

Inria

Protection juridique et technique des
données de santé

3^e rencontre devtech santé-numérique

Inria

Sommaire

01. Accompagnement RGPD et SSI
02. Protection juridique des données de santé
03. Protection technique des données de santé
04. Comment s'y prendre

01

Accompagnement RGPD et SSI

Déléguée à la protection des données



Anne Combe

(Centre Université de Nice)

... et son équipe (Emilie Masson + Juristes de centres)

Responsable de la sécurité du système d'information



Dominique Launay

(Centre Université de Rennes)

... et ses équipes (CSSI et SOC)

Nos objectifs

Vous aider à réaliser vos travaux

- **Partenariats**
- **Expérimentations**

...Tout en assurant

- **la protection des données**
- **La conformité vis à vis de la réglementation**

02

Protection juridique des données de santé

Données de santé (1/2)

Définition européenne

- Données relatives à la **santé physique ou mentale, passée, présente ou future, d'une personne physique** (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne
- Définition large englobe données de mesure à partir desquelles il est possible de déduire une information sur l'état de santé de la personne

Exemples

- 1) **les informations relatives à une personne physique** collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé
- 2) **les informations obtenues lors du test ou de l'examen d'une partie du corps** ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques
- 3) **les informations concernant une maladie**, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée (indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro)

Données de santé (2/2)

En pratique, 3 catégories de données

- **Données de santé par nature** : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc.
- **Données, qui du fait de leur croisement avec d'autres données, deviennent des données de santé** en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques...), croisement de la tension avec la mesure de l'effort, etc.
- **Données qui deviennent des données de santé en raison de leur destination**, c'est-à-dire de l'utilisation qui en est faite au plan médical

Important

- Des données de santé pseudonymisées restent des données de santé

Principaux régimes juridiques applicables aux données de santé (1/2)

RGPD - Europe

- Données de santé = données sensibles
- Traitement des données sensibles est par principe interdit mais exceptions prévues (ex : consentement des personnes concernées)

Loi informatique et libertés modifiée - France

- Article 8 - Repris du RGPD
- Chapitre IX - Régime applicable en France

Principaux régimes juridiques applicables aux données de santé (2/2)

Recherches impliquant la personne humaine (Loi Jardé) - France

- Fixe cadre juridique en adaptant réglementations en fonction des risques encourus pour les personnes participant à ces recherches

Dispositions sur l'hébergement des données de santé - France

- Article L. 1111-8 du Code de la Santé Publique
- FAQ Ministère de la Santé - 3 conditions pour l'hébergement HDS

Données de santé

Héberger les données pour le compte de patients ou de professionnels de santé (si hébergement interne pas de HDS)

Données collectées selon une finalité de prévention, diagnostic, de soins ou de suivi social et médico-social

Accès aux données du SNDS - Contexte

Décret n° 2021-848 du 29 juin 2021

- Autorise Inria et CNRS à traiter les données personnelles du SNDS dans le cadre de projets intéressant la santé publique
- Permet aux chercheurs Inria et CNRS d'accéder aux données pseudonymisées du SNDS
 - Données de l'assurance maladie (base SNIIRAM)
 - Profondeur historique de 19 ans Données des hôpitaux (base PMSI)
 - Profondeur historique de 19 ans Causes médicales de décès (base du CepiDC de l'Inserm) - depuis 2017

Accès aux données du SNDS - Organisation

Emilie Masson et Anne Combe sont Autorités d'Enregistrement Déléguées - AED

- Gèrent habilitations des chercheurs Inria accédant au SNDS
- Tiennent à jour Registre des projets utilisant accès au SNDS (communiqué à la CNIL)

Chercheurs accèdent aux données du SNDS

- Uniquement si projet de recherche d'intérêt public
 - Après avoir suivi 3 formations obligatoires et formations de leur choix
 - Après échange en visio avec Emilie Masson et/ou Anne Combe
 - En respectant le référentiel de sécurité du SNDS
- NB : Système de sécurité de la CNAM permet de tracer ce qui se passe

Processus de demande d'accès Inria

- <https://intranet.inria.fr/Inria/Directions/Direction-generale/Politique-RGPD/Processus-demande-d-acces-au-SNDS>

03

Protection technique

Échelle de sensibilité Inria

Impact	Niveau de classification	Chiffrement
Nul	Public	Non
Modéré	Diffusion limitée + mention	Non
Important	Confidentiel + mention	Non (si ressource interne non exposée et correctement cloisonnée)
Catastrophique	Restreint + mention	Oui

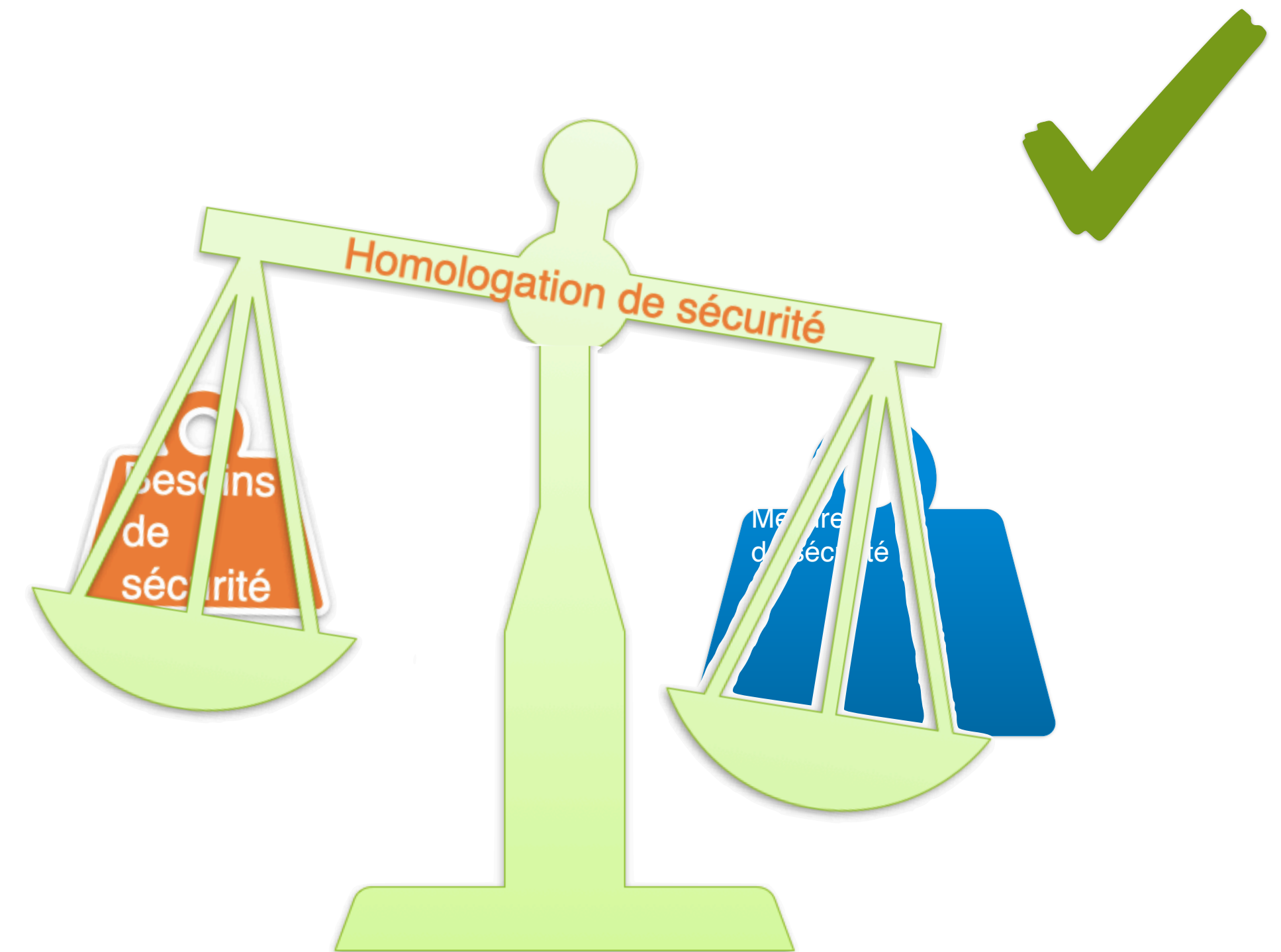
- <https://intranet.inria.fr/Inria/Directions/Direction-generale/Securite-Defense/Echelle-de-sensibilite>

04

Comment s'y prendre ?

Homologation de sécurité

- **Qui ?**
 - Porteur de projet
 - CSSI
 - RSSI
 - Commission des homologations
- **Quand ?**
 - Dès que les contours du projet sont dessinés
- **Durée ?**
 - Instance générique
 - Briques homologuées



<https://intranet.inria.fr/Inria/Directions/Direction-generale/Securite-Defense/PGSI>

Merci !

Inria