CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Comment assurer la sécurité des données de santé?

Le RGPD appliqué aux données de santé
18 novembre

Solenn BRUNET et Philippe RICHY
Ingénieurs experts à la CNIL

Que dit le RGPD ?

- **Article 25 - Protection des données dès la conception et protection des données par défaut**

- **Article 32 - Sécurité du traitement (extraits) :**
  - *… le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :*
    - a) la **pseudonymisation** et le **chiffrement** des données à caractère personnel;
    - b) des moyens permettant de garantir la **confidentialité**, l'**intégrité**, la **disponibilité** et la **résilience constantes** des systèmes et des services de traitement ;
    - c) des moyens permettant de **rétablir la disponibilité** des données à caractère personnel et l'accès à celles-ci dans des délais appropriés **en cas d'incident physique ou technique** ;
    - d) une procédure visant à tester, à analyser et à évaluer régulièrement l'**efficacité des mesures techniques et organisationnelles** pour assurer la sécurité du traitement.

Les risques liés aux données

- **Accès illégitime** aux données :
  - *Exploitation des données (vol, revente, diffusion, profilage…)*
- **Modification** non désirée :
  - *Dysfonctionnement (mauvaises consignes de soin, mesures erronées, attaque sur une pompe à insuline…)*
- **Disparition** :
  - *Dysfonctionnement (dossier médical ne signalant plus les allergies…)*
  - *Blocage (impossibilité de dispenser des soins, impossibilité d'exercer ses droits, démarches administratives interrompues…)*

Le RGPD en pratique

LES VIOLATIONS DE DONNÉES

Que dit le RGPD ?

- Article 4 – Définitions, point 12 :
  - *« une violation de la sécurité entraînant, de manière accidentelle ou illicite,* ***la destruction, la perte, l'altération, la divulgation non autorisée*** *de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'****accès non autorisé*** *à de telles données »*

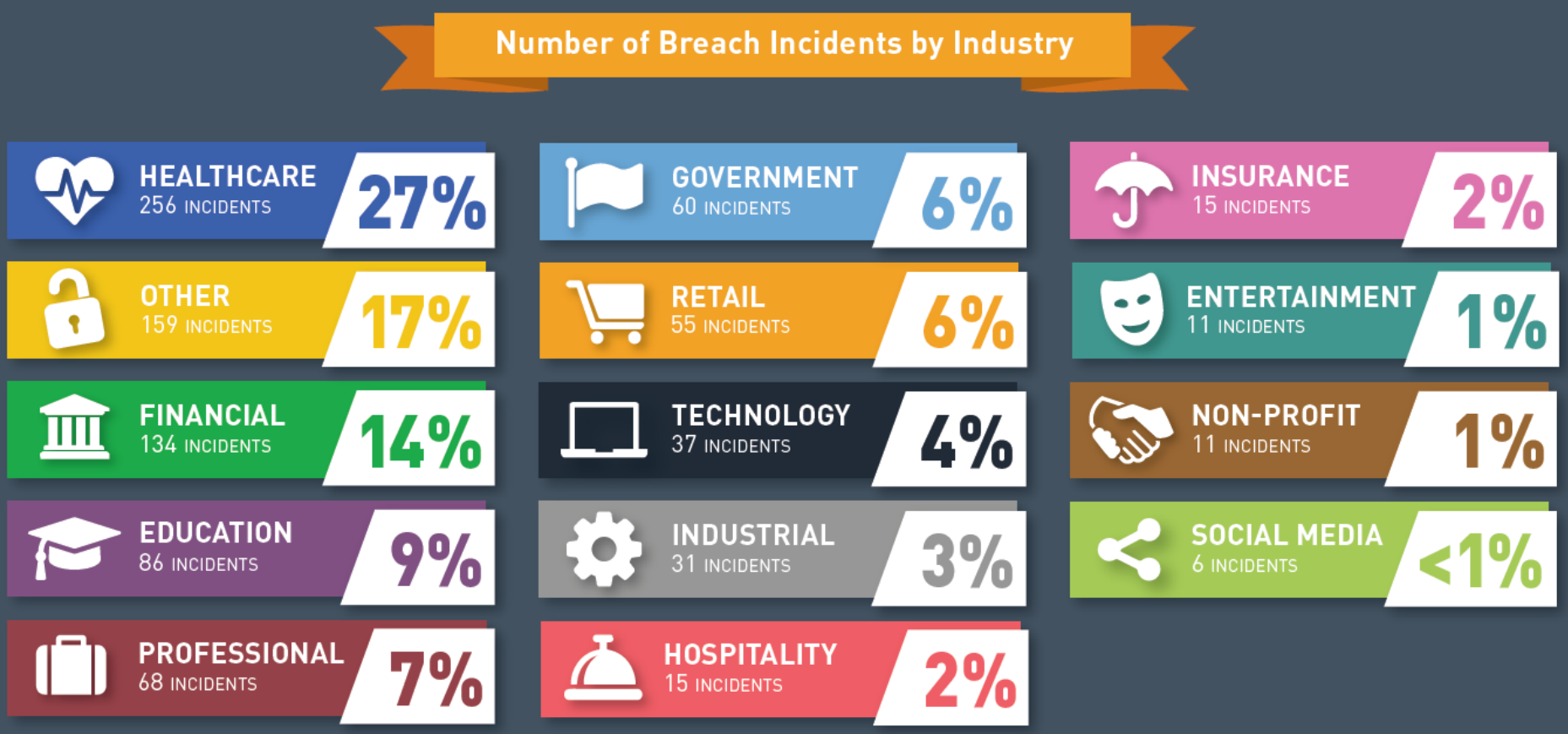
- Article 33 – Notification à l'autorité de contrôle
- Article 34 – Communication à la personne concernée

2 206 notifications reçues*

* au 18/09/2019

Les violations de données

Source : Gemalto, 1er semestre 2018



Première amende RGPD pour un hôpital portugais

le 05 Novembre 2018

Le CNPD portugais a condamné le centre hospitalier Barreiro-Montijo à 400 000 euros d'amende. (Crédit Photo : Free-Photos/Pixabay)

Le Portugal inaugure les sanctions financières au titre du RGPD. L'hôpital de Barreiro a écopé d'une amende de 400 000 euros en raison de sa politique d'accès aux bases de données des patients.

Le régulateur a constaté que plusieurs personnels administratifs avaient des accès réservés aux médecins. En parallèle, il a observé que 985 médecins avaient des habilitations pour accéder au dossier médical des patients, alors que l'établissement ne comprend que 296 médecins. Cet écart s'expliquerait par la présence de vacataires, mais le hic est que les comptes de ces médecins temporaires demeurent tout le temps actifs. Enfin, la délégation du régulateur a créé un compte test et a pu avoir accès à des données patients, montrant une faiblesse dans la gestion des comptes (habilitation, gestion des profils, ...)

Violations de données : les différents cas

Pour les personnes concernées, la violation engendre :	Aucun risque	Un risque	Un risque élevé
Documentation en interne par le RT sous forme d'un registre interne des différentes violations dont il est victime	X	X	X
Notification à l'autorité de contrôle, c'est-à-dire la CNIL en France, si possible en 72h	-	X	X
Information des personnes concernées dans les meilleurs délais, hors cas particuliers	-	-	X

Les acteurs concernés

Le sous traitant

notifie au RT toute violation de données dans les meilleurs délais après en avoir pris connaissance afin de lui permettre de respecter son obligation de notifier, si possible, dans les 72 h

Le responsable du traitement (RT)

- documente toute violation de données
- notifie à l'autorité de contrôle la violation dans les meilleurs délais, et si possible dans les 72 h de la connaissance de la violation

si la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques

- informe les personnes concernées en cas de risque élevé

L'autorité de contrôle

- reçoit la notification
- examine les éléments liés à la violation
- conseille le RT sur les mesures à prendre
- peut ordonner au RT de communiquer à la personne concernée la violation de données

La personne concernée

reçoit communication de la violation en cas de risque élevé pour ses droits et libertés.

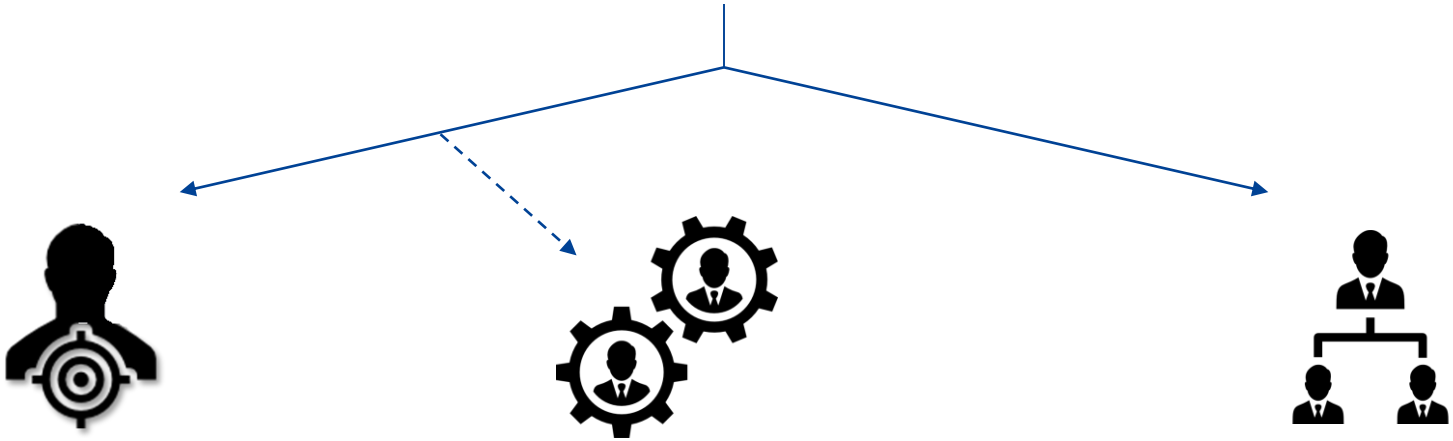
Formulaire « violations » sur cnil.fr

Le RGPD en pratique

LES OUTILS DE LA CONFORMITÉ

Responsabilisation de tous les acteurs

Rééquilibrage des situations juridiques
des responsables de traitement
et des sous-traitants

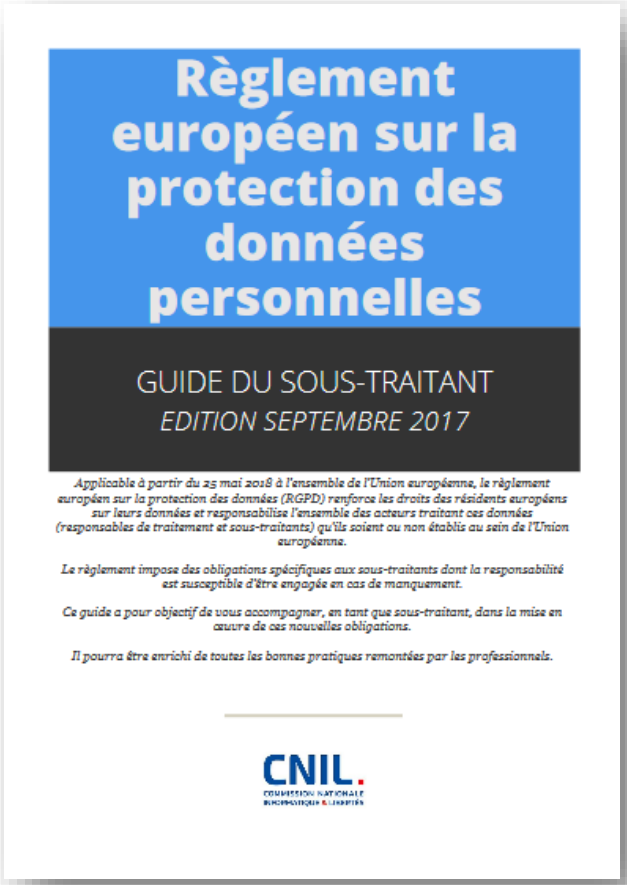


Responsable de traitement

Responsables de traitement conjoints

Sous-traitant

Responsabilité spécifique des ST



Contrat conforme à l'article 28 du RGPD

Elargissement des obligations du ST vis-à-vis du RT

Obligations propres du ST (délégué, registre)

Responsabilité propre du ST

Évaluer le niveau de sécurité des données personnelles de votre organisme

1. **Sensibiliser** les utilisateurs
2. **Authentifier** les utilisateurs
   - Identification + authentification simple ou authentification forte (= à deux facteurs, parmi ce que je sais, ce que je possède, ce que je suis)
3. Gérer les **habilitations**
   - Selon le « besoin d'en connaître » ; procédure « bris de glace »
   - Validation hiérarchique, durée limitée, revue régulière
   - Accès administrateurs à travers un « bastion »
4. **Tracer** les accès et gérer les incidents
5. Sécuriser les **postes de travail**
   - Verrouillage, antivirus…
6. Sécuriser l'**informatique mobile**
7. Protéger le **réseau** informatique interne
8. Sécuriser les **serveurs**

Évaluer le niveau de sécurité des données personnelles de votre organisme

9. Sécuriser les **sites web**
10. **Sauvegarder** et prévoir la continuité d'activité
    - Protection et tests réguliers des sauvegardes
11. **Archiver** de manière sécurisée
    - Protection des supports
12. Encadrer la **maintenance** et la **destruction** des données
13. Gérer la **sous-traitance**
    - Contractualisation et encadrement
14. Sécuriser les **échanges** avec d'autres organismes
15. Protéger les **locaux**
16. Encadrer les **développements informatiques**
    - Pas de données de production sur les serveurs de tests
17. Utiliser des **fonctions cryptographiques**
    - Chiffrement des flux, bases de données et sauvegardes

Mesures de sécurité

- Mesures sur les données du traitement
  - Chiffrer
  - Anonymiser
  - Cloisonner
  - Contrôler les accès logiques
  - Journaliser
  - Contrôler l'intégrité
  - Archiver
  - Sécuriser les documents papier
- Mesures générales de sécurité
  - Sécuriser l'exploitation
  - Lutter contre les logiciels malveillants
  - Gérer les postes clients
  - Sécuriser les sites web
  - Sauvegarder
  - Maintenance
  - Sécuriser les canaux informatiques
  - Tracer l'activité du système
  - Contrôler l'accès physique
  - Réduire les vulnérabilités des matériels
  - S'éloigner des sources de risques
  - Se protéger des sources de risques non humaines
- Mesures organisationnelles
  - Gérer l'organisation de la protection de la vie privée
  - Gérer la politique de protection de la vie privée
  - Gérer les risques
  - Intégrer la protection de la vie privée dans les projets
  - Gérer les incidents de sécurité et les violations de données
  - Réduire les vulnérabilités du personnel
  - Relations avec les tiers
  - Superviser le protection de la vie privée

Privacy Impact Assessment (PIA)

Méthode

pour se mettre en **conformité**

et le **démontrer**

Principes

fixés par la loi

non négociables

aucune modulation

Mesures techniques

et **organisationelles**

pour **protéger les données et les personnes**

Quand mener un PIA ?

- PIA obligatoire :
  - Liste CNIL des cas obligatoires
  - Au moins 2 critères parmi :
    - Évaluation/*scoring*
    - Décision automatique avec effet légal
    - Surveillance systématique
    - Données sensibles
    - Large échelle
    - Croisement de données
    - Personnes vulnérables
    - Usage innovant
    - Transfert hors UE
    - Blocage d'un droit/contrat
  - 1 critère, mais traitement à risque

+ Consultation de la CNIL
en cas de risques résiduels élevés

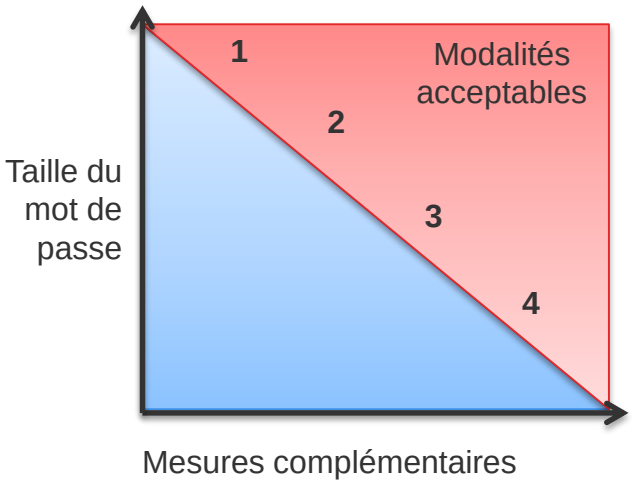
- PIA non obligatoire :
  - Liste CNIL des cas non obligatoires
  - Pas susceptible d'engendrer des risques élevés
  - Déjà autorisé (tant que le traitement n'a pas changé et que les conditions de mise en œuvre sont respectées !)
    - Autorisations unitaires
    - Formalités simplifiées
  - Base légale, nationale ou UE, avec un PIA déjà mené

La sécurité en pratique

PRÉCISIONS SUR CERTAINES MESURES DE SÉCURITÉ

LE MOT DE PASSE

Recommandation CNIL : mots de passe



1. Mot de passe seul (ex : *webmail*)
   - Au moins **12 caractères**
2. Mot de passe et blocage (ex : site de e-commerce)
   - Au moins **8 caractères**
3. Mot de passe et info complémentaire (ex : banque en ligne)
   - Au moins **5 caractères**
4. Mot de passe et matériel (ex : carte bancaire)
   - Au moins **4 chiffres**

Authentification forte

- Qui je suis : identifiant (login)

- + Deux facteurs d'authentification (*ou plus*) parmi :
  - Ce que je sais : authentifiant (mot de passe)
  - Ce que je possède : badge, carte à puce, certificat, accès VPN…
  - Ce que je suis : empreinte biométrique, signature, …

Authentification des PS

- Actuellement, authentification forte des professionnels accédant aux données médicales du patient
  - Utilisation de la carte CPS ou tout moyen équivalent d'authentification forte

- L'ASIP a publié un référentiel d'authentification qui détaille les différents dispositifs.
  - Ce référentiel est rattaché à la PGSSI-S
  - Il a vocation à être rendu opposable par un arrêté, pris après avis de la CNIL

Gestion fine des habilitations

- Seules les personnes ayant le besoin d'en connaître dans le cadre de la prise en charge du patient peuvent accéder au dossier médical
  - Médecin, infirmier, secrétaire, prestataire dans certains cas…

- Mise en œuvre d'une procédure type « bris de glace » pour les cas d'urgence

- Traçabilité des interventions (avec intégrité des traces)
  - Traces fonctionnelles, techniques et embarquées

Confidentialité des données

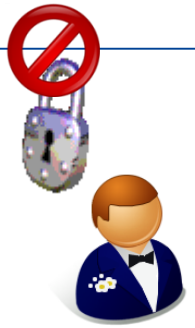
- Vis-à-vis de l'extérieur :
  - Chiffrement des canaux de communication (HTTPS, SMTPs…)

  - Chiffrement des supports de stockage amovibles :
    - ordinateurs portables, smartphones,
    - clés USB, disques externes …

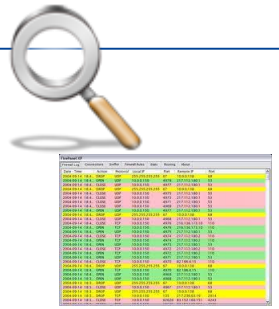
Confidentialité des données

- Télémaintenance
  - Par défaut le prestataire ne peut pas se connecter
    - **action positive préalable du responsable**
    - **accord** du médecin pour les données médicales
  - Compte rendu d'intervention et **traçabilité**

Prestataire



Responsable



Confidentialité des données

- Intervention physique :
  - Tenue d'une **main courante**
  - Interventions **en présence d'un responsable**
  - Support pour réparation : Effacement sécurisé
  - Support pour remplacement : Destruction

Confidentialité des données

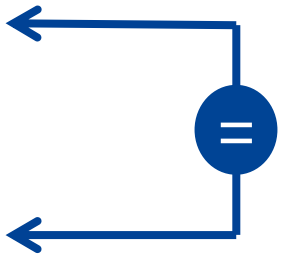
- Vis-à-vis de l'intérieur :
  - Administrateurs systèmes et gestionnaires de bases de données :
    - Chiffrement des données en base (plusieurs modes de chiffrement peuvent être implémentés)
    - Chiffrement des documents contenant des données de santé individuelles
  - Équipes de développement :
    - Utilisation de données fictives ou anonymes pour les tests logiciels

La minimisation des données

- Filtrage et retrait
  - ex. données EXIF d'une photo
- Réduction de la sensibilité par transformation
  - ex. remplacer l'adresse par la région
  - ex. cumuler les données sur une période de temps
- Réduction du caractère identifiant des données
  - Données anonymes, ou pseudonymes (si besoin de traçabilité)
- Réduction de l'accumulation de données
  - Scinder les données (ex. données de santé / état civil des patients)
  - Purger les données (durées de conservation)

La pseudonymisation

- La pseudonymisation permet la **traçabilité**
  - Exemple : Jean → 100073
    Paul → 233304
    Caroline → 328923
    Jean → 100073



- La pseudonymisation n'est **pas une anonymisation**
- Solutions techniques :
  - Table de correspondance secrète : réversible (difficile à sécuriser)
  - Chiffrement : réversible
  - Hachage : irréversible
  - Hachage avec clé secrète : évite les attaques dites de « dictionnaire » (attention à protéger la clé secrète)

Pourquoi anonymiser ?

- Le RGPD **ne s'applique pas aux données anonymisées, ce qui permet ou simplifie** :
  - l'utilisation de données **hors de leur finalité d'origine** ou **au-delà du délai de conservation** prévu ;
  - Le **transfert de données sans formalités** hors « pays adéquats » ;
  - la **mise à disposition de fichier au grand public** sur Internet (« open data ») ;
  - la réalisation de **jeux de test** pour le développement de logiciels ou pour des formations ;
  - la création de jeux de données pouvant être utilisés **à des fins de recherche** et **largement diffusés**.

Critères d'anonymisation

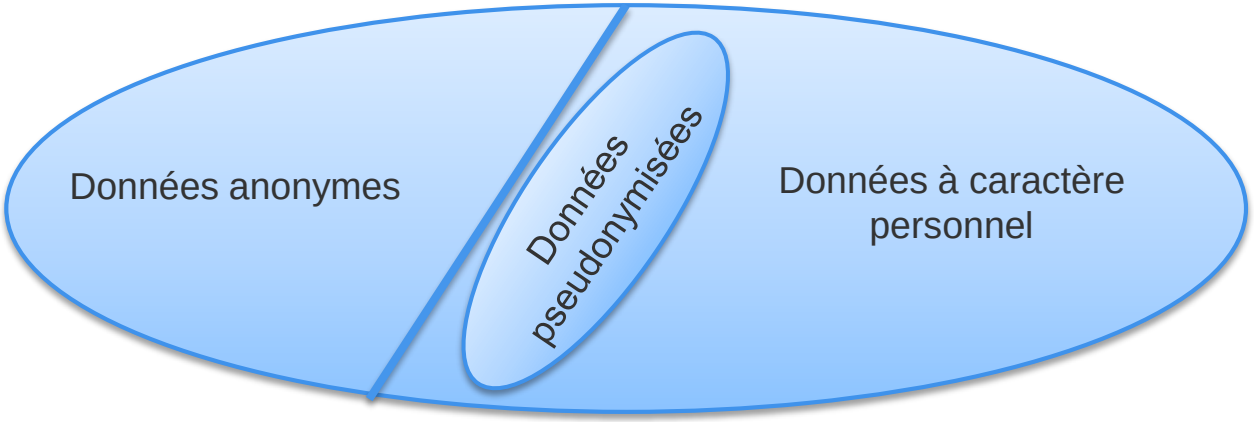
- **Selon l'avis 05/2014 du G29**, un jeu de données est anonyme :
  - **s'il est démontré qu'il n'est pas possible :**
    - d'**isoler** des informations relatives à un seul individu ;
    - ni de **relier** les données d'un même individu ou groupe d'individus ;
    - ni de **déduire** d'un ensemble d'attributs la valeur d'un autre attribut.
  - **OU si une analyse de risques de ré-identification** a été effectuée à la satisfaction des autorités compétentes.
    - En France, cela signifie des risques résiduels nuls.

L’anonymisation en pratique

- Déterminer l’objectif et les usages des données anonymes
  - Pourquoi est-ce que je veux des données anonymes ?
  - A quoi les données vont-elles servir ?
- Évaluer si l’anonymisation est réellement l’objectif à atteindre
  - A-t-on besoin d’information au niveau des individus ?
  - A-t-on suffisamment d’individus concernés pour garder les attributs intéressants ?
  - Est-on prêt à perdre de l’information ?
- Préparer les données
  - Supprimer les éléments d’identification directe et les valeurs rares
  - Définir les attributs importants / secondaires / supprimables
  - Définir la granularité optimale et acceptable pour chaque attribut à conserver
  - Définir les priorités
- Appliquer les techniques
  - Ajout de bruit, permutation, généralisation (former des groupes)
- Effectuer une veille des techniques d’anonymisation et de ré-identification
  - Le risque de ré-identification augmente avec le temps

Anonymisation, en résumé…

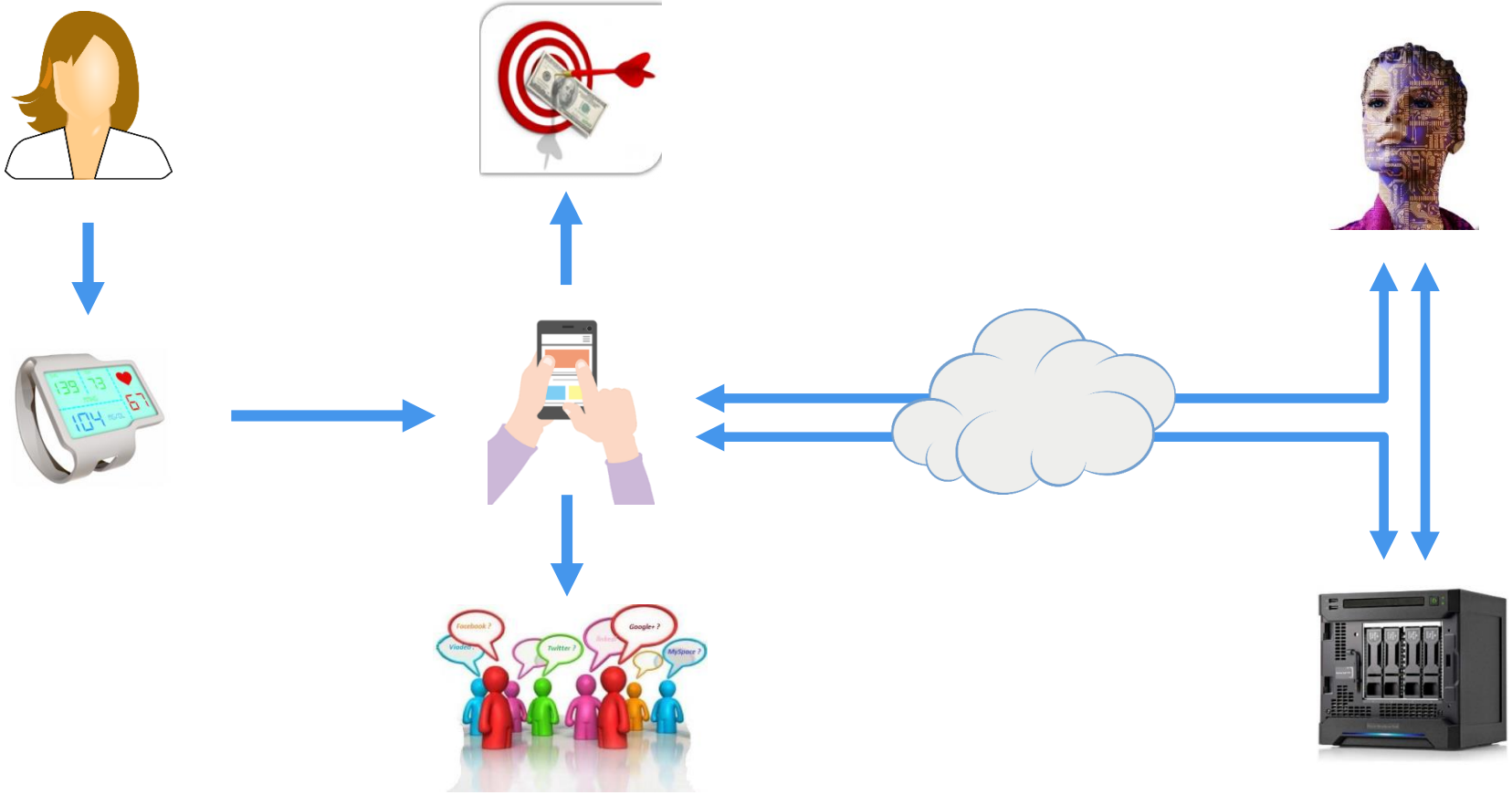
- Une donnée anonyme **n'est plus** une donnée à caractère personnel
- Le **processus d'anonymisation est un traitement de données** à caractère personnel (donc soumis aux obligations)
- Le processus d'anonymisation implique un **appauvrissement** des données brutes et une **restriction** du champ des exploitations possibles
- Un jeu de données **pseudonymisé n'est pas anonyme** mais offre une protection des données



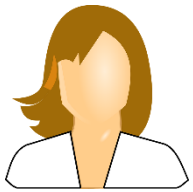
La sécurité et le PIA en pratique

ILLUSTRATION SUR UN OBJET CONNECTÉ

Objet connecté
Parcours des données



Objet connecté
Principes fondamentaux



Transparence
Consentement

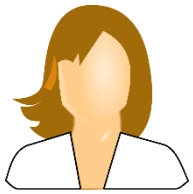
Transparence
Consentement

Finalité
Contrat, CGU
Consentement

CGU
Consentement

Information, consentement
HDS, Transferts hors UE
Conservation limitée
Droits (accès, rectification, portabilité, effacement limitation, opposition)

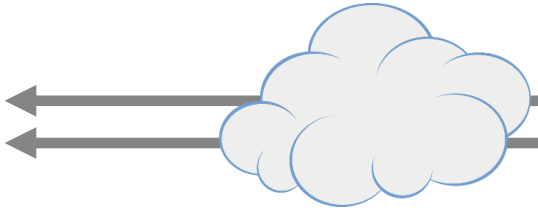
Objet connecté
Sécurité des données



Cookies

Pseudonymisation

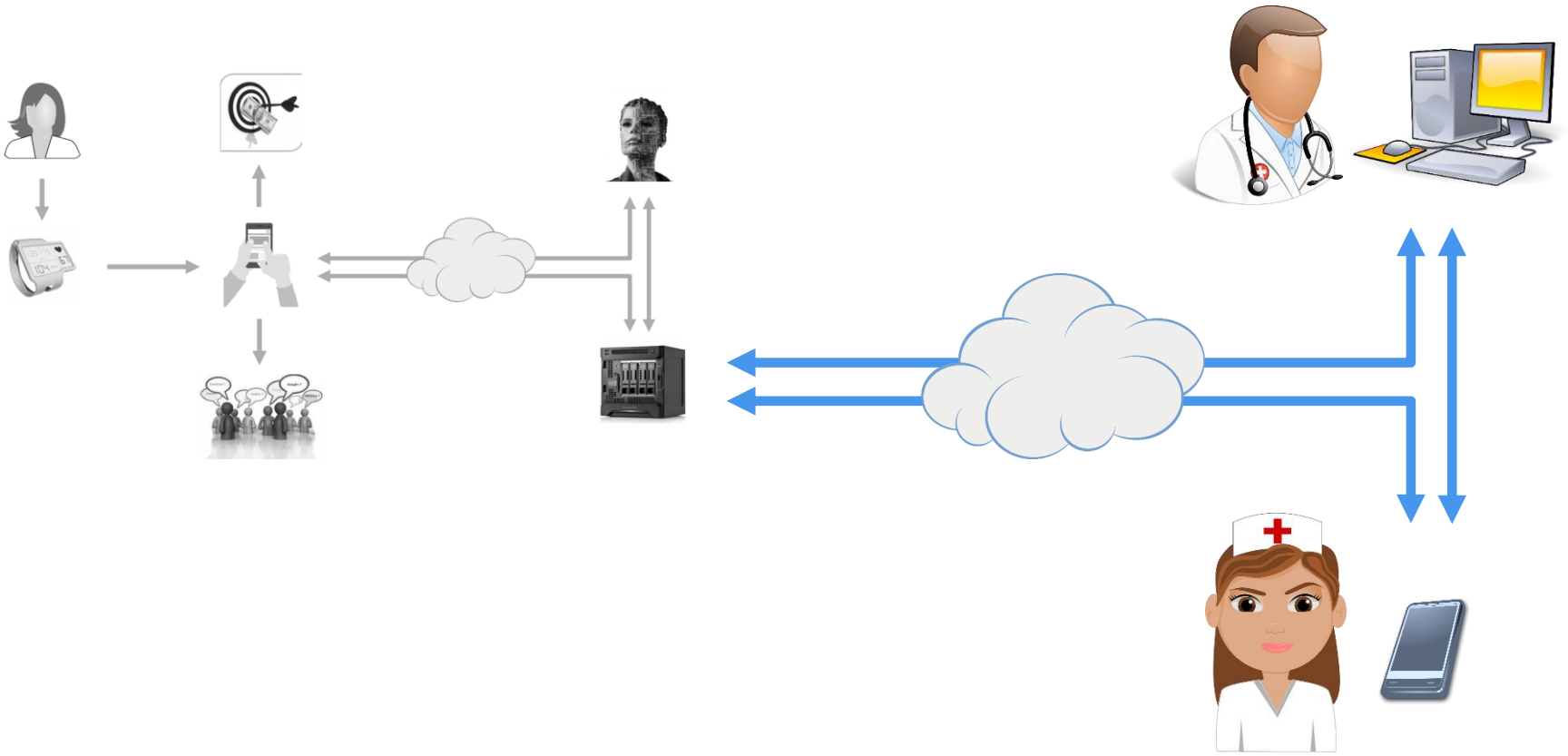
Minimisation
Exactitude
Mise à jour



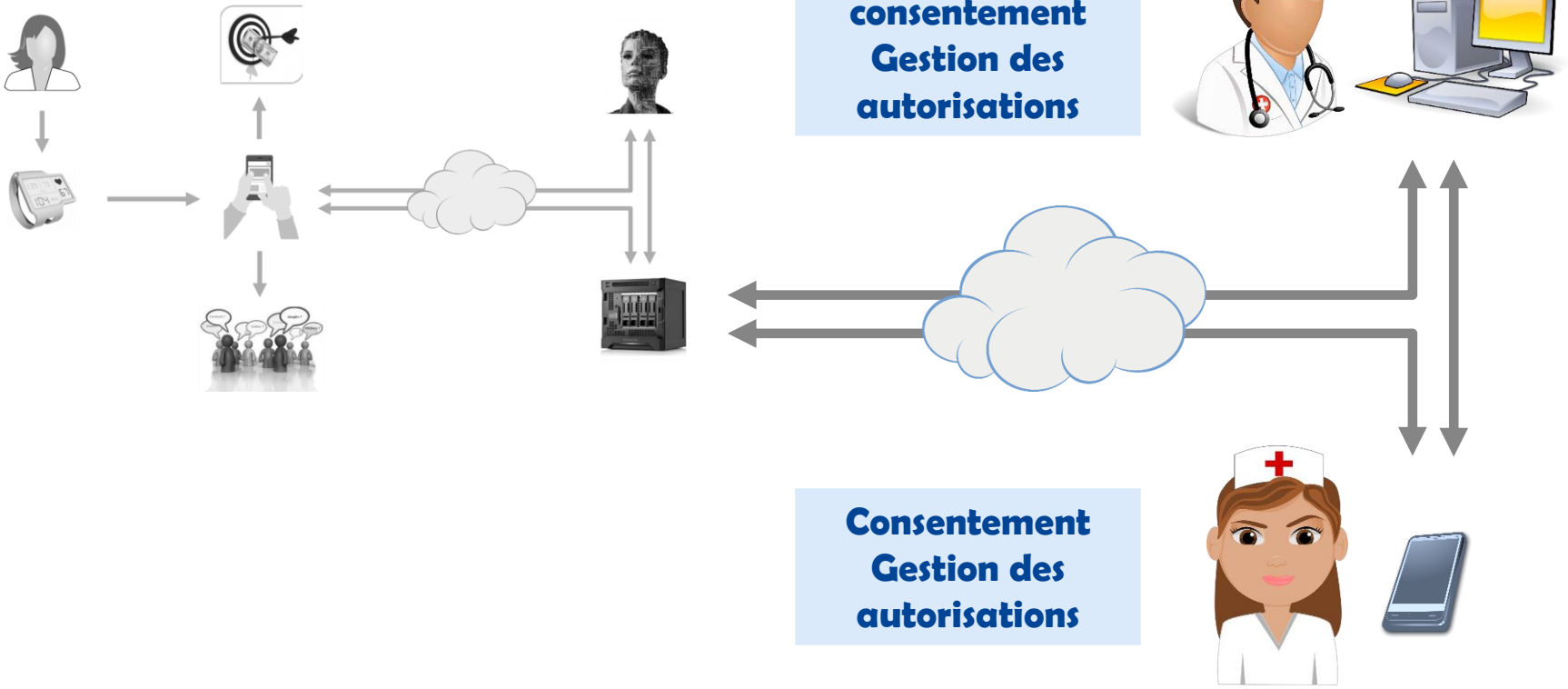
Réglages de confidentialité

Chiffrement
Minimisation
Pseudonymisation
Durée de conservation

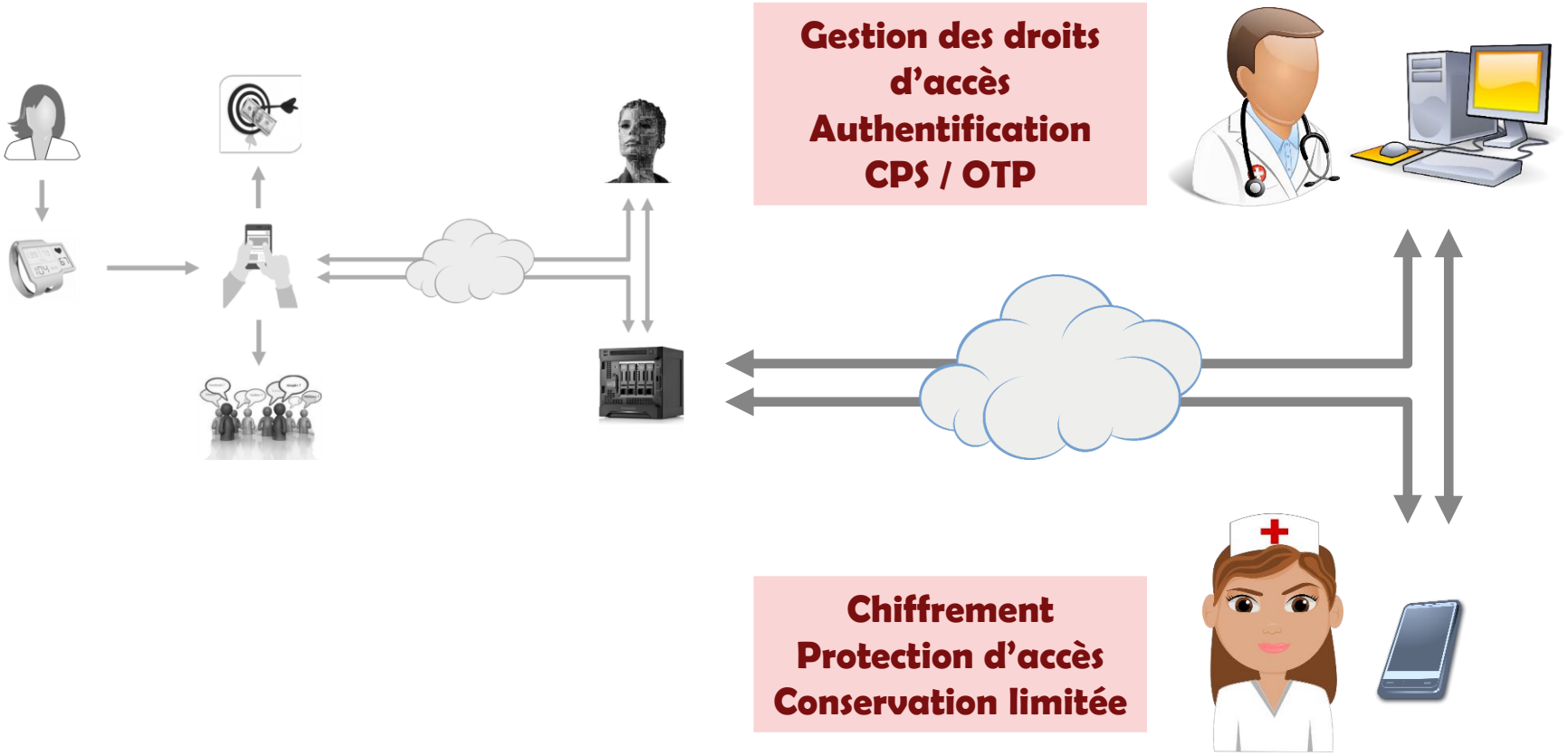
Parcours de soins
Parcours des données



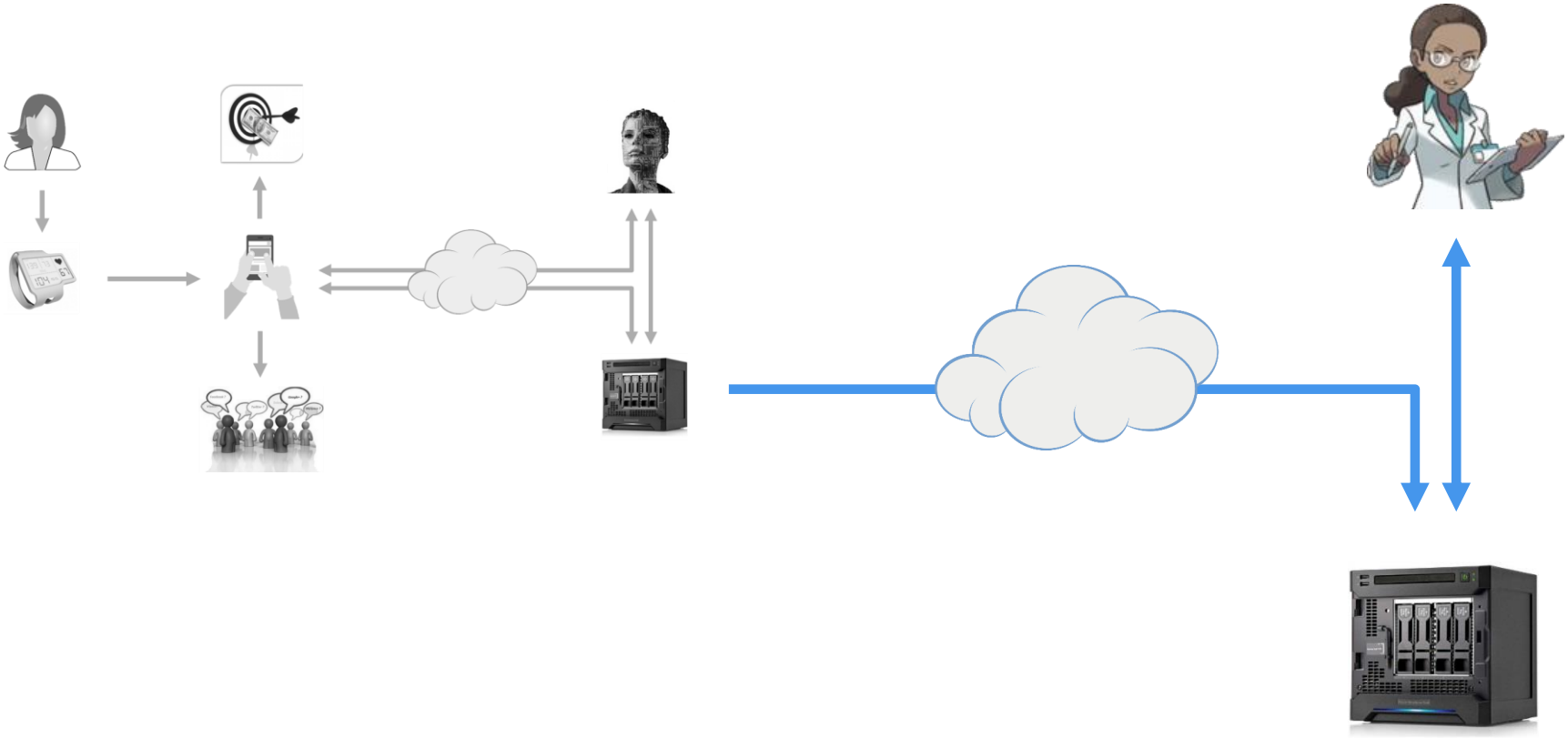
Parcours de soins
Principes fondamentaux



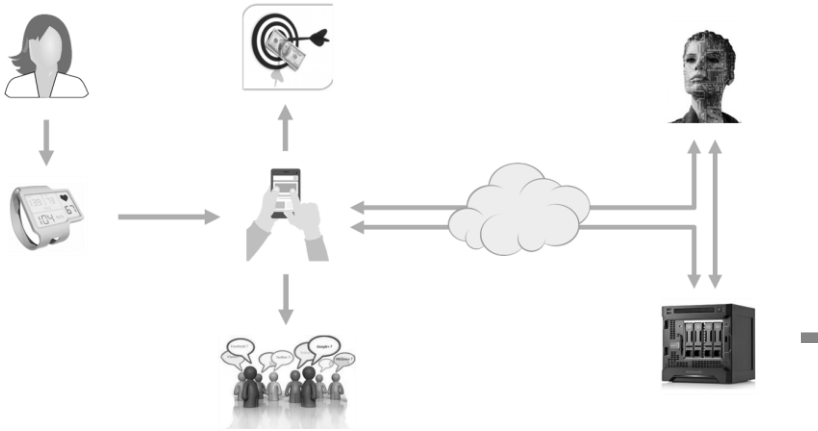
Parcours de soins
Sécurité des données



Utilisation en Recherche
Parcours des données



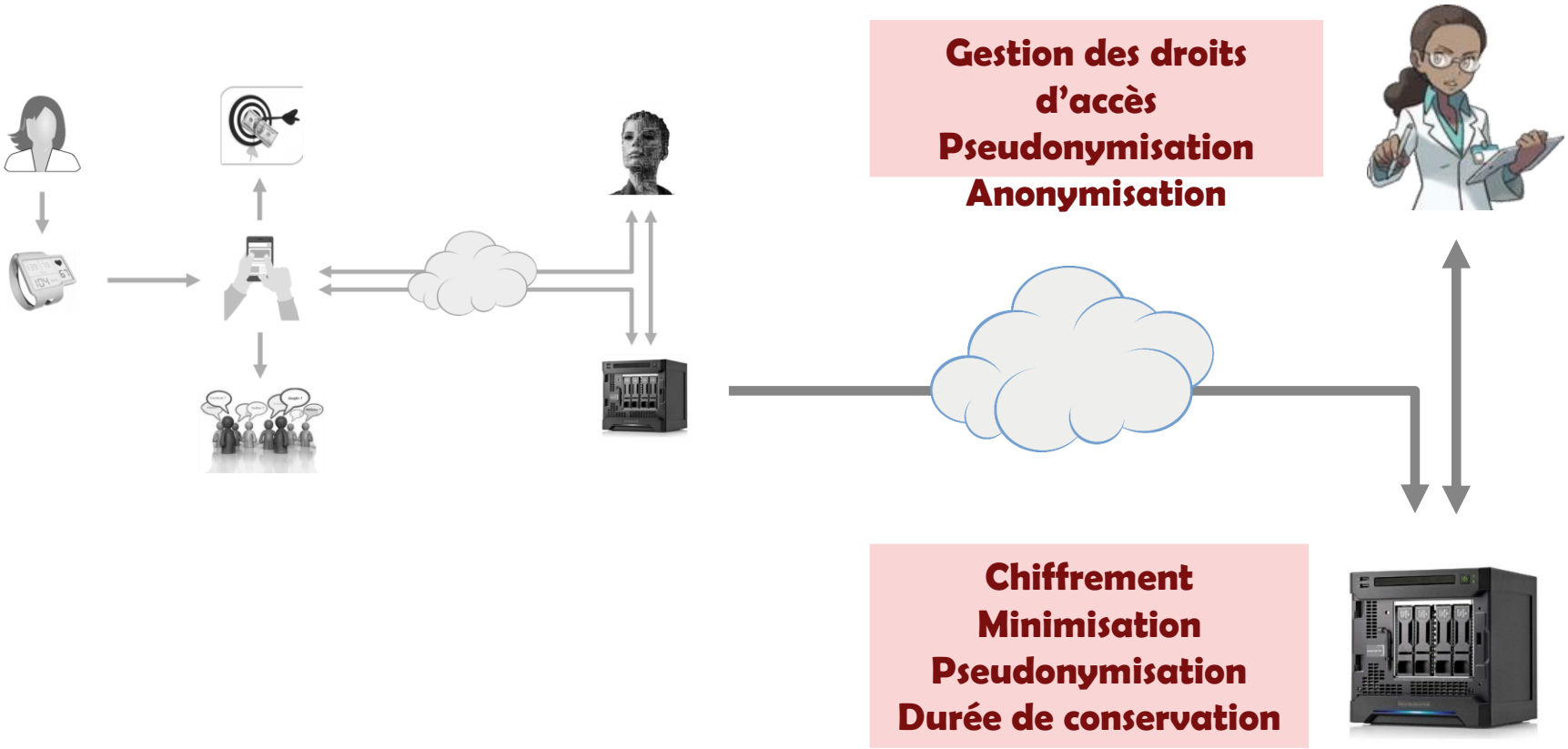
Utilisation en Recherche
Principes fondamentaux



Transparence
Consentement

Information, consentement
Transferts hors UE
Conservation limitée
Droits (accès, rectification, portabilité, effacement limitation, opposition)

Utilisation en Recherche
Sécurité des données



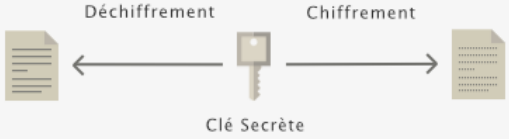
Protection des données personnelles, RGPD, PIA…

LA CNIL VOUS ACCOMPAGNE

Les fiches pratiques

CONFIDENTIALITÉ

Comment fonctionne le CHIFFREMENT ?



CHIFFREMENT SYMÉTRIQUE

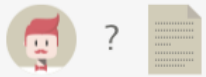
Le chiffrement symétrique permet de chiffrer et déchiffrer un fichier avec la même clé, dite secrète. Pour s'échanger un message il faut donc que les deux parties partagent la même clé.

MISE EN PRATIQUE

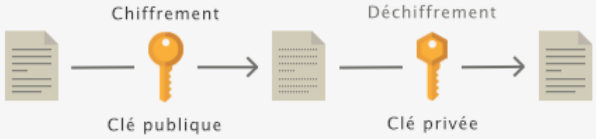
Alice vient d'enregistrer la liste des cadeaux de Noël de sa famille sur l'ordinateur familial. Elle souhaite être la seule à pouvoir y accèder.

1. Pour ce faire, Alice chiffre la liste en utilisant sa clé secrète.

2. Plus tard dans la journée, Bob trouve la liste et cherche à l'ouvrir.



3. Malheureusement pour lui, Bob est incapable de



CHIFFREMENT ASYMÉTRIQUE

Le chiffrement asymétrique repose sur l'utilisation d'une paire de clés : une publique et une privée.

La clé publique, accessible à tous, est utilisée pour chiffrer les fichiers. Seule la clé privée permet de déchiffrer ces fichiers, celle-ci étant connue que d'un seul individu.

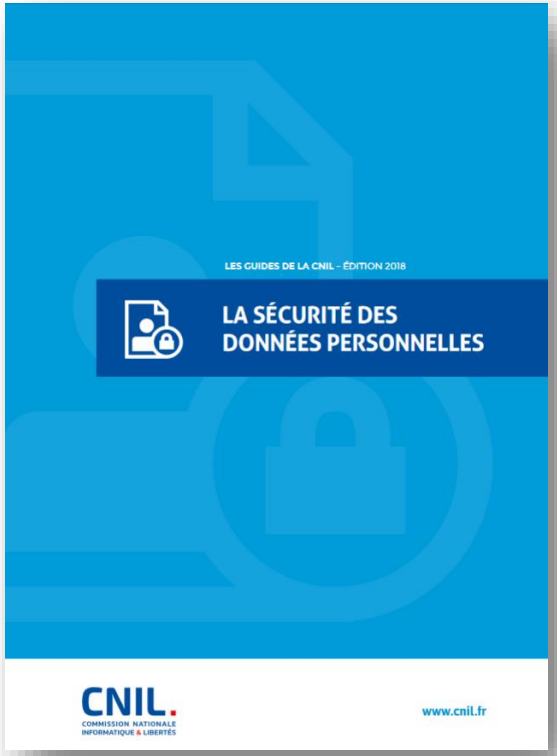
MISE EN PRATIQUE

Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.

1. Alice vient de récupérer la clé publique de Bob. Elle l'utilise pour chiffrer son document.

2. Elle l'envoie à Bob.

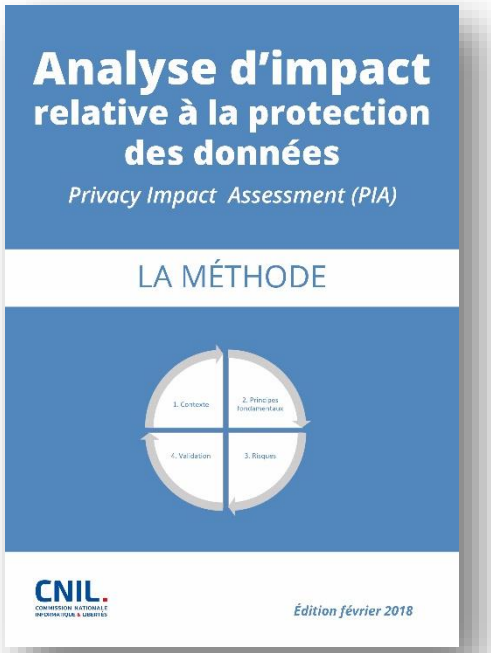
Le guide sécurité

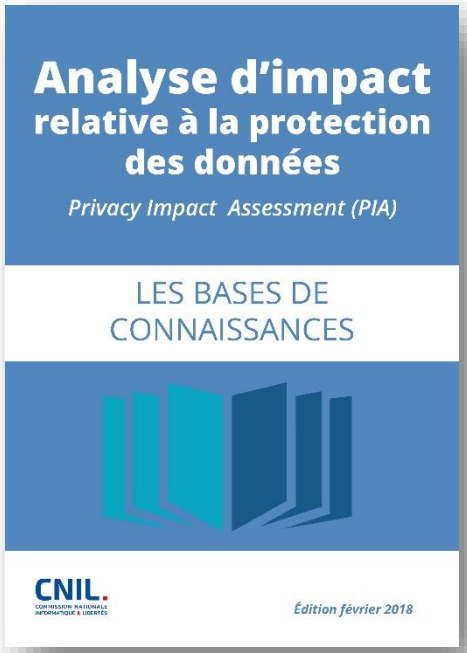


- Pour intégrer la **protection de la vie privée** et la **cybersécurité.**
- Pour faire du ***Privacy by design***…

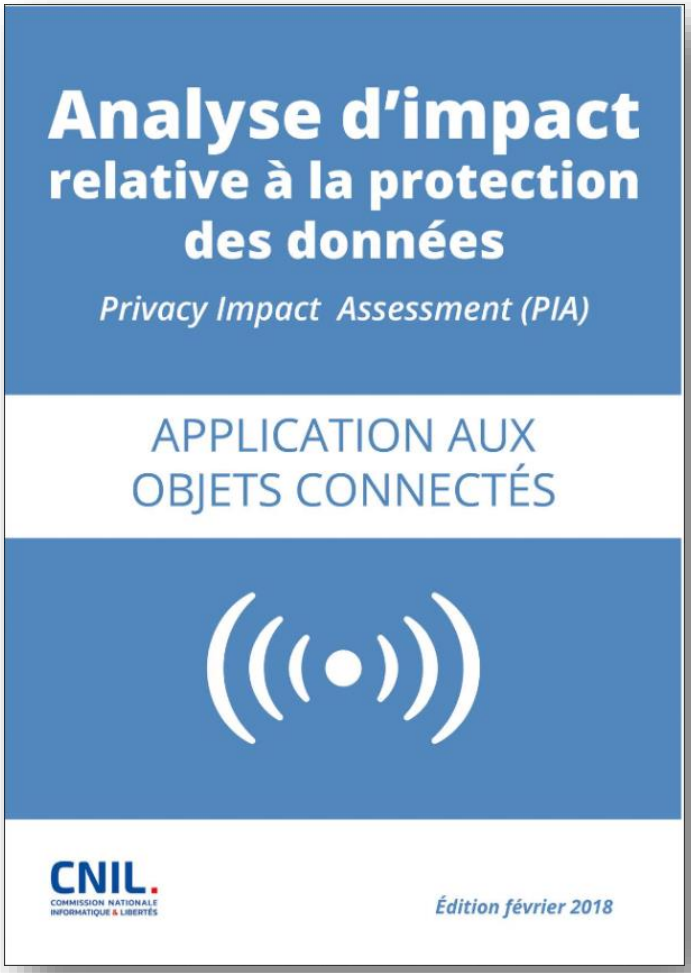
Les guides PIA de la CNIL

- Pour intégrer la **protection de la vie privée** et la **cybersécurité.**
- Pour faire du ***Privacy by design***…
- **Nouvelles versions adaptées au RGPD**





Exemple et modèle de PIA



Le logiciel PIA de la CNIL

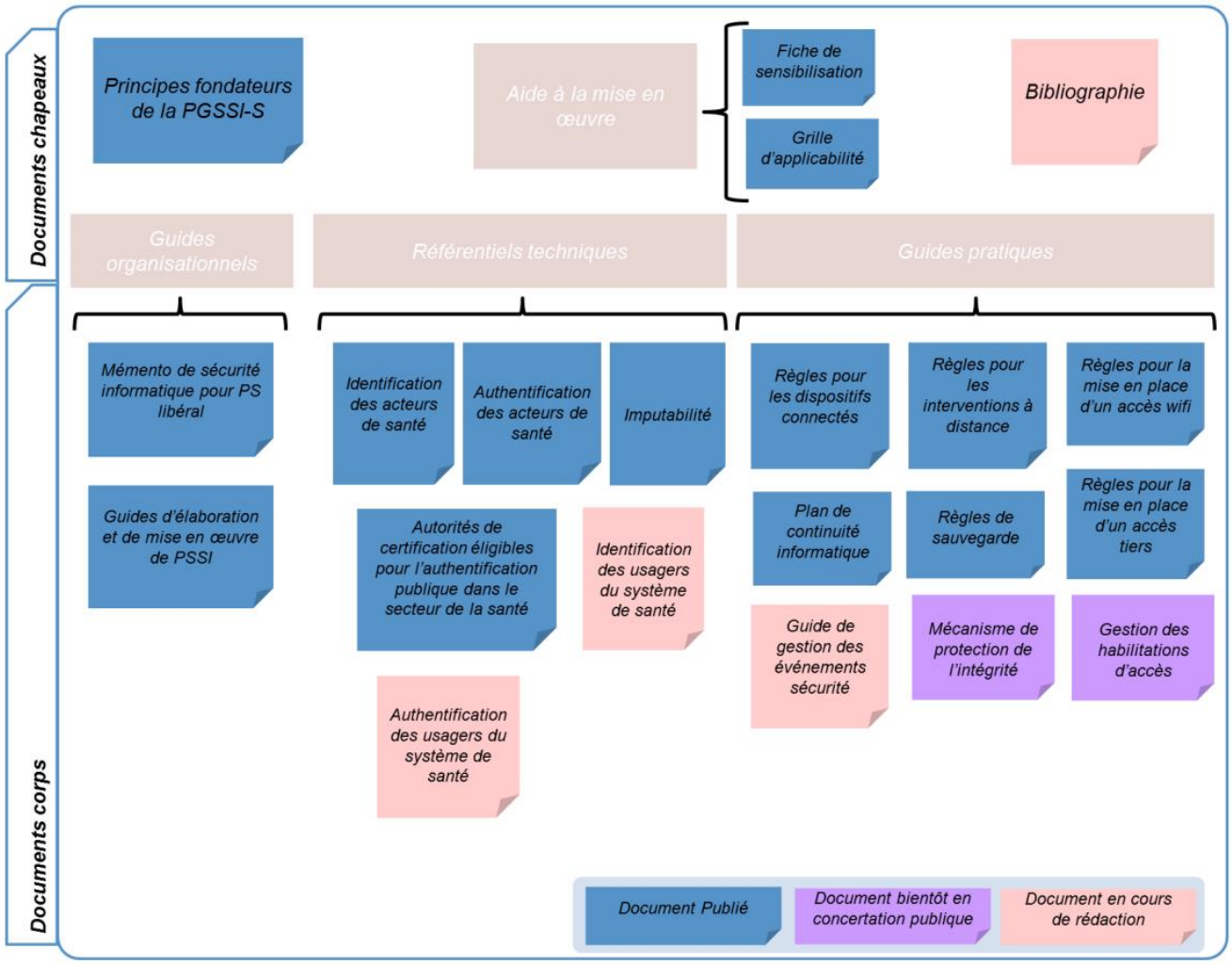
- Principales caractéristiques
  - Aider les entreprises qui ne disposent pas d'un outil
  - Solution **simple**, *user-friendly*
  - Logiciel **libre** et ***open source***, en français et en anglais
  - **Bases de connaissances** pour les principes de protection de la vie privée
  - **Cartographie des risques** et de leurs composantes
  - **Réutilisation** des PIAs

mHealth : bonnes pratiques

La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)

17 documents

575 pages



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Dossiers complets sur « www.cnil.fr »

www.cnil.fr/fr/sante

www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-pia

---

Merci de votre attention ☺

Abonnez-vous à la newsletter !