LES MATINEES

CEMKAfé

APPLICATION DU RGPD

aux études non interventionnelles et retour d'un audit CNIL

Intervenants: Dr Stéphane Bouée – Viviane Jeanbat – Juliette Roth-Bonté

17 octobre 2019

Sommaire

INTRODUCTION

RGPD

- **Règlement général sur la protection des données**
- **General Data Protection Regulation**

- Applicables dans l'ensemble des 28 États membres de l'Union européenne à compter du 25 mai 2018

- **DPO** (Data Protection Officer)
- DPD ? … Délégué à la protection des données

- **DPIA** (*Data Protection Impact Assessment*)
- AIPD analyses d'impact relatives à la protection des données

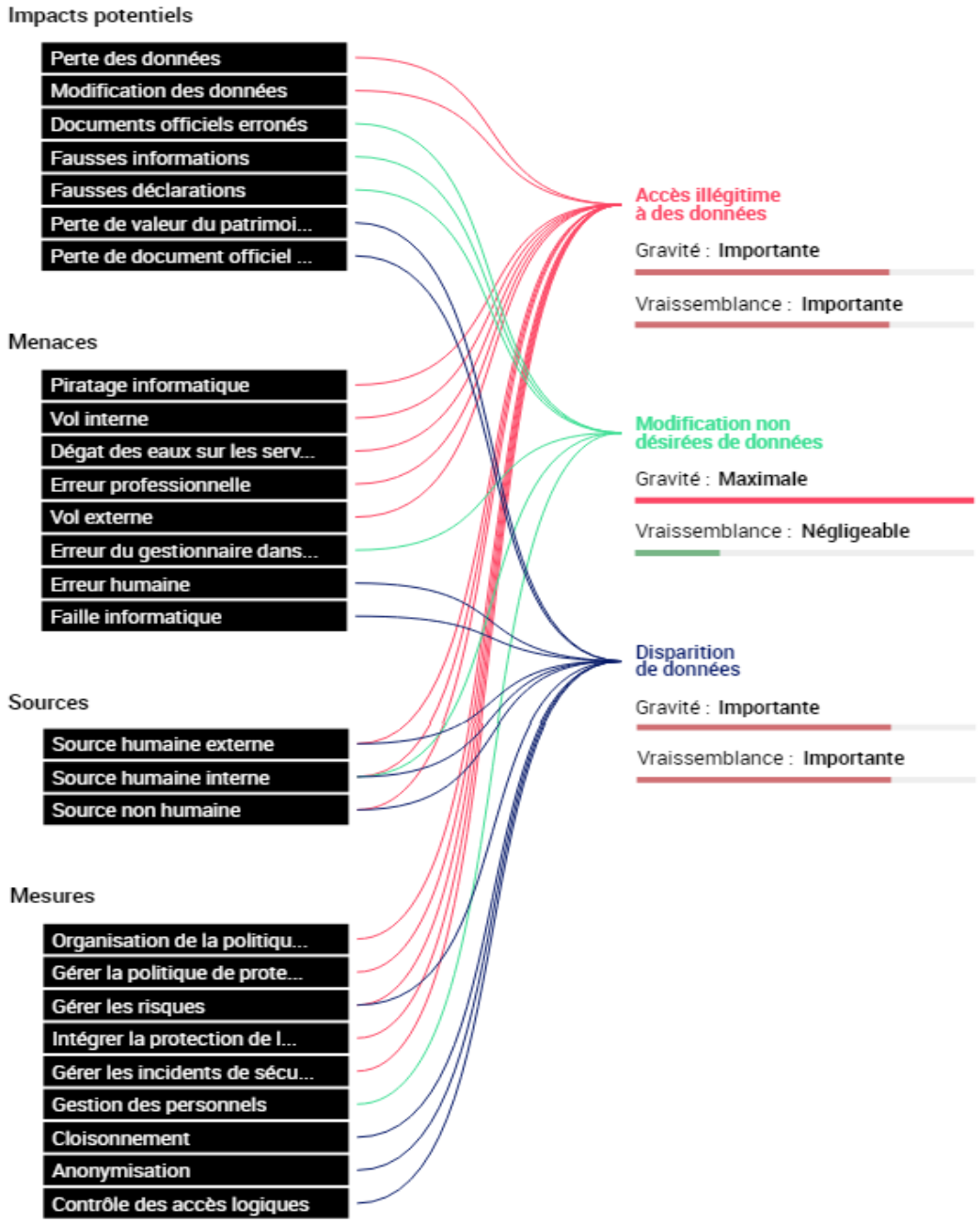
RGPD

Qui est le bon interlocuteur ?

- DPO du promoteur (Responsable de traitement)
- DPO du sous traitant (responsable de la mise en œuvre du traitement)

DPIA

Qui fait la DPIA ?



Application à …

SNDS (SNIIRAM, EGB, PMSI)

Etudes sur cas patients (RIPH & RNIPH)

(MR-001)

MR-003

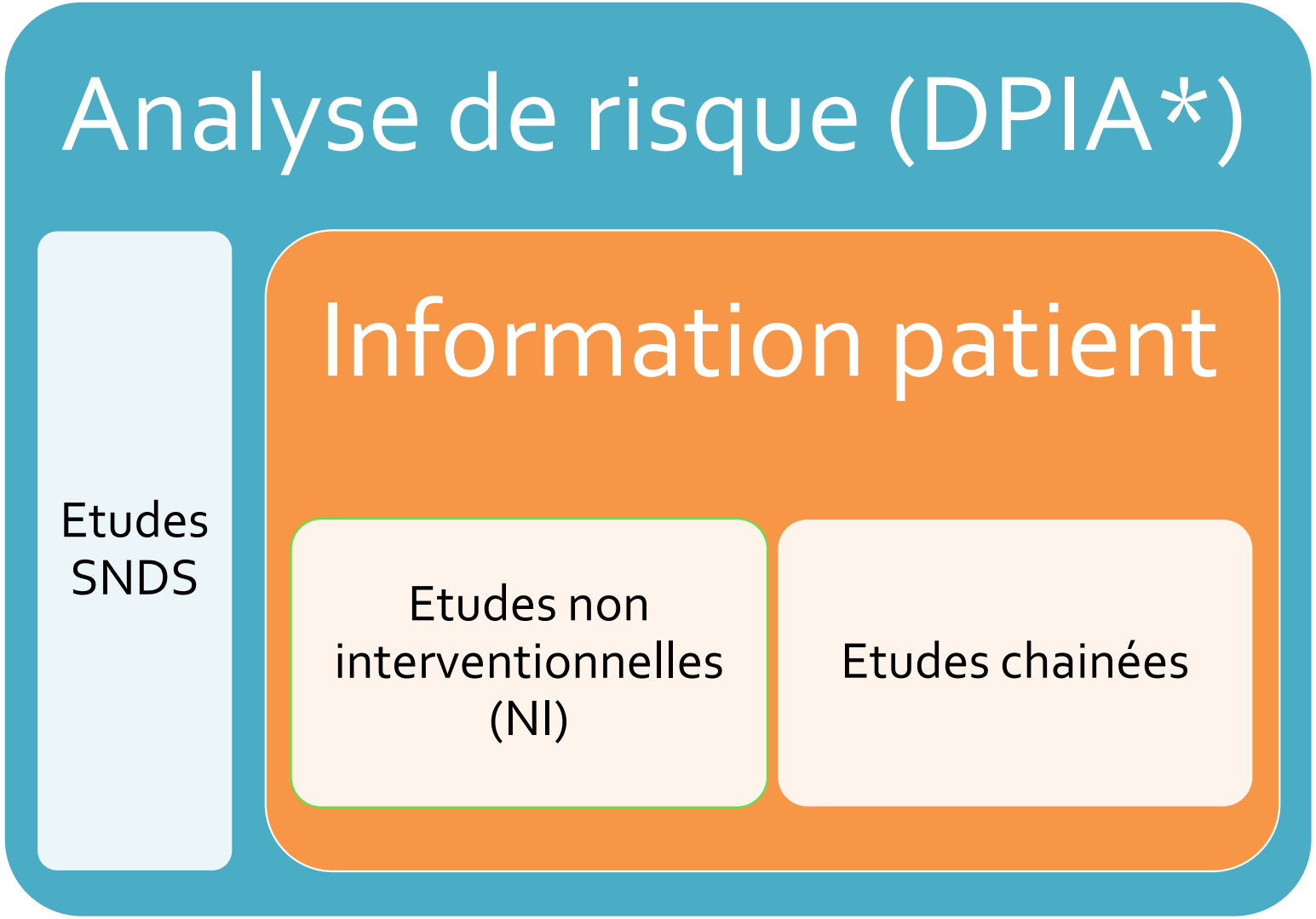
MR-004

Etudes chainées

Appariement

- Probabiliste
- Déterministe

Application du RGPD



*Data Protection Impact Assessment

Information du patient

Information du patient

Avantages

- Peu de changements par rapport à la Loi Informatique & Libertés avant l'application du RGPD
- Souci de bien informer le patient

Inconvénients

Lettres plus complexes pour le patient :

- multiples contacts (investigateurs, DPO, CNIL)
- Longueur de la lettre

Difficultés pratiques

- Traitement des réclamations des patients
- Difficultés pour prouver que le patient a été informé en absence de consentement écrit :

  - études rétrospectives avec patients contactés par courrier/mail par l'investigateur

  - habituer les investigateurs à noter l'information dans le dossier médical

Information du patient en pratique

- Mise en avant dans la lettre d'information du point de contact principal = l'investigateur

- DPO = celui du responsable de traitement
- Réclamations patient: gérées par le DPO

- Envoi de l'information par courrier / Mail (études rétrospectives):
  - Délai de 3 à 4 semaines pour considérer que l'absence de réponse du patient vaut accord conseillé par la CNIL
- Noter l'information du patient dans le dossier médical:
  - à préciser dans la convention financière passée avec l'investigateur
  - à préciser dans le protocole
  - à rappeler aux investigateurs lors de la mise en place de l'étude
  - à vérifier dans le dossier médical du patient si du monitoring sur site est prévu

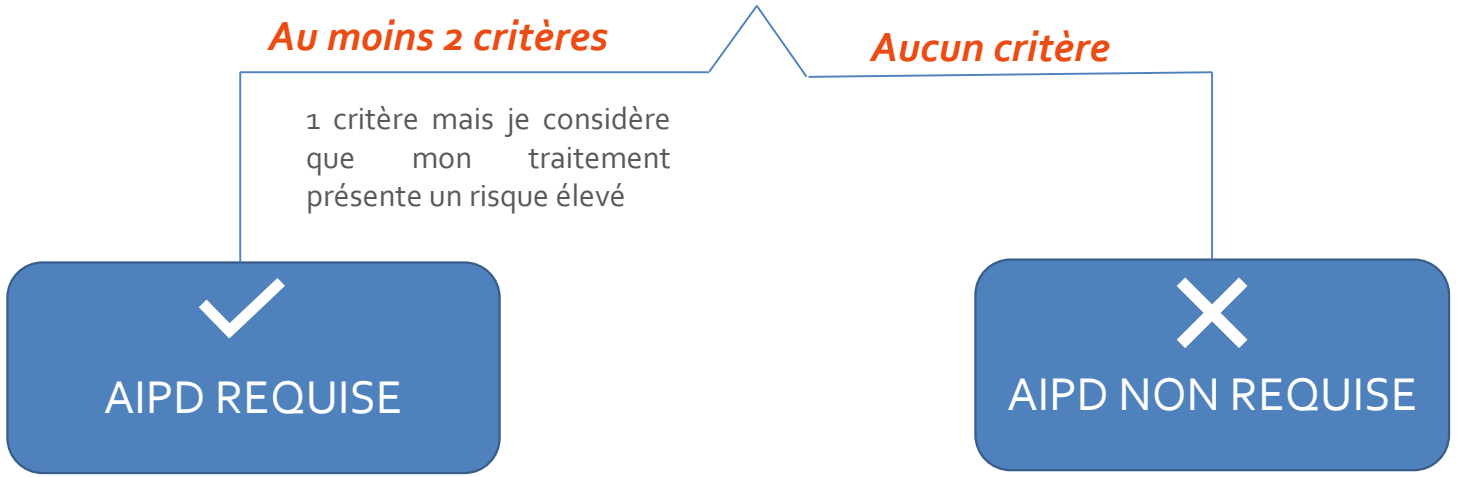
DPIA

Rappel des critères de la CNIL

(DPIA* obligatoire pour MR-003 & MR-004)

Combien de critères mon traitement remplit-il parmi les suivants?

- 1. Evaluation / Scoring (y compris le profilage)
- 2. Décision automatique avec effet légal ou similaire
- 3. Surveillance systématique
- **4. Données sensibles ou hautement personnelles (santé, géolocalisation, etc..)**
- **5. Collecte à large échelle**
- **6. Croisement des données**
- **7. Personnes vulnérables (patients, personnes âgées, enfants, etc..)**
- 8. Usage innovant (utilisation d'une nouvelle technologie)
- 9.Exclusion du droit/ contrat



https://www.cnil.fr/fr/infographie-dois-je-faire-une-aipd

*Data Protection Impact Assessment

Evaluation du risque

Etudes SNDS

- Plateforme sécurisée de la CNAM : durée d'accès + droits d'accès limités
- **PMSI : MR-006: pas de DPIA**
- Attention: si plateforme externe (« système fils ») : risque ++++

Etudes NI

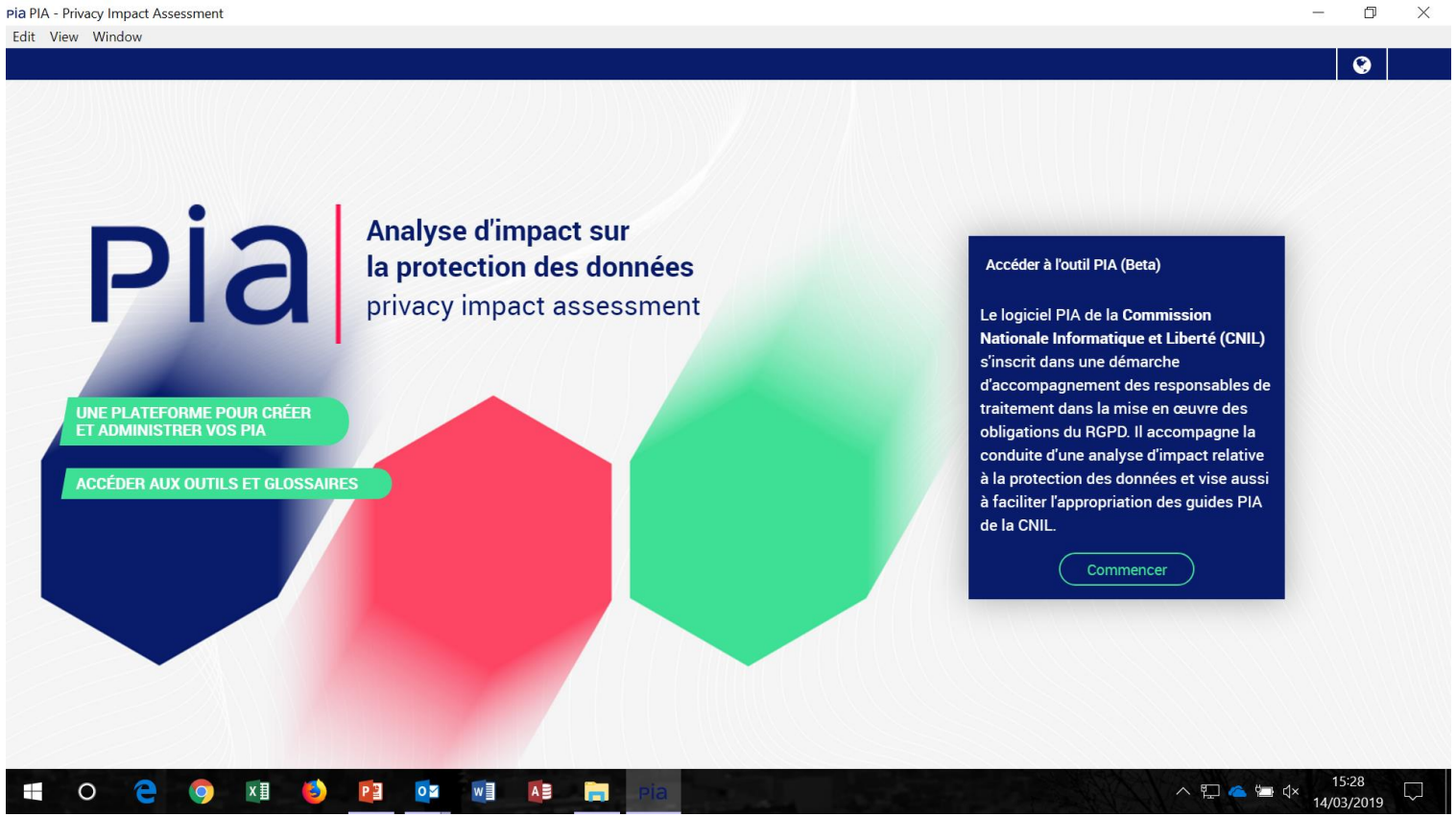
- Flux de données plus important :
- Outils de recueil multiples : CRFs papier, eCRFs
- Multiples intervenants: investigateurs, CRO, autres prestataires (saisie, eCRF)

Etudes chainées

- Risque accru : **croisement de bases de données**
- Flux de données important, multiples intervenants
- Appariement probabiliste : risque ++
- **Appariement avec le NIR ++++++**

En pratique

- Responsabilité du RT; La CRO doit aider le RT à faire la DPIA
- La CRO a un devoir d'information vis-à-vis du RT
- En pratique, la CRO fait souvent la DPIA, puis validation par le RT
- Outil: PIA de la CNIL: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil



DPIA

Avantages

- Fait prendre conscience de l'ensemble des risques
- Permet d'identifier et d'analyser toutes les failles potentielles et d'améliorer le système

Inconvénients

- Complexe mais possibilité de faire des modèles-types à adapter ensuite à chaque étude
- Une étape en plus à prévoir dans les projets

Difficultés pratiques

- Sensibilisation des personnes : concept encore flou, vu comme quelque chose de fastidieux
- Exercice difficile à faire : s'appuyer sur des exemples de la CNIL et sur le DPO (https://www.cnil.fr/fr/nouveautes-sur-le-pia-guides-outil-piaf-etude-de-cas)

Etudes SNDS

Etudes SNDS (hors PMSI-MR-006)

1/ Information du patient

Information et droits du patient

- Néant *

*Article 14 du RGPD : « Toutefois, il n'est pas nécessaire d'imposer l'obligation de fournir des informations lorsque la personne concernée dispose déjà de ces informations, lorsque l'enregistrement ou la communication des données à caractère personnel est expressément prévu par la loi **ou lorsque la communication d'informations à la personne concernée se révèle impossible ou exigerait des efforts disproportionnés** »

Etudes SNDS (hors PMSI-MR-006)

2/ Sécurité des données

Sécurisation des données gérées par la CNAM

- Plateforme sécurisée de la CNAM: accès limité dans le temps et personnalisé (i.e.: 1 calculette/étude/statisticien(ne))
- Seuls les résultats sont exportés vers le RT

Sécurisation des données dans un système fils

- Décrire les moyens de sécurisation mis en place dans le système fils
- Seuls les résultats sont exportés vers le RT

Etudes SNDS (hors PMSI-MR-006)

3/ Description du flux de données

Flux de données simple

- Seuls les résultats sont transmis au RT
- Peu de sous-traitants: CNAM / CRO

Etudes non interventionnelles répondant aux MR-003 / MR-004

Etudes NI MR-003 MR004 (sans chainage)

1/ Information du patient

Information et droits du patient

- Consentement signé ou absence d'opposition
- Preuve de la passation de l'information
- Preuve de l'accord ou de la non-opposition* du patient

*Délai préconisé par la CNIL: 3 semaines après l'envoi de la lettre d'information

Etudes NI MR-003 MR004 (sans chainage)

2/ Sécurité des données

Sécurisation des données : gérée par les sous-traitants

- Hébergement des données du eCRF (en Europe, HDS)
- Saisie des données: en Europe; décrire les modalités de transfert
- Sécurisation des données papier et des autres flux (fax ou boites mails sécurisés par exemple)
- Formation des investigateurs et des ARCs Free-lance à la sécurité des données
- Traitement au sein de la CRO: droits d'accès, sécurisation des pc & du serveur, sauvegardes, traçabilité

Etudes avec données identifiantes (donc hors MR) : risque de violation +++ : sécurisation des données identifiantes : envoi/réception, qui a accès, stockage, durée de conservation?

Etudes NI MR-003 MR004 (sans chainage)

3/ Description du flux de données

Flux de données plus complexe

- Multiples sous-traitants : investigateurs, saisie, eCRF, CRO, ARCs Free-lance ⇛ risque de violation ++
- Contrats à passer avec chaque prestataire
- Flux multiples : voie postale, fax, voies électroniques…

Etudes mixtes avec appariement probabiliste

Etudes chainées avec appariement probabiliste

1/ Information du patient

Information et droits du patient

- Consentement signé ou absence d'opposition
- Preuve de la passation de l'information
- Preuve de l'accord ou de la non-opposition* du patient
- **Informer de l'existence d'un chainage**
- **Informer de la nature des données qui serviront à l'appariement**

*Délai préconisé par la CNIL: 3 semaines après l'envoi de la lettre d'information

Etudes chainées avec appariement probabiliste

2/ Sécurité des données

Sécurisation des données : gérée par les sous-traitant (dont la CNAM)

- Hébergement des données du eCRF (en Europe, HDS)
- Saisie des données: en Europe; décrire les modalités de transfert
- Sécurisation des données papier et des autres flux (fax ou boites mails sécurisés par exemple)
- Formation des investigateurs et des ARCs Free-lance à la sécurité des données
- Traitement au sein de la CRO: droits d'accès, sécurisation des pc & du serveur, sauvegardes, traçabilité
- **Durée de conservation des données d'appariement qui ne sont pas forcément utiles pour l'analyse**
- **Lieu d'analyse des données appariées : plateforme de la CNAM**

Etudes avec données identifiantes (donc hors MR) : risque de violation +++ : sécurisation des données identifiantes : envoi/réception, qui a accès, stockage, durée de conservation?

Etudes chainées avec appariement probabiliste

3/ Description du flux des données

Flux de données plus complexe

- Multiples sous-traitants : investigateurs, saisie, eCRF, CRO, ARCs Free-lance ⇛ risque de violation ++
- Contrats à passer avec chaque prestataire
- Flux multiples : voie postale, fax, voies électroniques…
- **Envoi des données d'appariement à la CNAM (canal sécurisé via la plateforme de la CNAM) : Qui, comment?**

⇛ **risque de violation +++**

Etudes mixtes avec appariement via le NIR

Etudes chainées avec le NIR
1/ Information du patient

Information et droits du patient

- Consentement signé ou absence d'opposition
- Preuve de la passation de l'information
- Preuve de l'accord ou de la non-opposition* du patient
- Informer de l'existence d'un chainage
- **Informer du recueil du NIR : pourquoi? Qui aura accès? Flux de cette donnée?**

*Délai préconisé par la CNIL: 3 semaines après l'envoi de la lettre d'information

Etudes chainées avec le NIR
2/ Sécurité des données

Sécurisation des données : gérée par les sous-traitant (dont la CNAM)

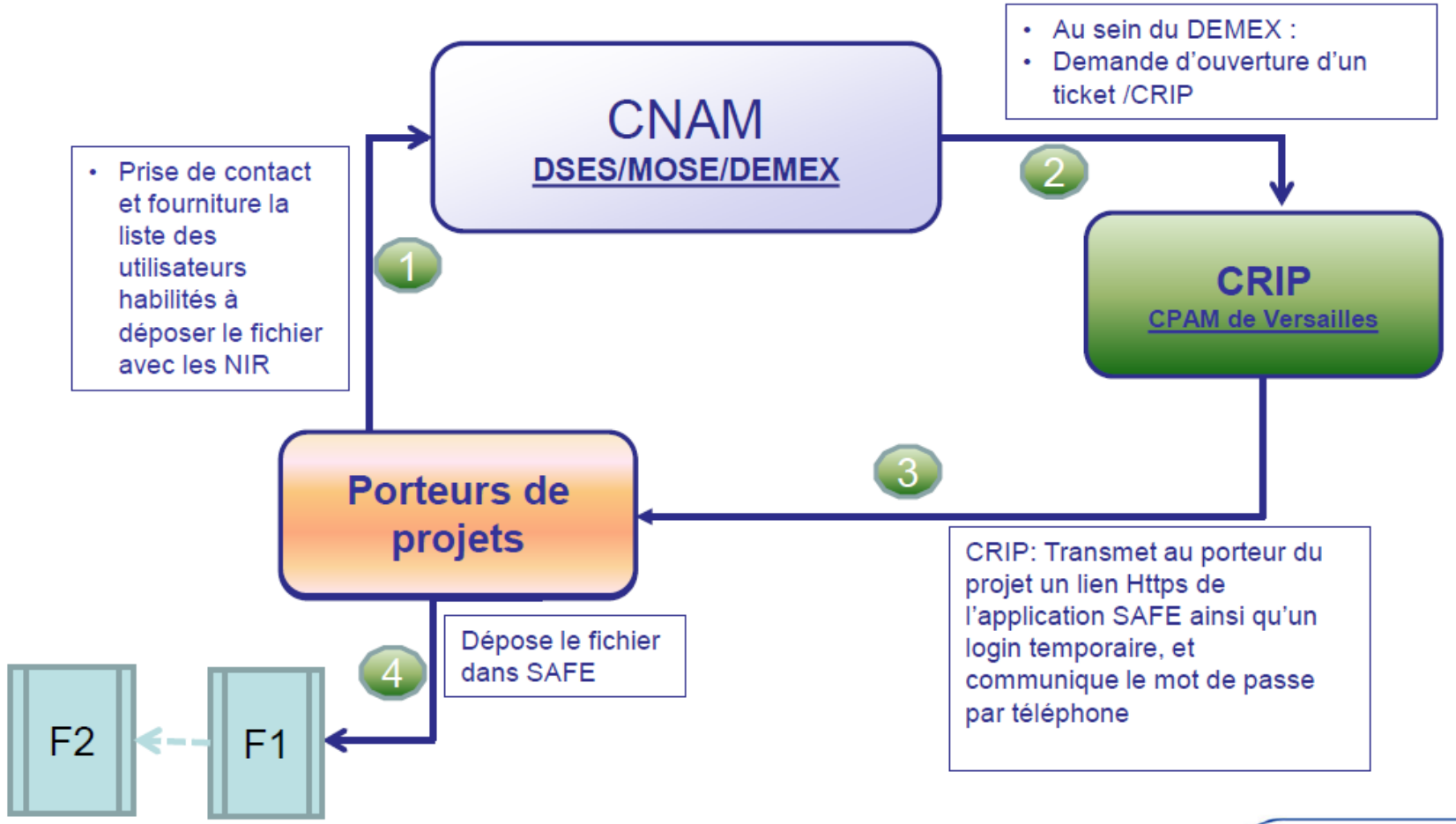
- Hébergement des données du eCRF (en Europe, HDS)
- Saisie des données: en Europe; décrire les modalités de transfert
- Sécurisation des données papier et des autres flux (fax ou boites mails sécurisés par exemple)
- Formation des investigateurs et des ARCs Free-lance à la sécurité des données
- Traitement au sein de la CRO: droits d'accès, sécurisation des pc & du serveur, sauvegardes, traçabilité
- Durée de conservation des données d'appariement qui ne sont pas forcément utiles pour l'analyse
- Lieu d'analyse des données appariées : plateforme de la CNAM
- **Protection du NIR pendant le recueil et lors du transfert à la CNAM pour la foinisation**

Faire la DPIA et ce, avant le dépôt à la CNIL car celle-ci est susceptible de la demander

Etudes chainées avec le NIR

3/ Description du flux des données : rappel du schéma du flux

Rappel du Circuit de circulation/transformation des identifiants



Etudes chainées avec le NIR

3/ Description du flux des données

Flux de données plus complexe et surtout à haut risque du fait du recueil du NIR

- Multiples sous-traitants : investigateurs, saisie, eCRF, CRO, ARCs Free-lance ⇛ risque de violation ++
- Contrats à passer avec chaque prestataire
- Flux multiples : voie postale, fax, voies électroniques…
- **Comment est recueilli le NIR?**
- **Envoi des données d'appariement à la CNAM (canal sécurisé via la plateforme de la CNAM) : Qui, comment?**

⇛ risque de violation ++++

Audit CNIL

Objet de l'audit CNIL

- Visite surprise le 28 mars 2019
- 2 inspecteurs qui ont montré leur carte et leur ordre de mission datant du 15 février 2019
  - 1 juriste du service des contrôles
  - 1 auditeur des systèmes d'information au service des contrôles
- Objet de l'audit : Gestion des études SNDS
- (+ au passage… Conformité au RGPD)
- Durée de l'audit: 1 journée

Questions générales sur le respect du RGPD

- 1ère question: « Qu'avez-vous mis en place par rapport à l'application du RGPD? »
- « Pourquoi un DPO externalisé? »
- « Avez-vous eu des violations de données? »

Documents demandés sur le respect du RGPD

- Rapports d'audit des prestataires (eCRF, hébergeur externe)
- Fichier de suivi des audits des prestataires
- Derniers rapports d'audit des prestataires
- Exemple d'un contrat signé avec le prestataire eCRF
- Contrat signé avec l'hébergeur de données
- Exemples de DPIAs
- Fichiers de traitement
- Fichier de violation de donnée et tous les documents annexes
- Charte informatique
- Contrat signé avec le DPO
- Procédure RGPD
- Feuille de présence aux formations RGPD (mais copie non demandée)

Questions sur la gestion des études SNDS

- Les 2 auditeurs sont venus voir sur les postes des statisticiens les modalités de connexion aux bases SNDS (plateforme CNAM et plateforme CASD) : simulation en réel avec copies d'écran de chaque étape

- Ils se sont assurés que nous n'exportions que des données agrégées

Documents demandés sur les études SNDS

- Contrats de travail des statisticien(ne)s
- Attestations de formation CASD des statisticien(ne)s
- Liste des personnes ayant accès à l'EGB en annexe de l'une des conventions passée avec la CNAM
- Tous les contrats signés avec la CNAM (N=16)
- Conditions Générales d'Utilisation du Portail et des Données SNIIRAM
- Convention signée avec l'ATIH et ses annexes
- Exemple de sortie de résultats PMSI et EGB (*pas SNIIRAM car l'accès n'était pas fonctionnel: la CNAM venait de changer sa procédure de connexion avec des calculettes qui n'étaient pas encore activées*)
- Copies d'écran de chaque étape de connexion aux plateformes (PMSI et EGB)
- Exemple de mail de la CNAM envoyé au statisticien pour la connexion au portail pour une étude donnée
- Tous les contrats signés avec le RT (demande faite 4 mois après l'audit)

Documents annexes demandés

- Bilan financier des 3 dernières années
- Copie du dernier rapport d'audit client
- Procédure informatique
- Procédure Plan de reprise d'activité informatique
- Process de gestion des comptes réseau

Rendu

- A la fin de l'audit : Rédaction du PV d'audit par la CNIL puis relecture par Cemka pour éventuelle correction.
- PV signé par la CNIL et par Cemka le jour même : 1 copie imprimée et signée laissée sur place + 1 copie envoyée par courrier au Directeur général
- Le PV rapporte tout ce qui a été dit et récapitule la liste de tous les documents fournis par Cemka

- Rapport d'audit: En attente depuis le 28 mars

MERCI