CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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

Cyber-risques et mesures de sécurité

Gouvernance de la protection des données

Erik BOUCHER de CREVECOEUR, ingénieur-référent santé, service de l'expertise technologique, CNIL

Soben CHHEM, responsable de la sécurité des systèmes d'information, Université de Bordeaux

Valérie ALTUZARRA, directrice du pôle qualité gestion des risques et prévention et directrice des systèmes d'information et du numérique, CHU de Bordeaux

Cybersécurité :
Les tendances actuelles

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…)*

L'évolution des menaces

- **Professionnalisation et spécialisation de la sphère criminelle**
  - **Crime organisé déterminant avec précision ses cibles**

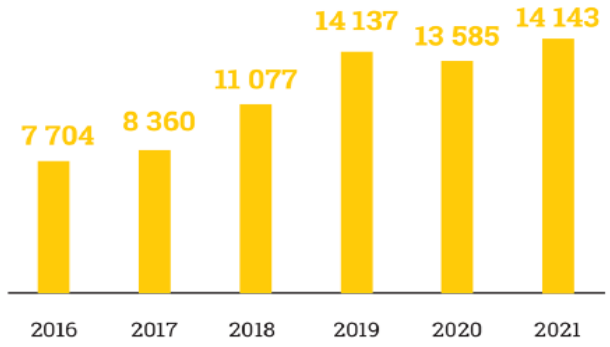
- Très forte augmentation de la menace, notamment rançongiciels :
  - **Chiffrement malveillant de données**
  - **Et aussi : exfiltration de données personnelles**

- L'hameçonnage reste un vecteur d'attaque majeur
- Forte progression des **attaques sur les boîtes mails** (dont Microsoft 365)

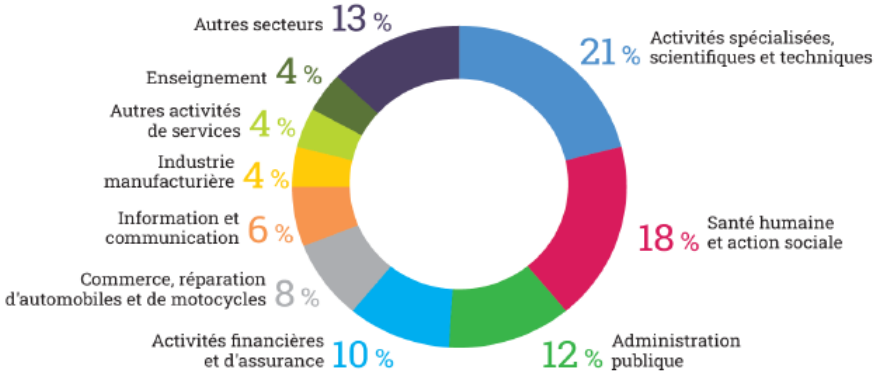
Les tendances observées depuis mai 2018

- **Multiplication des usages et du volume de données** (outils numériques, indicateurs, recherche, etc.).
- **Hausse constante du nombre de violations de données** : 5.000 notifications en 2021; l'attaque la plus répandue reste le rançongiciel : 43 % des notifications; ¼ de ces notifications concerne le secteur de la santé et de l'action sociale)
- **Augmentation du nombre de plaintes** : en 2021, env. 14. 000 plaintes (soit 2/3 d'augmentation depuis mai 2018; +4% depuis 2020)
- Prise en compte progressive de la sécurité et de la protection des données dans les **mesures de financement**

Nombre de plaintes par année



Part de notifications par secteur d'activités



Les violations de données

- La CNIL a reçu **5037** notifications de violations de données à caractère personnel sur l'année 2021, contre **2821** en 2020 correspondant à une **augmentation de 79%.**

- **22% des notifications** concernent des **données sensibles** (les catégories particulières de données définies à l'article 9 du RGPD).

- Le **secteur de la santé** et de l'action sociale est le **troisième secteur** en nombre de notifications reçues.

- La majorité (**69%**) des notifications de violations reçues par la CNIL concerne une **perte de confidentialité.**

- Nette progression des notifications liées à une **perte d'intégrité et de disponibilité**, notamment due à la progression des attaques par **rançongiciel.**

- En 2021, le **piratage informatique a représenté 59% du total** des notifications, soit 2993 notifications contre 1313 en 2020 (**soit une hausse de 228%**)

- Plus de **14 700 000 personnes** informées de l'existence d'une violation en 2021.

Les actions de la CNIL

- **Mises en demeure** (publiques ou non)
- **Sanctions** pour des manquements à la sécurité des données :
  - **Transmissions de données non sécurisées**
  - **Absence de mesures de limitations d'accès**
  - **Défaut de chiffrement**
  - **Politique de mot de passe non conforme**

- **Accompagnement et prévention** :
  - https://www.cnil.fr/fr/multiplication-des-attaques-par-rancongiciel-comment-limiter-les-risques
  - https://www.cnil.fr/fr/cybersecurite

Les sanctions CNIL et la sécurité des données

Les sanctions de la CNIL en 2021

2021
214 106 000 €
+ 55 %

La moitié des sanctions concerne en partie une **mauvaise sécurité des données**

4 décisions de la CNIL en coopération avec d'autres **autorités européennes**

17 dossiers européens **examinés par la CNIL**

Outre la sécurité, parmi les manquements les plus fréquents figurent :

- **le défaut d'information des personnes**
- **des durées de conservation excessives**

https://www.cnil.fr/les-sanctions-prononcees-par-la-cnil

Les actions prioritaires

CNIL.

Les actions prioritaires

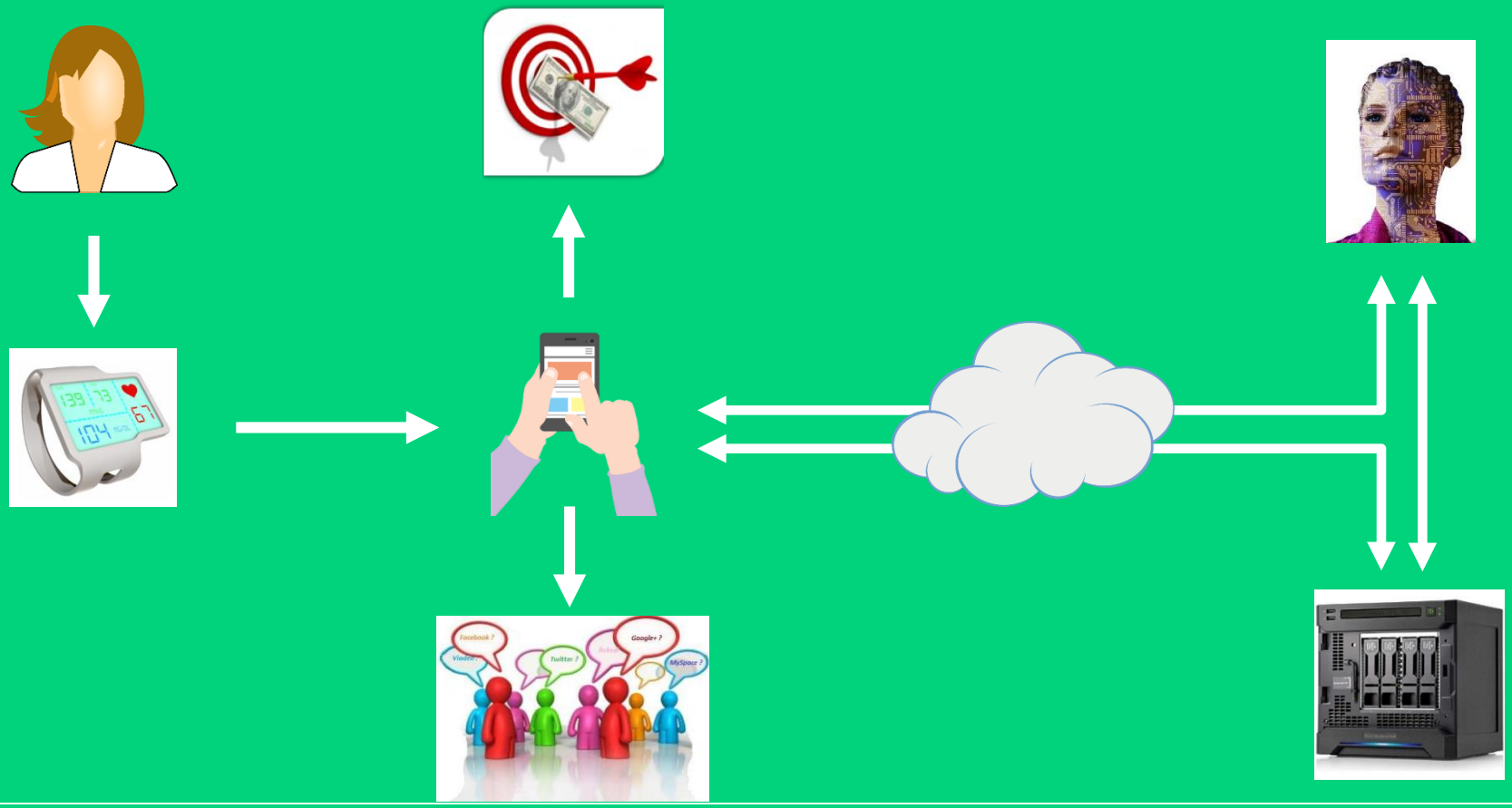
LES MESURES DE SÉCURITÉ SELON LES PARCOURS DE DONNÉES DE SANTÉ

Les mesures de sécurité fondamentales

- **Chiffrement** des données **au repos et en transit**
- **Pseudonymisation et cloisonnement des données identifiantes**
- **Authentification forte** des accès (par ex. avec un code temporaire ou une carte à puce) qui permet de protéger et de tracer l'utilisation des données
- **Contrôle proactif et régulier des traces**

Objet connecté

Parcours des données



LINC
CNIL.

Objet connecté
Sécurité des données

Minimisation
Exactitude
Mise à jour

Cookies

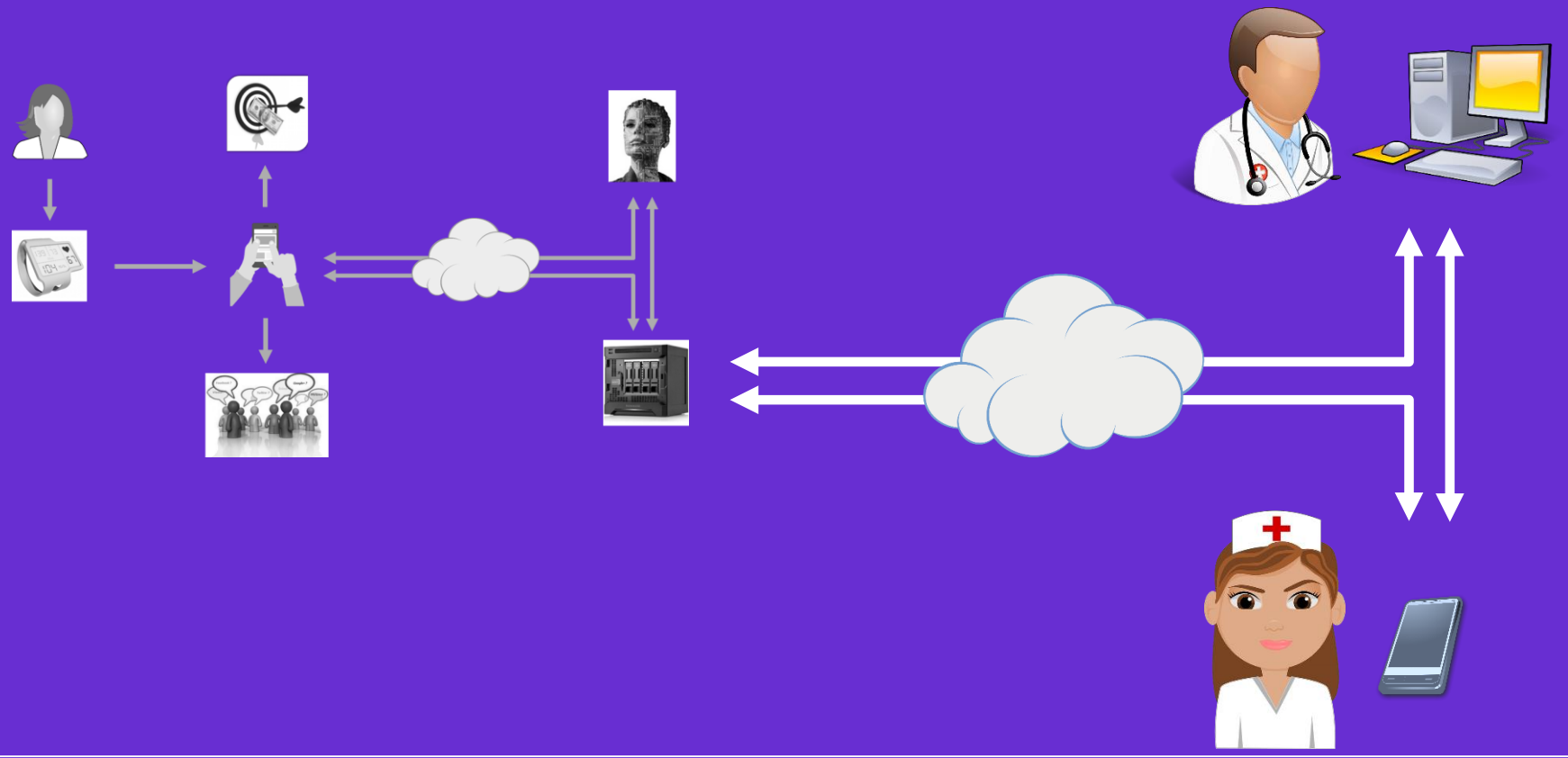
Réglages de confidentialité

Pseudonymisation

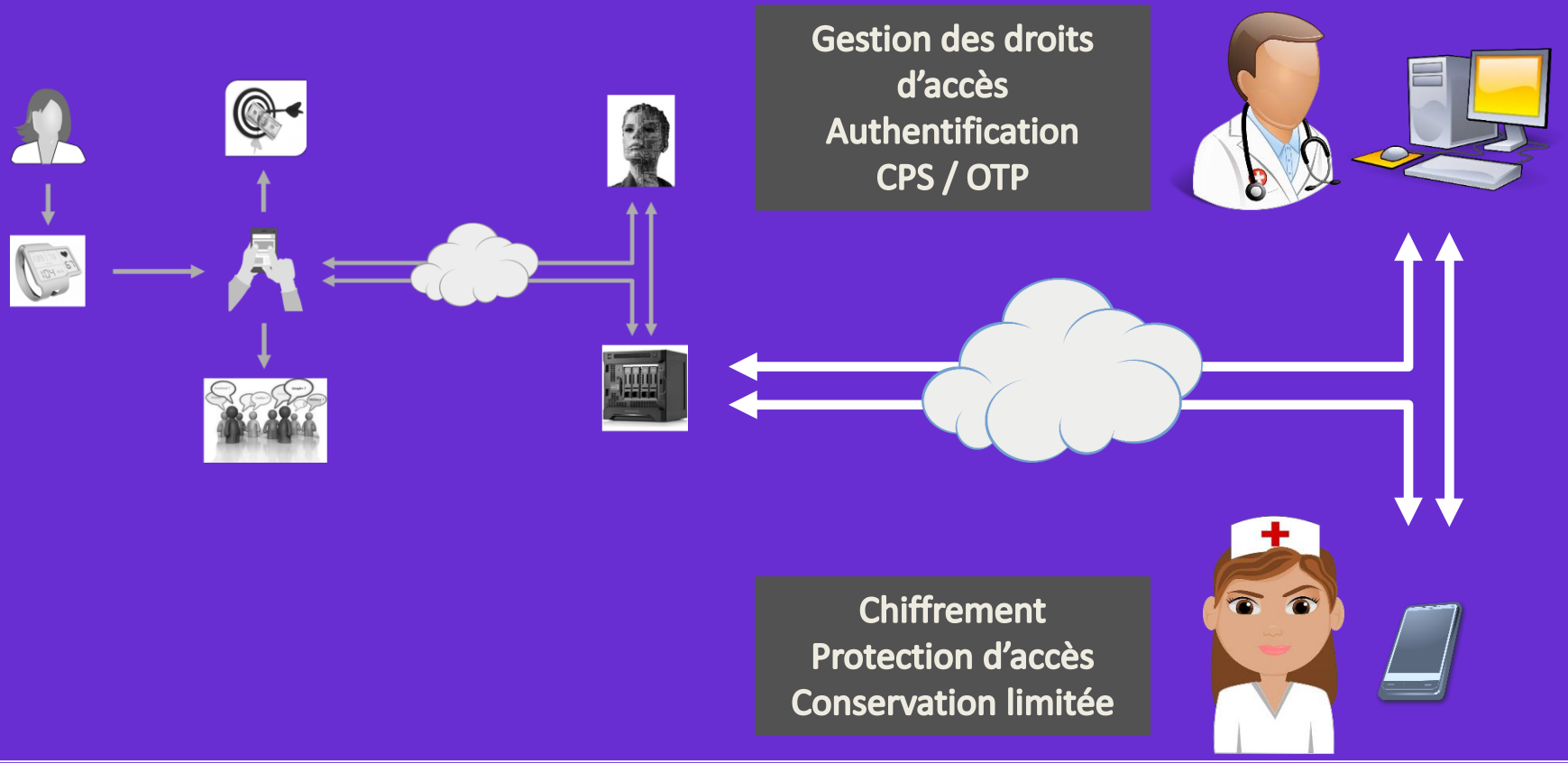
Chiffrement
Minimisation
Pseudonymisation
Durée de conservation
Gestion des incidents

LINC
CNIL.

Parcours de soins
Parcours des données

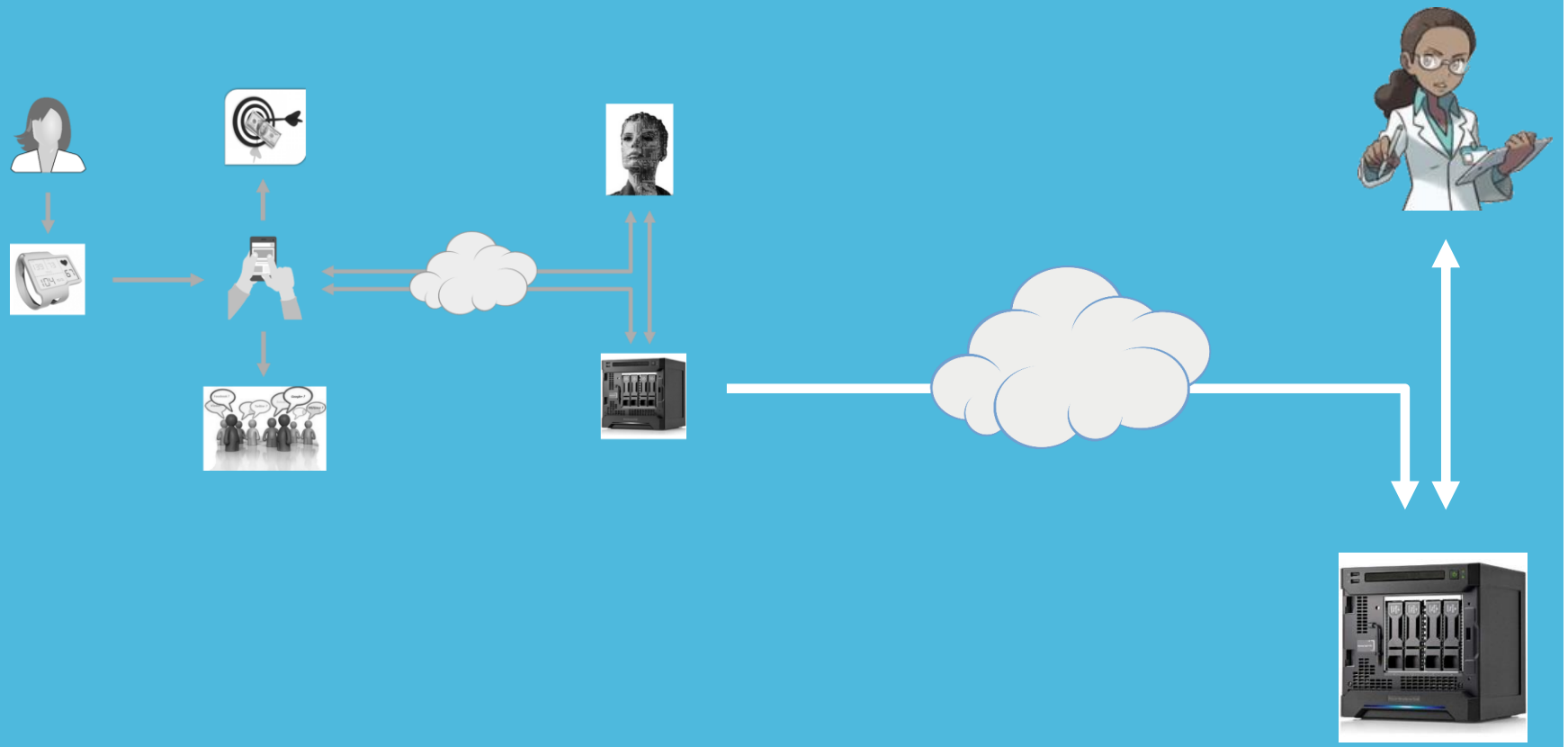


Parcours de soins
Sécurité des données



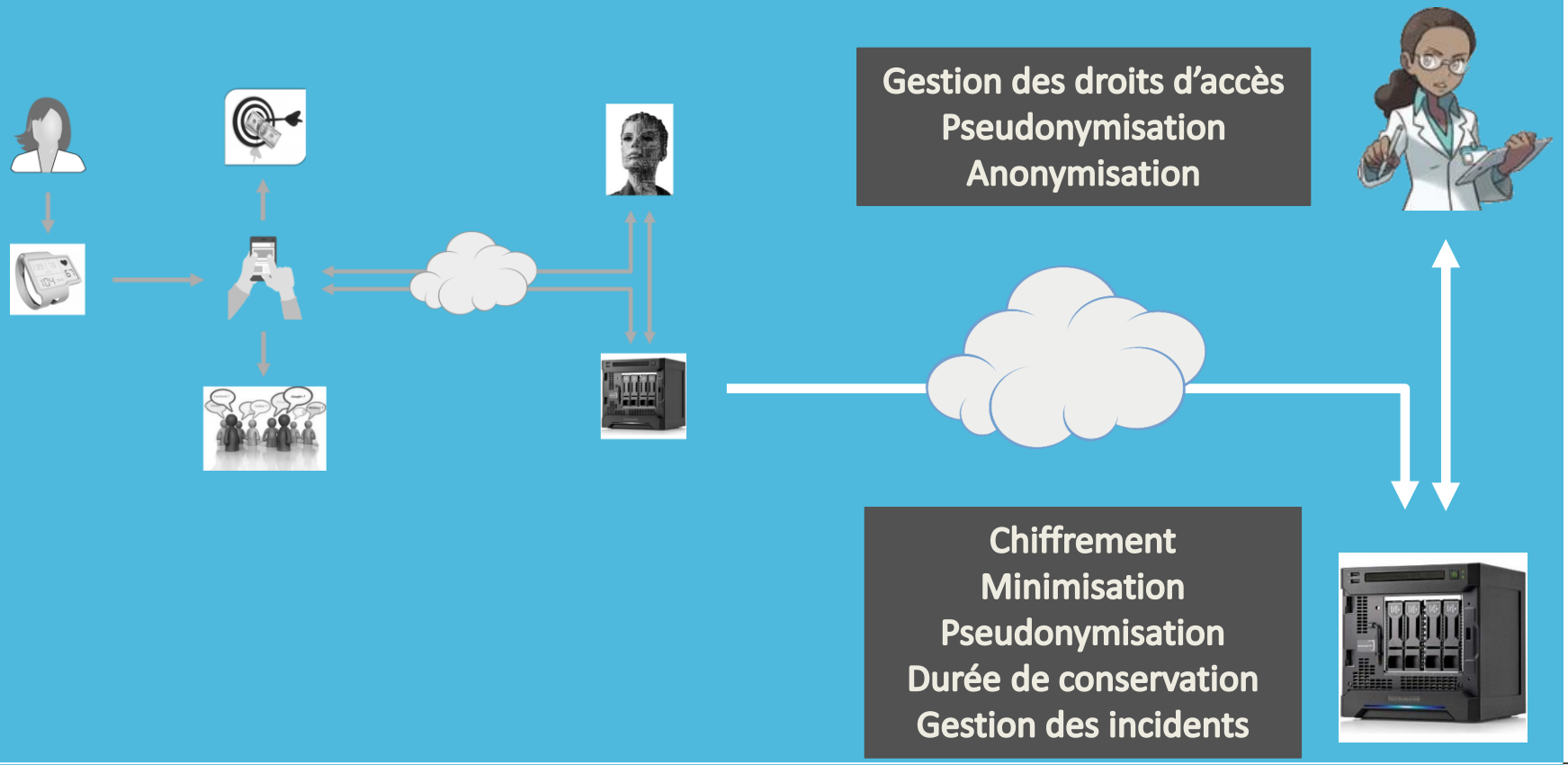
Utilisation en Recherche

Parcours des données



Utilisation en Recherche

Sécurité des données



CNIL.

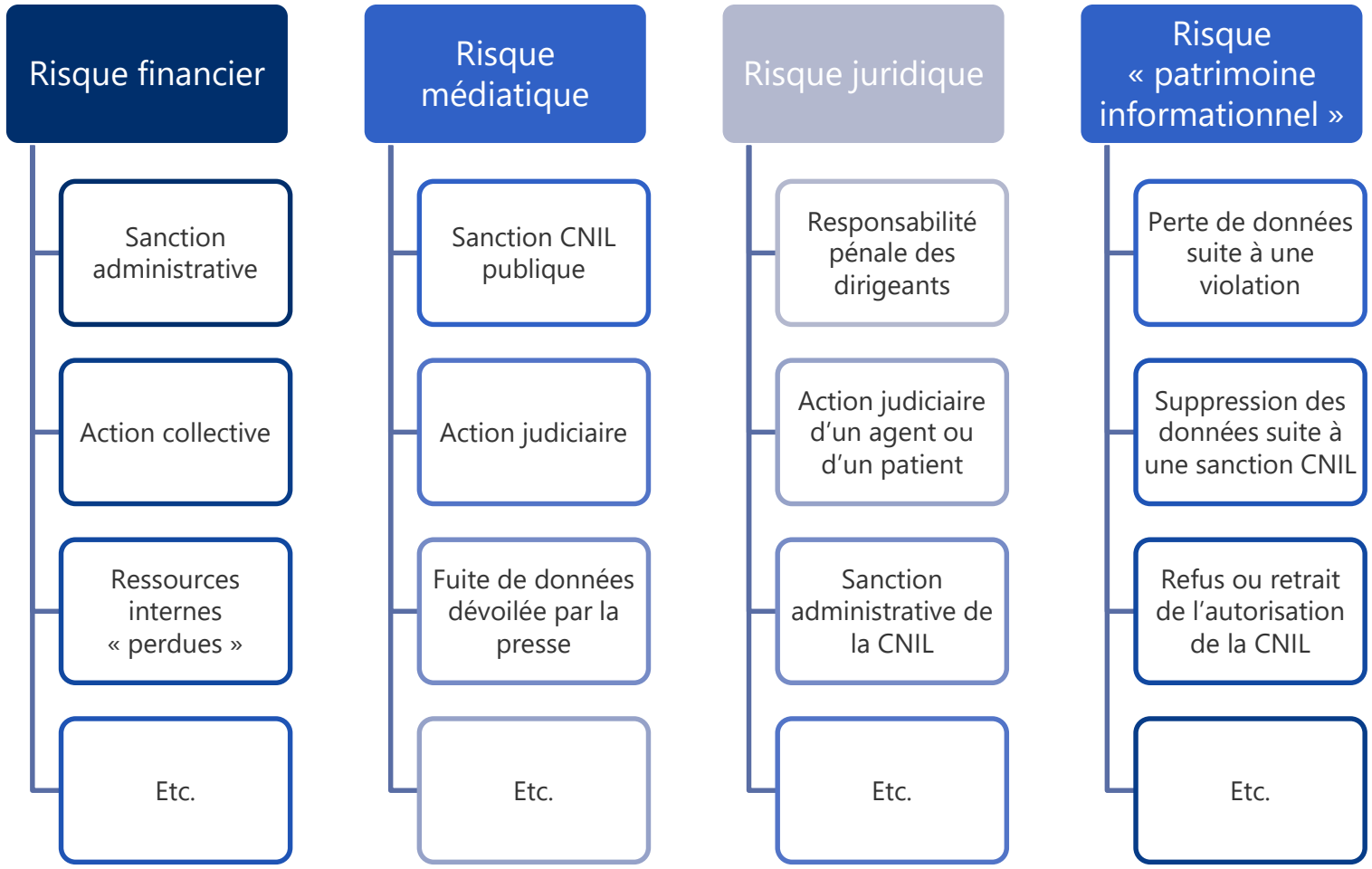
Les actions prioritaires
LA GOUVERNANCE DE LA PROTECTION DES DONNÉES

Une gouvernance pour créer de la confiance

Vis-à-vis du patient

Vis-à-vis du personnel soignant

Une gouvernance pour se protéger



Une gouvernance pour faciliter l'utilisation et la réutilisation des données

- **Procédures et outils** pour faciliter le lancement et la mise en œuvre de projets nécessitant d'utiliser des données (ex: portail de transparence « recherche », etc.)

- **Bénéficier des cadres de référence** (méthodologies de référence, référentiels, etc.) pour rationnaliser et faciliter les démarches

Une gouvernance prévue par les textes

- **De nombreux cadres réglementaires** en protection des données incluent aujourd'hui une logique de preuve :
  - RGPD : « Accountability » et PIA
  - Certification HDS et homologation SNDS
  - Homologation pour l'usage du téléservice INS
  - Référentiel d'identification des professionnels de santé
- La mise en place d'une gouvernance est le meilleur moyen de maintenir le niveau requis dans la durée
- Comme pour les processus « qualité », la protection de la vie privée nécessite une **démarche d'amélioration continue**

Une norme internationale pour la gouvernance de la sécurité et de la protection des données

ISO/IEC 27701:2019

- **Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices**
- *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

***NF** ISO/IEC 27701 : version française publiée en octobre 2020*

L'ISO 27701 complète les standards de Cybersécurité et permet la certification du respect de la vie privée

- **Approche intégrée** : le terme « sécurité de l'information » dans 27001 et 27002 doit être remplacé par « **sécurité de l'information et protection de la vie privée** »

- **Exigences spécifiques** pour un système de management de la protection de la vie privée (extension d'ISO 27001) :
  - Inclusion des données personnelles dans le **système de management**
    ⇨Privacy Information Management System (**PIMS**)
  - **Gestion des risques** sur la vie privée liés aux données personnelles

- **Lignes directrices spécifiques** pour les responsables de traitement et les sous-traitants (extension d'ISO 27002) :
  - Principes fondamentaux (bases légale, PIA…)
  - Droits des personnes
  - *Privacy by design and by default*
  - Partage, transfert et mise à disposition

Exemples d'exigences additionnelles à 27001

- Ajout au 4.1 : L'organisme doit **se déterminer** comme **responsable de traitement** ou comme **sous-traitant**
  - Annexe A : responsable de traitement
  - Annexe B : sous-traitants

- Affinement du 6.1.2 c) : Réaliser une **évaluation des risques** sur la **sécurité de l'information** et sur la **vie privée**, afin d'identifier les risques associés à la perte de confidentialité, intégrité et disponibilité ainsi que les risques liés au traitement de données personnelles

- Affinement du 6.1.2 d) : L'organisme doit **évaluer les conséquences,** y compris celles **pour la vie privée des personnes concernées**

Exemples de lignes directrices additionnelles à 27002

- Précisions sur les bonnes pratiques 27002
  - **Contrôle d'accès, gestion des incidents, etc.**

- Bonnes pratiques additionnelles à 27002
  - Principes fondamentaux :
    Base légale, consentement, PIA, contrats
  - Droits des personnes :
    Information, consentement, opposition, rectification, accès, etc.
  - Privacy by design and by default :
    Pertinence, minimisation, durée de conservation, etc.
  - Partage, transfert, mise à disposition :
    Base légale, traçabilité, responsabilité conjointe, etc.

Articulation de l'ISO 27701 avec le RGPD

- **Correspondance indicative avec les Articles 5 à 49 du RGPD**.
  - à l'exclusion de l'article 43 sur les Organismes de certification

  ⚠ ce n'est pas une « certification RGPD »

- La conformité aux exigences et aux mesures de l'ISO 27701 est une **très bonne base** pour satisfaire aux obligations du RGPD.

  ⚠ Mais il incombe aux organisations d'évaluer leurs obligations légales et de décider comment s'y conformer.

CNIL.

Les actions prioritaires

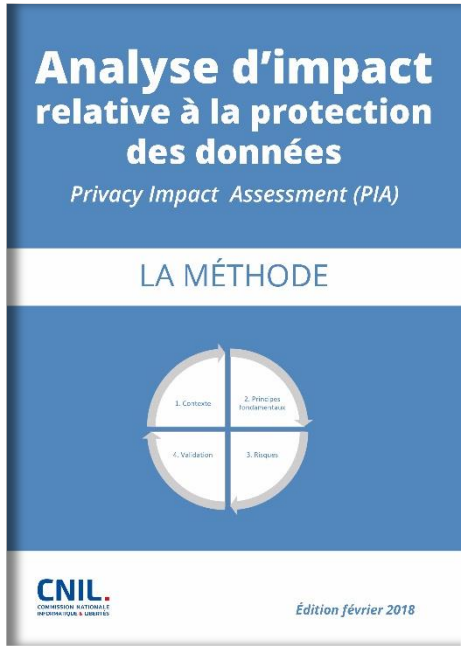
LES ÉTAPES DE MISE EN PLACE D'UNE GOUVERNANCE ET D'UNE DÉMARCHE QUALITÉ AUTOUR DES DONNÉES

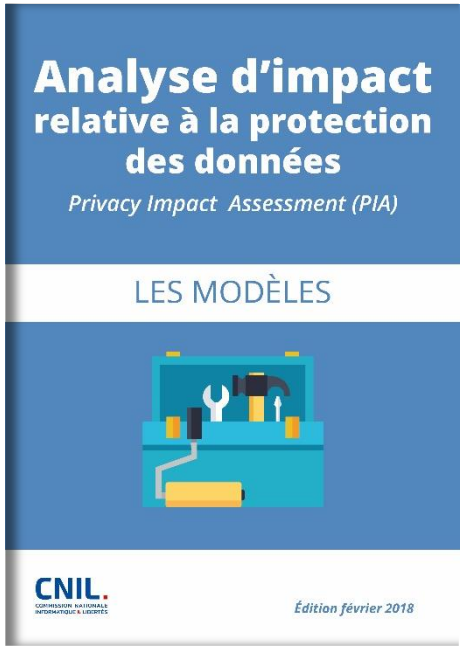
1. Evaluer ce qui est en place et le reste à faire

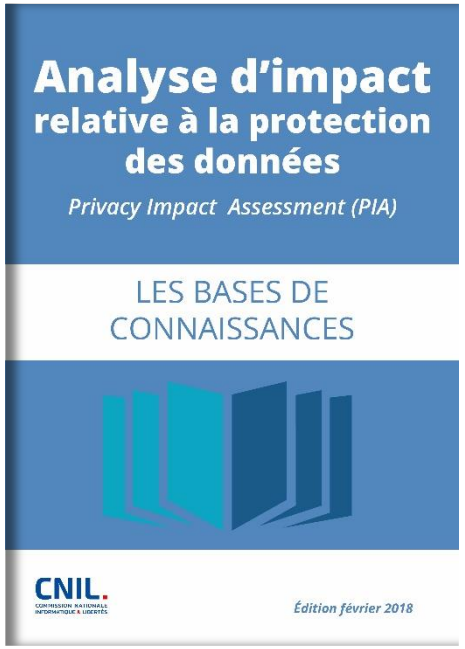
- Comme pour tout système de management « qualité », on commence par :
  - Cerner le **périmètre** des traitements de données personnelles
  - Evaluer les **attentes** des parties prenantes (patients, professionnels, autorités de contrôle)
  - Evaluer la **conformité juridique** des traitements
  - Evaluer les **risques de sécurité** sur les données
  - Etablir un **plan d'action** juridique et technique
- On peut s'appuyer sur le registre du DPO, les AIPD et les démarches entreprises pour l'entrée en vigueur du RGPD

Les outils : la méthode PIA de la CNIL

- Le *Privacy Impact Assessment* :
  - pour intégrer la protection de la vie privée et la cybersécurité
  - pour faire du Privacy by design…

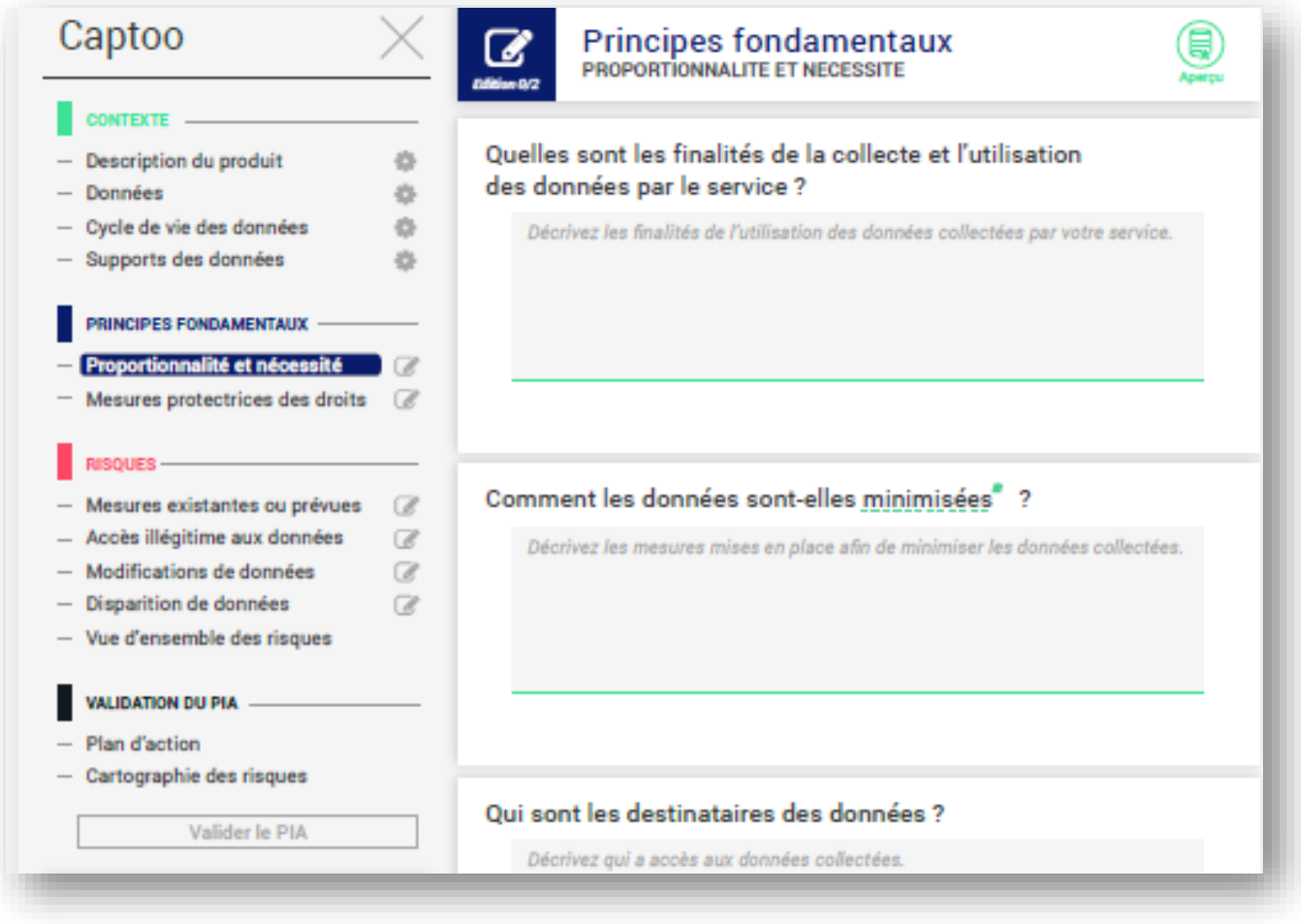






Les outils : le logiciel PIA de la CNIL

- Aider les entreprises
- Solution simple, *user-friendly*
- Logiciel libre et open source, en 18 langues
- Bases de connaissances pour les principes de protection de la vie privée
- Cartographie des risques et de leurs composantes
- Réutilisation des PIAs



2. Identifier les forces vives disponibles

- Le système de management de protection des données repose sur des acteurs clés :
  - La **direction** de l'établissement
    - Définit la politique générale et alloue les moyens nécessaires
  - Le **chef de projet** RGPD
    - Est chargé de la cartographie des traitements et de l'évaluation de leur conformité juridique et technique
  - Le **RSSI** et le **DPO**
    - Assurent au quotidien le maintien de la conformité, par la gestion des écarts juridiques et techniques, et par la coordination des plans d'action

3. Définir des procédures et réaliser des retours d'expériences sur lesquels capitaliser

- Il faut installer les **processus** qui « feront tourner » le **système de management de la protection de la vie privée** :
  - Mise en œuvre et suivi du **plan d'action** juridique et technique
  - Traitement des **incidents** et des **violations** de données
  - Traitement des **demandes** et des **plaintes**
  - **Réévaluation régulière** de la conformités et des risques, en fonction de l'évolution du **contexte** et des **traitements**
  - Consolidation des **retours d'expérience**
  - **Revues de direction** et allocation des **moyens** humains et budgétaires

4. Sensibiliser et former pour instaurer une véritable culture/hygiène en « protection des données »

- Pour que les processus fonctionnent, il faut **impliquer** et **former** l'ensemble des **personnels**
  - Rappel des **règles de sécurité** informatique (PSSI, charte)
  - Rappel des **grands principes de protection des données**
    - Politique spécifique, ou fusionnée avec la PSSI
  - **Fiches réflexes** pour la conduite à tenir en cas d'incident et de violation de données, de demande et de plainte
  - **Retours d'expérience** sur les violations et les plaintes :
    - Pour l'établissement et le secteur hospitalier en général
    - Sanctions des autorités de protection en France et en UE

Gouvernance : les clés du succès

Un fort soutien du top management

- **Un reporting facilité et efficace au niveau le plus élevé**
- **Un appui de la direction envers les acteurs désignés**
  - DPO, RSSI, chef de projet RGPD, responsables métiers
- Prévoir des rendez-vous réguliers avec les acteurs
- Instaurer la pratique d'un bilan annuel

Une gouvernance à formaliser

- **Un réseau de relais formés et investis** (fiche de poste, moyens)
- Des procédures à mettre en place et à auditer

Octroyer des ressources

- **Des ressources humaines** (personnel dédié, temps, etc.)
- Des ressources matérielles (budget, etc.)
- La formation et la sensibilisation
- Un accès aux ressources, services et documentation adéquats

Questions-réponses