

A destination de tous

Décret n° 2019-1036 du 8 octobre 2019

Ce texte vous permet de prendre connaissance du décret relatif à **l'utilisation du numéro d'inscription au RNIPP comme matricule INS**

A destination des structures / professionnels de santé (PS)

Corpus documentaire (outils complémentaires)

1 Organisation et identitovigilance

Les fiches pratiques INS

Ce document vous permet de prendre connaissances **des règles d'identitovigilance opposables** à tout acteur de santé, à respecter au niveau local

Liste des référents régionaux IV

Consultez la liste **des référents régionaux d'identitovigilance**

Les webinaires INS

Accédez au replay **des webinaires INS** dédiés aux structures

2 Système d'information

Editeurs

Consultez **les roadmaps des éditeurs** concernant le développement et le déploiement de la solution compatible INSi, ainsi que les éditeurs **autorisés par le CNDA**

Questionnaire d'autoévaluation

Ce document vous permet de faire **un état des lieux organisationnel / identitovigilance / SI** et vous permettra d'obtenir un plan d'actions adapté à votre situation

Les actions menées et en cours auprès du médico-social

Actions auprès des structures

- Exploration des **cas d'usage** INS avec une dizaine d'entretiens métiers réalisés
- Réalisation de plusieurs **webinaires** à destination des structures médico-sociales
- Publication d'un **questionnaire d'autoévaluation** pour les EHPAD
- **Intervention** auprès de quelques associations à leur demande (AVENIR APEI,…) et notamment en lien avec les lauréats Structures 3.0
- Une **phase d'observation** lancée avec l'ADAPEI 69 et son éditeur, AGM Informatique
- Un **retour** sur le déploiement de l'INS prévu avec **2 EHPAD** et leur éditeur, Berger Levrault
- Un groupe de travail **INS / PMI** prévu mi-avril avec l'éditeur Inetum (ex-GFI) et ses clients

Actions auprès des éditeurs

- Participation au **GT CNSA** éditeurs (Avril 2020) et **GT éditeurs du GIE SESAM-Vitale** (Juin 2020)
- **19 entretiens** réalisés avec les principaux éditeurs du secteur (janvier-mars 2021) et plusieurs **en cours de programmation**

Actions auprès des acteurs nationaux

- COPIL « **INS dans le médico-social** » en présence notamment de la CNSA et de l'ANAP (Avril 2020)
- COPIL **CNSA** (Mars 2021)

Dynamique observée dans le médico-social, avec des éditeurs qui se mobilisent sur l'INS

Editeurs en cours d'autorisation

INTERCAMSP – Solution : Orgamedi
Début du déploiement **à partir de fin mai / début juin**

DIR IPS – Solution : DIR IGAMI
Pas de visibilité sur une date de déploiement à ce stade

TERANGA – Solution : NetSoins
Déploiement **fin mars** (si autorisation obtenue) ou **octobre**

MALTA / DICSIT – Solutions : Titan et MicroSoins
MicroSoins disponible **début mai** ; déploiement Titan **courant juin / juillet**

Medialis – Solution : Mediateam
Travaux finalisés d'ici **la fin S1**. Pas davantage de visibilité à ce stade

Editeurs autorisés

Berger Levrault – Solution : BL Senior
A commencé le déploiement auprès de 2 EHPAD pilotes

EIG Santé – Solution : EO FSE
Déploiement prévu **courant mars** auprès de bêta-testeurs

Informatique Service – Solution : GECKOS
Non contacté

BOREAS – Solution : Airmes
Pas de visibilité sur une date de déploiement à ce stade

Cegi Santé– Solution : Administratif
Déploiement prochain sur des ESMS pilotes, avant **généralisation** à partir d'**avril**.

Editeurs non encore engagés dans la démarche CNDA

Solware – Solution : Livia
Déploiement envisagé **courant juin**

XELYA – Solution : XIMI
Déploiement envisagé à partir de **septembre**

GIES – Solution : Atena
Pas de visibilité à ce stade

Evolucare – Solutions : Osiris / Imago
Pas de visibilité à ce stade

Groupe UP – Solutions : Dôme, Web Apologic
Déploiement prévu **courant juin**

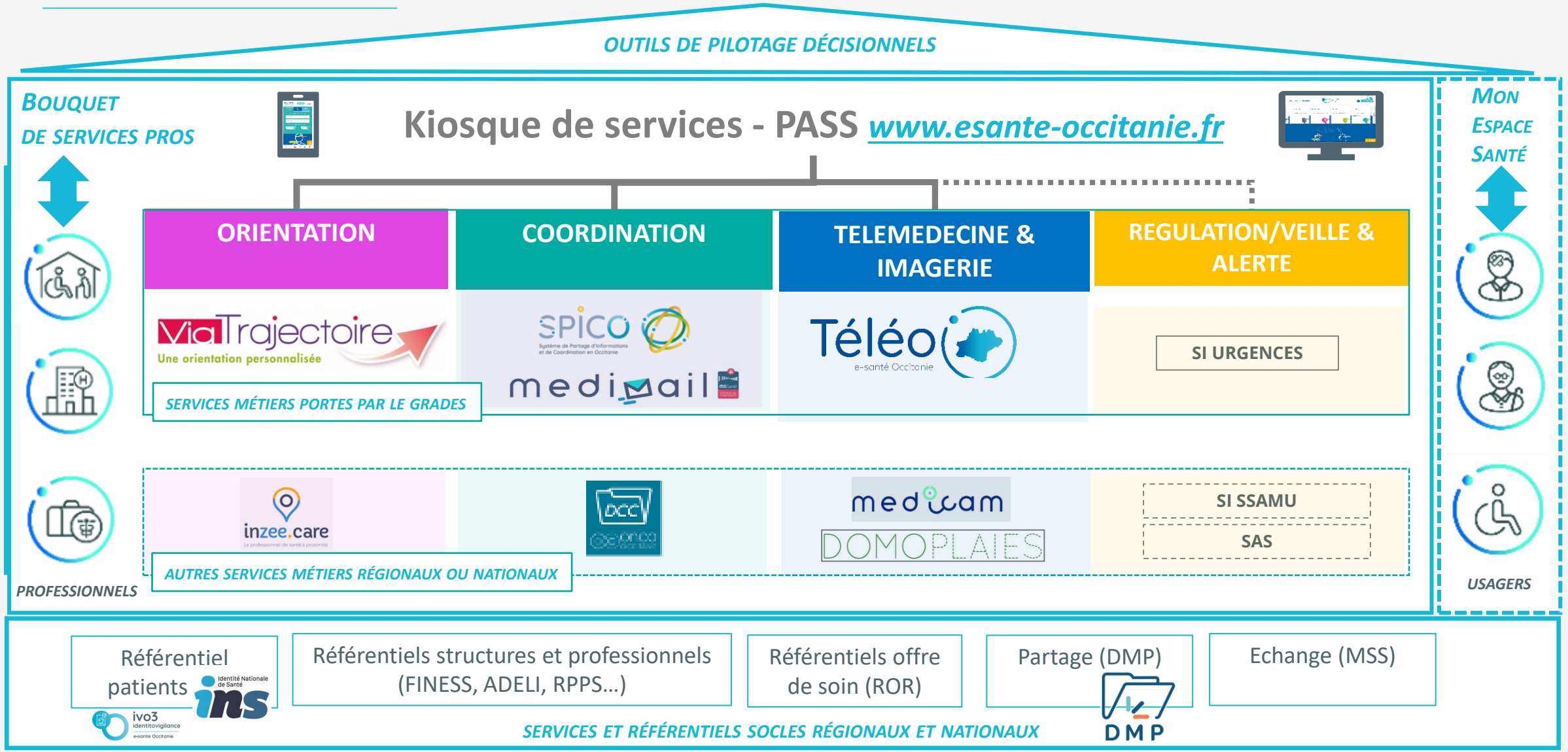
Socianova– Solution : OGYRIS
Déploiement envisagé **courant juin**

KI LAB – Solution : Globule
Pas de visibilité à ce stade

Maincare – Solution : IdeoPHM (esclave)
Déploiement prévu à partir de **T3**

MEDISYS
Pas de visibilité à ce stade

L'INS dans l'offre e-santé



?

Questions

Conclusion

Avant de nous quitter

Prochaine réunion du collectif MS&Numérique : **14 Juin**

Prochaine rencontre du club des DRSI : **6 Juillet**

- Thème : **cybersécurité**
- Orateurs déjà positionnés : O. MUSSEAU, S. SAINT-ALME, H. BAROU-CROUTZAT, J. ALASTUEY
- D'autres candidats ?

La **participation de notre club** pour :

- contribuer à développer les services régionaux
- contribuer aux groupes de travail nationaux

L'idée de créer un **annuaire** du groupe pour favoriser les échanges

=> Lien beekast pour donner votre accord : Accueil - 8tav (beekast.com)

Notre « to do »

Les résultats de la priorisation sont donnés ci-après, par ordre d'importance décroissant :

PRIORITAIRE	IMPORTANT	A NE PAS OUBLIER
RGPD, sécurité informatique, identito-vigilance	Partager des expériences d'élaboration et de déploiement du SI	Partager sur l'écart entre les fonctionnalités proposées par les logiciels et les demandes utilisateurs
	Méthodologie projet pour le déploiement d'un SI et/ou DUI	Partager des actualités numériques
	Réfléchir à l'efficience des systèmes sur la qualité des services rendus aux usagers	
	Tout savoir sur l'interopérabilité	
	Infrastructure cible dans le cadre de la stratégie numérique	
	Hiérarchisation des projets issus de la feuille de route	
	Formation des utilisateurs (et administrateurs)	

Merci de votre attention.

e-santé Occitanie
Connecter pour mieux soigner