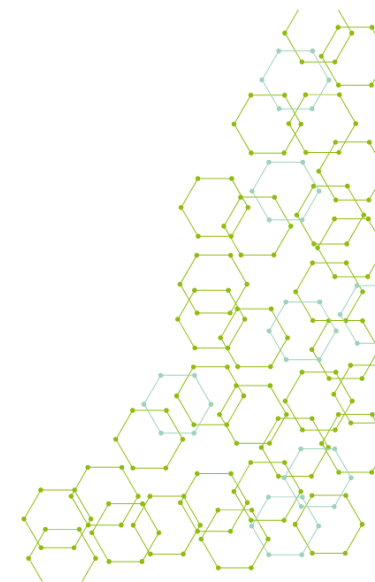


3^{ème} Rencontre Régionale de l'URPS Pharmaciens Centre-Val de Loire

Alors... Deux boîtes de Rindox et un peu
d'empathie... Pour l'empathie, voyez
avec ma collègue.



PROGRAMME

CONFÉRENCES | 18h30 – 20h30

Françoise GUEGAN – Présidente de l'URPS Pharmaciens

Mot d'accueil

Elisa BENAZECH / Cyril LEROSIGNOL – GRADeS

Intervention sur le Ségur

Ugo SCHURIG – GRADeS

Vivre dans un monde de cybermenaces

Patrice LAIGLE – GRADeS

Définition et périmètre de l'intelligence artificielle. Présentation d'un cas d'usage, évaluation et retour d'expérience

Françoise TRAN – Ethik-IA

À partir de cas d'usage concrets repartez avec l'essentiel pour comprendre l'IA

TABLE RONDE | 20h30 – 20h45

Animée par Françoise Guegan & Vanessa Auroux

- Elisa BENAZECH,
- Patrice LAIGLE,
- Cyril LEROSIGNOL,
- Ugo SCHURIG,
- Françoise TRAN

COCKTAIL DINATOIRE | 20h45



Rencontre Régionale URPS Pharmaciens

Volet Ségur du Numérique en Santé

Équipe Socle National

09/04/26



Fonctions structurantes



Un objectif majeur : généraliser le partage fluide et sécurisé de données de santé entre professionnels et avec l'utilisateur pour mieux prévenir et mieux soigner.

RÉFÉRENTIELS



Référencement des données avec une identité nationale de santé



Identification électronique centralisée pour les professionnels de santé

Application carte vitale

Identification et authentification numérique des usagers

SERVICES



Stockage des données de santé dans le Dossier Médical Partagé



Echanges via les messageries sécurisées de santé

Mon espace santé

MSS et échanges de documents avec les patients

SONS vague 2

● Prépublication du financement SONS vague 2 Officines prévue au 1^{er} semestre 2026

Service Socle	Fonctionnalités	Usage pour le professionnel
MSSanté	Intégration des boîtes aux lettres MSSanté dans les logiciels de gestion d'officines	Envoi de MSSanté directement depuis le dossier patient du logiciel de gestion d'officines (LGO)
DMP/MES	Consultation du DMP depuis le dossier patient du LGO	Avoir accès aux informations contenues dans le DMP directement depuis le LGO
INS	Aide à la qualification des INS dans le LGO	Qualifier les identités complexes afin d'alimenter Mon Espace Santé depuis le LGO
Pro Santé Connect/ Moyens d'identifications électroniques	Intégration systématique de Pro Santé Connect pour l'authentification des professionnels sur les LGO	Sécuriser l'accès aux données de santé pour le professionnel et garantir la sécurité des données sensibles des patients

MIE et RPPS+ définitions

● **Moyen d'identification électronique (MIE)**

- Dispositif matériel et/ou immatériel contenant un **identifiant personnel** et utilisé pour **s'authentifier sur un service numérique en santé**. Il permet de **garantir l'identité d'une personne**, basée sur un enregistrement initial.

● Il existe différents types de Moyens d'identification électronique :

- Cartes CPS
- Clés FIDO
- Les cartes à puces
- Badges
- Etc...

- Chaque type de Moyen d'identification électronique doit être conforme au référentiel d'identité électronique (cadre réglementaire). Il doit être obligatoirement compatible via Pro Santé Connect.

RPPS +

- **RPPS** : Répertoire Partagé des Professionnels de Santé :
 - Les chirurgiens-dentistes
 - Les infirmiers
 - Les masseurs-kinésithérapeutes
 - Les médecins
 - **Les pharmaciens**
 - Les pédicures-podologues
 - Les sage-femmes

- **RPPS +** : pour **sécuriser** les accès aux services numériques, **le portail RPPS +** permet aux professions sans ordre **de disposer d'un numéro RPPS** au même titre que les professions à ordre.

Différences entre RPPS et RPPS+

RPPS

Registre Partagé des Professionnels de Santé

CONCERNE :

Professionnels à Ordre
Professionnels ADELI/ARS

Enregistrement **OBLIGATOIRE**

Identifiant **unique et permanent** à 11 chiffres

Permet l'obtention d'une **carte CPS physique** pour connexion via Pro Santé Connect.

RPPS+

Portail d'enregistrement des professionnels à rôle

CONCERNE :

En officine, les préparateurs en pharmacie et en milieu hospitalier les préparateurs en pharmacie hospitalière.

Enregistrement **POUR ÊTRE CONFORME AU Référentiel d'identité électronique**

Identifiant **unique et permanent** à 11 chiffres, enregistré au RPPS

Permet d'obtenir une identité numérique sécurisée donnant accès à une adresse MSS nominative, aux services numériques et par défaut à une **e-CPS** accessible via un terminal mobile (appli e-CPS) pour connexion via Pro Santé Connect.

Calendrier réglementaire

RIE V2

1^{er} semestre 2026
Version disponible
sur le site de l'ANS
en attente de
validation

Cartes CPE

31 décembre 2026
Arrêt de l'utilisation
des cartes CPE via Pro
Santé Connect

RIE

31 décembre 2028
Obligation d'utiliser
un MIE via Pro Santé
Connect pour accès
LGO

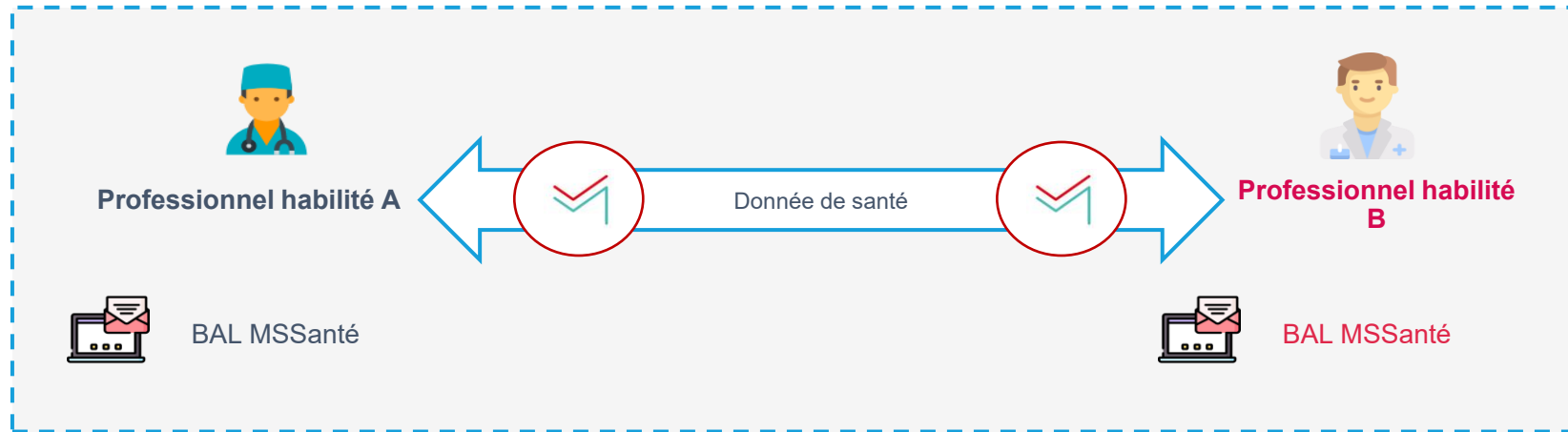
Avril 2026
Ouverture
inscription aux PP
et PPH au RPPS+

**Enregistrement des professionnels à rôle
dans le portail RPPS +**

RPPS +

● Pour vous accompagner, le GRADeS organise des webinaires d'information RPPS+ régulièrement

MSSanté : principes généraux



- MSSanté : dispositif de messagerie sécurisée permettant d'échanger entre professionnels et avec l'utilisateur des informations sensibles/ de santé au sein d'un espace de confiance fermé
- Mon espace santé introduit une fonctionnalité de messagerie sécurisée de santé pour tous les citoyens qui disposent d'un accès au service MES
 - Outil : webmail intégré au site MES ou à l'application mobile
 - Boîte nominative : ins@patient.mssante.fr
 - Possibilité d'envoi et réception de pièces jointes issues ou à destination des documents de MES

MSSanté régionale Wraptor



- **Offre régionale MSSanté:** proposer aux professionnels de santé et aux établissements de la région de s'équiper en MSSanté pour améliorer la prise en charge sécurisée des données de santé et personnelles.
- Offre Officines : création de BALs MSSanté Organisationnelles afin de recevoir les ordonnances des patients (via Mon Espace Santé) en lien avec l'Assurance Maladie.
- En mars 2026, 62% des officines de la région sont équipés en MSSanté Organisationnelle

Opérateur Wraptor

Deux noms de domaine :

- cvl.mssante.fr
- esante-centre.mssante.fr

Possibilité de création de BAL :

- Nominatives
- Organisationnelle
- Cabinet
- Applicatives

Gestion des BALS :

- Équipe socle national
- Équipe technique

Accompagnement de l'équipe Ségur

● MSSanté:

En partenariat avec les DNS de l'Assurance Maladie :

- Gestion et support MSSanté régionale
- Accompagnement à l'interfaçage des BàL MSSanté en lien avec les éditeurs LGO
- Organisation de webinaires régionaux

● MIE / RPPS + :

- Veille réglementaire et technologique en lien avec l'ANS et la DNS
- Accompagnement des professionnels dans l'appropriation des moyens d'identification électronique et leurs habilitations
- Accompagnement et formation à l'utilisation du portail RPPS+

● Financement SONS Vague 2 Ségur

- Veille réglementaire en lien avec l'ANS et la DNS
- Organisation de webinaires régionaux à destination des Officinaux
- Accompagnement à la relecture des bons de commandes SONS
- Accompagnement et relais avec les éditeurs de solution LGO

Pour nous contacter : segur@esante-centre.fr



VIVRE DANS UN MONDE DE CYBERMENACES

Jeudi 9 avril 2026

Rencontre régionale URPS Pharmaciens

Êtes-vous une autruche ?



- Remettre à plus tard la stratégie cyber
- Déléguer sans vérifier (confiance aveugle)
- Penser que « ça n'arrive qu'aux autres »

En vérité, le risque n'est pas QUE technique :

- Manque de structure et d'organisation
- PCA/PRA ??

- Qui décide quoi ?
- Quoi faire dans les 4 premières heures ?
- Quels sont vos systèmes critiques ?

Si votre SI tombe demain matin à 8h, que feriez-vous dans l'heure qui suit ?



La cybersécurité, c'est quoi ?



L'ensemble des moyens déployés pour protéger les systèmes d'information (SI) : PSSI, PC, serveurs, mobiles, réseaux, données systèmes électroniques,... contre les intrusions et attaques malveillantes .

- **PRÉVENIR :**
 - Sensibilisation, sauvegardes...
- **CONTRÔLER :**
 - Audits, scan des systèmes, surface d'exposition, vulnérabilités...
- **DÉTECTER :**
 - Pare-feu, antivirus, SIEM, EDR/XDR...
- **RÉAGIR ET REMEDIER :**
 - Gestion de crise, assistance incidents, reconstruction des systèmes

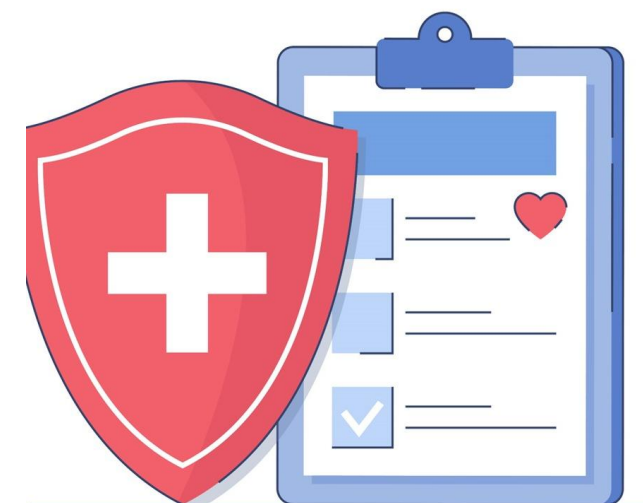


La cybersécurité, c'est quoi ?



- **Qu'avez-vous à protéger au sein de votre SI ?**
 - Les données de vos patients (sensibles et onéreuses)
 - Les données des collaborateurs (identifiants et accès)
 - Informations confidentielles (santé)
 - Les logiciels métiers (LGO, CRM...)
 - Vos sauvegardes (3 2 1 -> 3 2 1 1 0)

- **Une sensibilisation primordiale**
 - L'humain est le premier rempart à toute forme d'attaque cyber. C'est le maillon fort !



*(90% des cyberattaques sont liées à une erreur humaine. Source IBM Institute 2024)
Selon l'ANSSI, plus de 80 % des cyberattaques débutent par un email frauduleux.*

Un monde de cybermenaces



- **Les types de cybercriminels :**

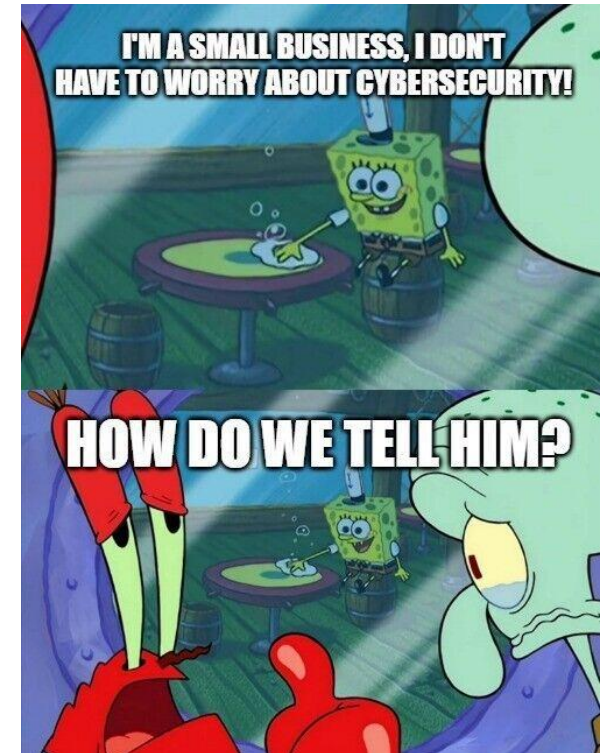
- Etats nations
- Cybercriminels
- Hacktivistes
- Groupes terroristes
- Script Kiddies
- Menace interne

- **Leurs objectifs :**

- Gains financiers
- Vol de données
- Nuisance / Vengeance
- Espionnage

- **Les principales cyberattaques :**

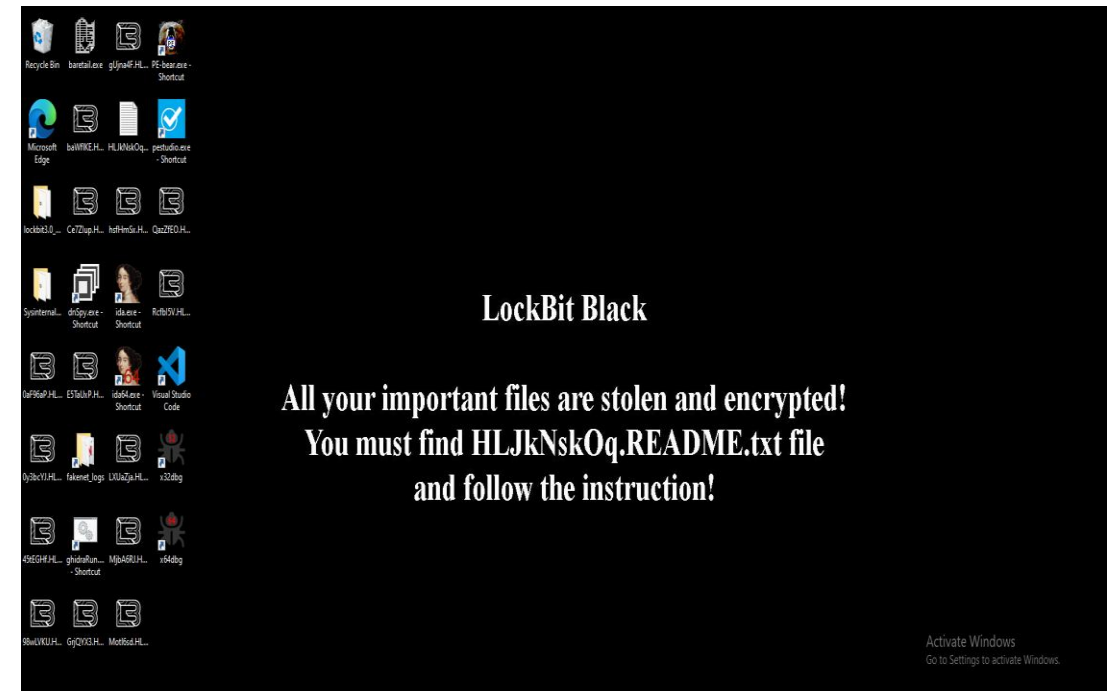
- Malwares (Ransomware)
- Phishing – Smishing – Quishing (SE)
- Vol de données
- DDOS



Un monde de cybermenaces



- **Les signes probables d'une cyberattaque**
 - Des applications qui ne fonctionnent plus (enfin plus comme d'habitude)
 - Des ralentissements réseau extrêmes
 - Des imprimantes qui crachent des notes de rançons
 - Un nouveau fond d'écran super stylé, mais quelque peu anxiogène.
 - Altérations/suppressions de fichiers (file.txt.hacked)
- **Les conséquences d'une cyberattaque**
 - Perte financière
 - Interruption totale ou partielle d'activité
 - Indisponibilité du SI
 - Vol de données
 - Réputationnel
 - Juridique



La menace cyber en santé



- **l'IA au service du crime**
 - Spear Phishing - Deep Fakes
 - Usurpation d'identité et chantage
 - Sophistication accrue
- **Pourquoi la santé ?**
 - Valorisation d'un dossier médical.
 - Données sensibles
- **Des précédents qui nous obligent à réagir**
 - ARS, GRADeS, CH, EHPAD...
 - CEGEDIM
 - 37 alertes en région CVL sur 2025 dans le domaine de la santé

- Un dossier médical vaut 250\$ dollars sur le dark web.
- 1 français sur 4 s'est fait pirater ses données médicales rien qu'en 2025.
- 15,8 millions de dossiers volés
- 1500 cabinets médicaux piratés

Phishing ou pas phishing ?



ESPACE CLIENT ▾

PORTAL TV ET ▾

SERVICES PLUS POUR VOUS ▾

Facture impayée (N°72937438)

Chère Cliente, Cher Client,

Nous sommes au regret de vous informer que le prélèvement mensuel dû au règlement de votre facture a été refusé par votre établissement.

Dans l'attente d'une suite favorable, nous vous invitons à régler les frais de votre abonnement dans les plus brefs délais dans un de nos magasins ou sur votre espace client en cliquant sur le lien ci-dessous

<http://www.bouyguetelecom.fr/mon-compte/suivi-conso/factures>

Vous disposez de 48h pour régler votre facture, dans le cas où votre facture n'est toujours pas réglée, votre abonnement sera automatiquement résilié.

Nous vous remercions de votre confiance.

S'IDENTIFIER



ESPACE CLIENT ▾

PORTAL TV

SERVICES PLUS POUR VOUS ▾

Facture impayée (N°72937438)

Chère Cliente, Cher Client,

Nous sommes au regret de vous informer que le prélèvement mensuel dû au règlement de votre facture a été refusé par votre établissement.

Dans l'attente d'une suite favorable, nous vous invitons à régler les frais de votre abonnement dans les plus brefs délais dans un de nos magasins ou sur votre espace client en cliquant sur le lien ci-dessous

<http://www.bouyguetelecom.fr/mon-compte/suivi-conso/factures>

Vous disposez de 48h pour régler votre facture, dans le cas où votre facture n'est toujours pas réglée, votre abonnement sera automatiquement résilié.

Nous vous remercions de votre confiance.

S'IDENTIFIER

Phishing ou pas phishing ?



Alerte de sécurité Boîte de réception x



Google <no-reply@accounts.google.com>

À moi ▾

De: **Google** <no-reply@accounts.google.com>
à:
Date: 30 oct. 2025 09:41
Objet: Alerte de sécurité
Envoyé par: gaia.bounces.google.com
signé par: accounts.google.com
sécurité: Chiffrement standard (TLS) [En savoir plus](#)



Nouvelle connexion au compte



Nous avons détecté une nouvelle connexion à votre compte Google. Si c'était vous, aucune action de votre part n'est requise. Dans le cas contraire, nous vous aiderons à sécuriser votre compte.

[Consulter l'activité](#)

Vous pouvez aussi voir l'activité liée à la sécurité de votre compte ici :
<https://myaccount.google.com/notifications>

Cet e-mail vous a été envoyé pour vous informer de modifications importantes apportées à votre compte et aux services Google que vous utilisez.

© 2025 Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland

Phishing ou pas phishing ?



Réagir en cas de cyberattaque



1^{ère} étape : arrêter l'hémorragie

- Isolement de la machine infectée (quarantaine) en débranchant les câbles réseau et le Wi-Fi.
- **N'éteignez surtout pas les ordinateurs** (empreintes numériques)

2^{ème} étape : alerter le 17 cyber : <https://17cyber.gouv.fr/>

- Réponse technique avec des mesures réflexes selon l'incident.
- Disponible 24h/24 et 7j/7

3^{ème} étape : Faites appel à des spécialistes :

- En cas de virement suspect : appeler votre banque, exiger un rappel de fonds.
- Appeler votre prestataire informatique pour la remédiation. Ne surtout rien effacer (copier les preuves avant de tout réinstaller), trouver l'origine de l'intrusion.

On respire,
paniquer ne sert à rien !



Réagir en cas de cyberattaque



4^{ème} étape : dépôt de plainte

- Avec les forces de l'ordre (Police ou Gendarmerie), il y a des cellules cyber dans chaque département.

5^{ème} étape : Si fuite de données

- Alerter la CNIL sous 72h.
- Informer également vos clients/fournisseurs si vol d'informations personnelles.

**NE JAMAIS PAYER
LA RANÇON !**



“

LA QUESTION N'EST PLUS

« est-ce que cela peut vous arriver ? »

MAIS PLUTÔT

« **êtes-vous prêts si cela arrive ?** »

”

Se préparer à la menace cyber

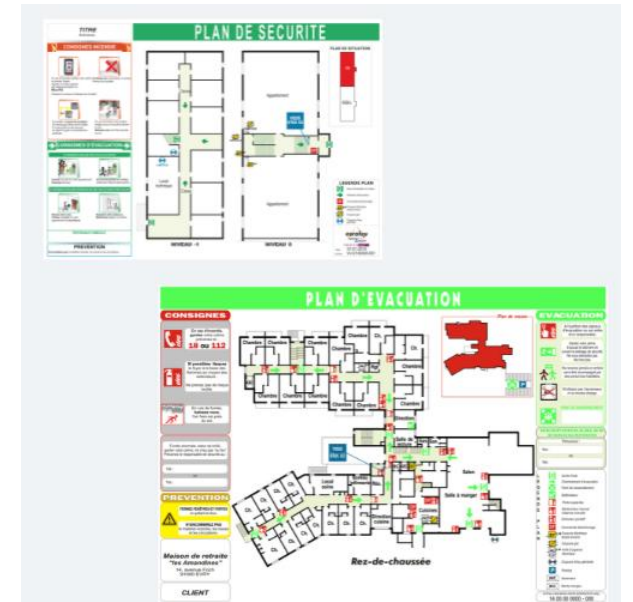
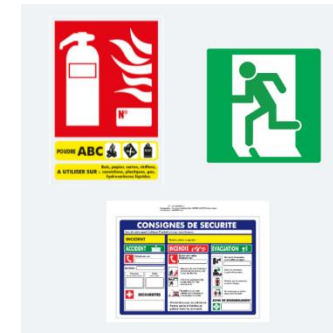
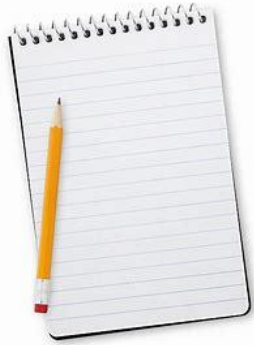


- 3 principes de base en cybersécurité
 - Moindre privilège
 - Droit d'en connaître
 - Défense en profondeur

- Diagnostic cybersécurité



Se préparer à la menace cyber



Se préparer à la menace cyber




- Fini les post-it ! On utilise un gestionnaire de mot de passe (keepass...). Mot de passe = mouchoir
- On verrouille sa session en cas d'absence
- Anonymiser les données si utilisation de l'IA
- Bannir les adresses Google/Yahoo/Hotmail... si envoi de documents confidentiels. MSS...quoi?
- Activer le MFA, le vrai, le TOTP clé physique ou MS Authenticator
- Mettre à jour les équipements
- Avoir des sauvegardes, testées, et qui peuvent être déconnectées (règle du 3 2 1 1 0)
- Méfiez-vous des messages inattendus et des comportements suspects ! On signale.
- Vigilance avec les supports amovibles (rubber ducky)



MIEUX VIVRE DANS UN MONDE DE CYBERMENACES

Ugo SCHURIG
Chargé de mission Cybersécurité



Intelligence artificielle : Comprendre, évaluer et intégrer les usages en santé



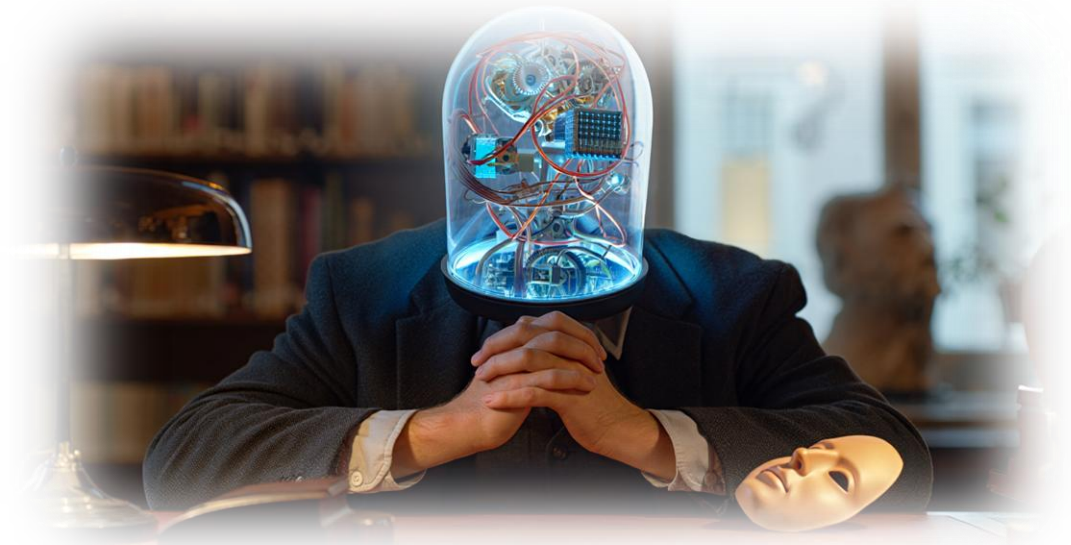
Patrice LAIGLE
Réfèrent technique, Pôle Expertises & Innovation

Définir pour comprendre

Daniel Andler résume parfaitement l'enjeu :

« L'IA ne pense pas : elle calcule. Elle produit des résultats pertinents, parfois spectaculaires, mais sans compréhension profonde du monde ni intention propre. » (*Intelligence artificielle, intelligence humaine : la double énigme*, 2023).

- L'IA = **ensemble de techniques qui permettent à des machines d'imiter certaines fonctions cognitives humaines**
- L'IA **perçoit, reconnaît, prédit, décide**
- Mais elle **ne possède pas une intelligence humaine !**
- « L'intelligence artificielle n'a rien d'intelligent. » (Yann LeCun)



Ce qui change aujourd'hui : **échelle des données, puissance de calcul, intégration au poste de travail**

Quelques repères historiques

1930 - 1950

Travaux fondateurs d'Alan Turing
Base théorique de l'informatique moderne



1980s

Systèmes Experts
IA Symbolique



2020+

Démocratisation IA générative
Création de contenus, images, recommandations

2017

Modèles génératifs
Transformers

Dartmouth Workshop
Naissance officielle du terme *Artificial Intelligence*

1956 Dartmouth Conference:
The Founding Fathers of AI



1956

Explosion du *deep learning*
Vision, OCR
Arrivée de l'IA dans la vie courante (assistants vocaux, GPS, Netflix...)

2010s

IA Act
Adoption du règlement européen sur l'Intelligence Artificielle

2023

Les 4 grandes familles d'IA

1

IA symbolique

Règles logiques « si... alors »

Exemple : alertes posologiques dans un LGO – règle métier : « Si patient > 65 ans et benzodiazépine → alerte »

✓ Analogie : énorme tableau de règles

2

IA statistique / Machine Learning

Apprentissage de régularités dans les données

Exemple : prédiction de rupture de stock à partir de l'historique

✓ Analogie : repérer des habitudes dans un tableau

3

Apprentissage profond / Deep Learning

Réseaux neuronaux avec de nombreuses couches

Exemple : OCR avancé pour lire les ordonnances floues, reconnaître un tampon

✓ Analogie : filtres empilés qui extraient automatiquement les bons indices

4

IA générative / Transformers

Modèles capables de produire du texte, images, etc.

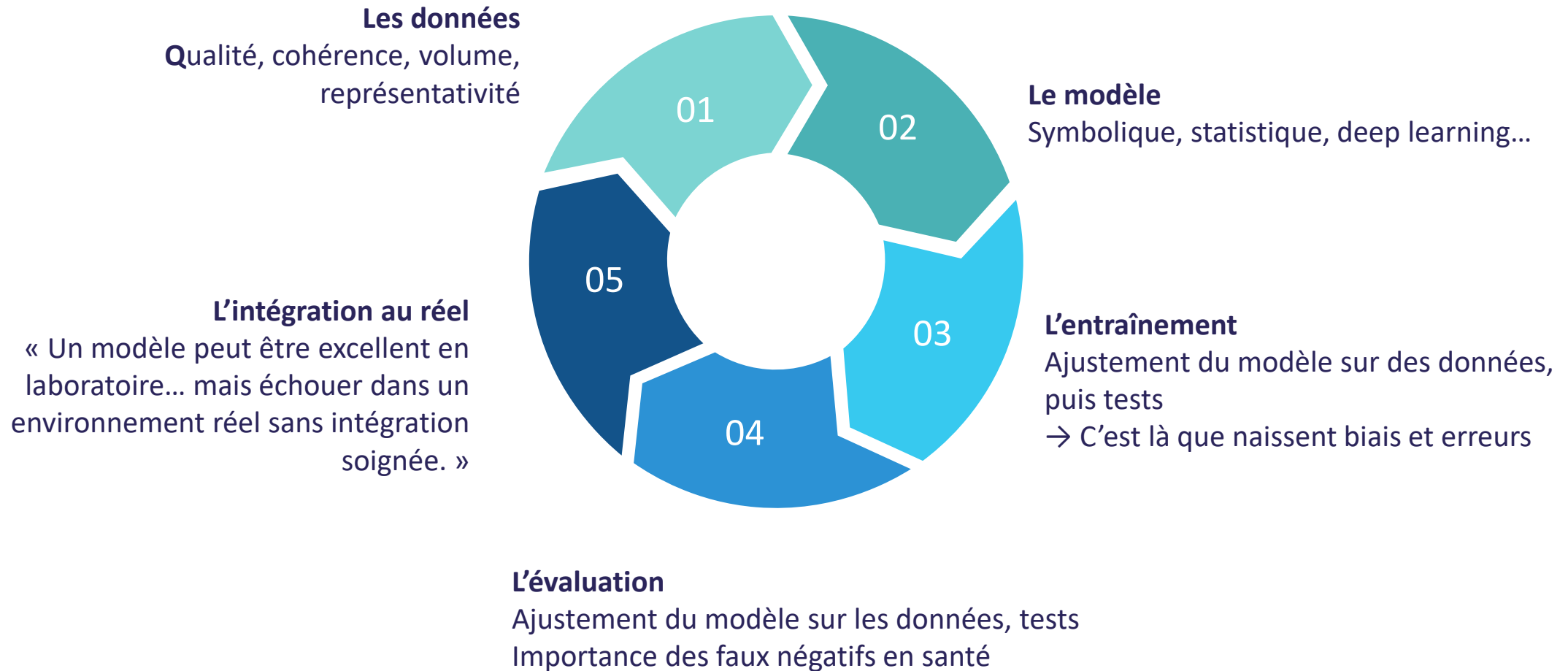
Exemple utile : résumer une notice médicament, répondre à une question clinique simple

Exemple dangereux : fausses ordonnances réalistes générées par IA

✓ Analogie : super-autocompléteur statistique très puissant

Les composantes d'un système IA

Un projet d'IA repose toujours sur les mêmes briques :



Comment un projet d'Intelligence Artificielle est-il étudié ?

1. Besoins réels & valeur métier

Quel problème concret est résolu ? Quelle charge retirée ?

2. Données disponibles

Annotées ? Exploitable juridiquement ? Représentatives ?

3. Performance utile

Pas seulement technique : quel est l'impact des erreurs ?

4. Intégration SI

Compatibilité avec votre logiciel, ergonomie

5. Gouvernance & conformité

Traçabilité, RGPD, sécurité, responsabilité

6. Soutenabilité & coûts

Maintenance, mises à jour, monitoring, formation

7. Résilience face aux fraudes

Exemple en pharmacie : fausses ordonnances générées par IA

Pourquoi les IA « buguent » ? Les vraies limites

Cas d'usage en officine :

1) Variabilité des documents

« Photos floues, manuscrits, tampons partiels... l'OCR s'effondre. »

2) Fraudes assistées par IA

« Fausses ordonnances quasi indiscernables... faux QR code bien formé. »

3) Systèmes non intégrés

« La solution d'intelligence artificielle n'est pas intégrée au LGO : ressaisies, PDF... lourdeur. »

4) Absence de compréhension

« L'IA imite, mais ne comprend pas. »

Un principe fondamental

- L'IA aide à la décision, mais ne remplace jamais le jugement humain
- En santé, cela constitue une exigence de sécurité

Une IA fiable, éthique & au service de l'humain

Enjeux clés

- **Biais des données** : une IA entraînée sur un système (ex : américain) peut orienter différemment les décisions qu'en contexte français
- **Impact sur les décisions** : l'IA s'intègre dans nos choix → dilemmes éthiques
- **Autres enjeux majeurs** : environnementaux, souveraineté numérique, économiques, sociétaux (déshumanisation, peur du remplacement)

Spécificités santé

- Nécessité de **données représentatives de la population**
- Alignement avec la **politique de santé publique**
- Préservation de l'indépendance face aux influences extérieures

Gouvernance & responsabilité

- Importance de la **vigilance**, de la **gouvernance** et de l'**intégration maîtrisée**
- Vers une **IA vigilance** et une **garantie humaine systématique**

Rôle du GRADeS

Garantir des projets IA :
Utiles,
Sûrs,
Intégrés,
Pérennes

Animation Régionale – Innovation & IA en Santé

SAVE THE DATE

Webinaire régional IA & Innovation - 5 mai 2026 (13H-14H)

Lien de connexion Teams : [ici](#)

Présentation des résultats de l'enquête

Ambitions régionales, premières actions d'accompagnement

Afin de contribuer à notre enquête sur l'état des lieux et les besoins en outils innovants, notamment en intelligence artificielle, nous vous invitons à prendre quelques instants pour répondre à notre questionnaire :



Lien du questionnaire :

<https://forms.cloud.microsoft/Pages/ResponsePage.aspx?id=Myyy2X9JgkihUAywleii-615gr2wdJIrtGR1lhYOkpUQ0piWURYSV4k4REFVRIIKNEMyT0tQV0tYSi4u>

Animation Régionale – Innovation & IA en Santé

SAVE THE DATE

Journée Innovation du GRADeS Centre-Val de Loire – 30 septembre 2026

Lieu à définir

Remise des prix du Concours IA & Santé :

Transformez des dossiers médicaux papier en synthèses intelligentes grâce à l'IA

Concours ouvert aux étudiants & aux start-ups

Grands Prix : 5000€ (par catégorie)



Lien vers le formulaire d'inscription :

<https://forms.cloud.microsoft/Pages/ResponsePage.aspx?id=Myyy2X9JgkihFUywlEii-615gr2wdJIrtGR1lhYOkpUMDhHREdGUExQTzhYNENLW EY4OVpSS1Y2Si4u>



Merci de votre attention

Ethik - IA
Garantie Humaine de l'

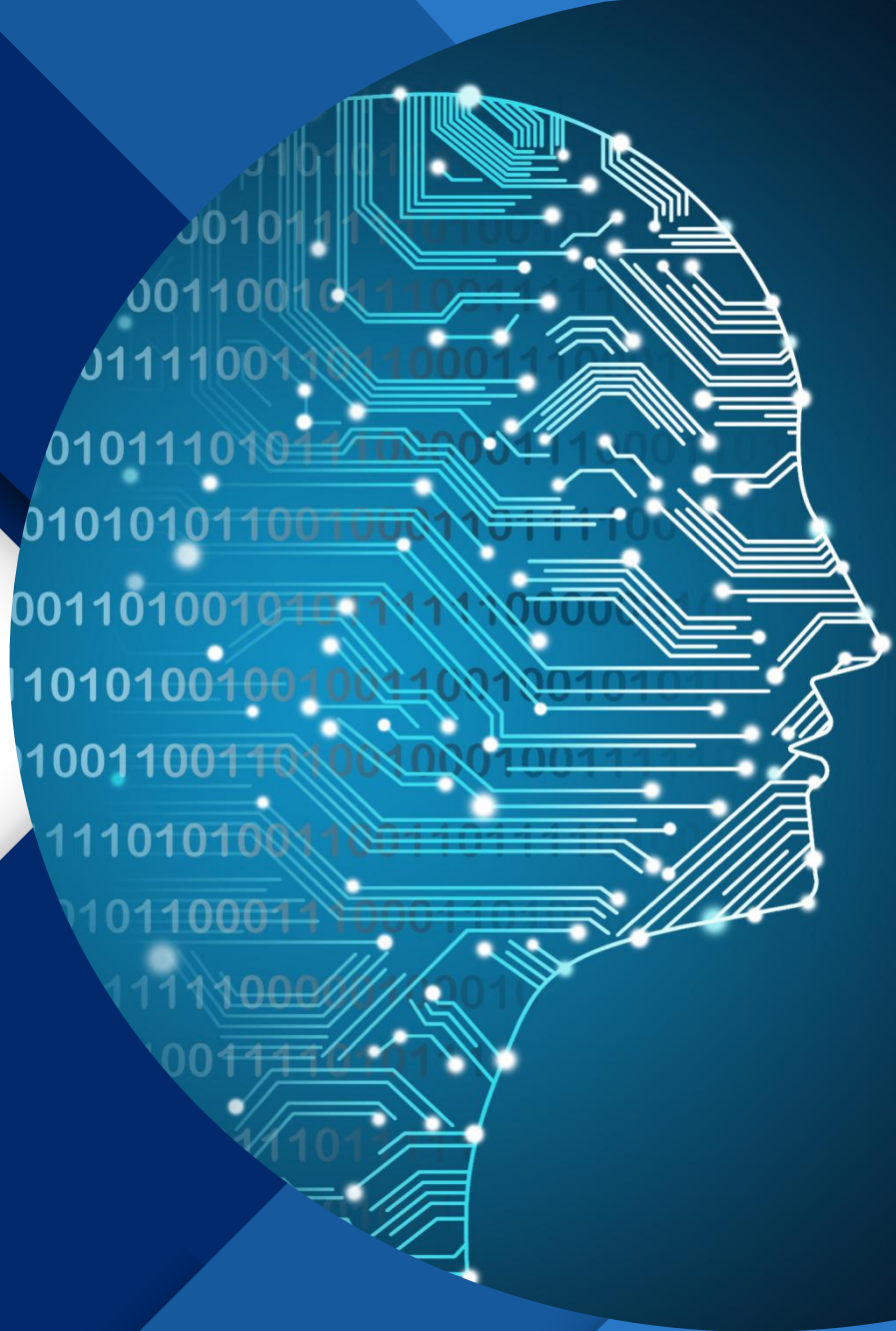
RENCONTRE RÉGIONALE
URPS PHARMACIENS CENTRE VAL DE LOIRE

**IA EN PHARMACIE : INNOVATION, ÉTHIQUE
ET CADRE REGLEMENTAIRE**

— — — — —
9 Avril 2026 - Blois



URPS Pharmaciens
Centre-Val de Loire



1

Ethik - IA
Garantie Humaine de l'

Cas d'usage de l'intelligence artificielle en pharmacie d'officine

Au comptoir : 4 situations concrètes où l'IA peut faire gagner du temps et sécuriser la délivrance



Ordonnance difficile à lire ou longue

Problème : écriture peu lisible, ressaisie chronophage, risque d'erreur.

Réponse IA : lecture assistée et préremplissage des éléments utiles ; signale les zones ambiguës.

Bénéfice : gain de temps, moins de ressaisie, validation facilitée pour le pharmacien.



Risque d'interaction ou d'incohérence

Problème : schémas complexes, automédication, cumul de traitements.

Réponse IA : repère interactions, redondances, doses inhabituelles ; alerte pour vérification.

Bénéfice : sécurisation renforcée avant délivrance ; traçabilité facilitée.



Affluence au comptoir / patient pressé

Problème : files d'attente, tension sur l'équipe, priorisation difficile.

Réponse IA : synthétise les infos clés ; aide à prioriser ; prépare étiquetage et conseils.

Bénéfice : débit amélioré sans sacrifier la qualité d'échange ; charge mentale réduite.



Rupture de stock ou indisponibilité

Problème : produit manquant au moment de la demande du patient.

Réponse IA : signale les ruptures de façon anticipée ; suggère des alternatives conformes.

Bénéfice : réponse plus rapide au patient ; continuité de traitement mieux assurée.

Au comptoir : 4 autres usages utiles pour mieux accompagner le patient



Patient âgé ou polymédiqué

Problème : explications nombreuses, risque d'incompréhension.

Réponse IA : synthèse claire des informations clés et du schéma de prise à reformuler au patient.

Bénéfice : message plus lisible, observance potentiellement améliorée.



Conseil personnalisé

Problème : besoin d'adapter le conseil au profil et au contexte du patient.

Réponse IA : aide à structurer les points de conseil et suggère les questions utiles.

Bénéfice : entretien plus pertinent, plus homogène et mieux tracé.



Orientation dans le parcours

Problème : doute sur la conduite à tenir ou sur le bon niveau d'orientation.

Réponse IA : repérage de signaux d'alerte et appui à l'orientation du patient.

Bénéfice : meilleure vigilance, décision finale laissée au professionnel.



Anticipation des besoins de l'officine

Problème : demandes récurrentes, saisonnalité, tensions difficiles à prévoir.

Réponse IA : repérage de tendances et aide à l'anticipation des commandes.

Bénéfice : stock mieux ajusté et continuité de service améliorée.

2

Ethik - IA
Garantie Humaine de l'

Sensibilisation aux enjeux éthiques, juridiques et environnementaux de l'IA

QUELQUES ENJEUX ÉTHIQUES ET JURIDIQUES DE L'IA

Pourquoi faut-il réglementer ?



OPACITÉ ET EXPLICABILITÉ

Le fonctionnement de nombreuses IA est opaque. Cela crée un risque de décisions impossibles à expliquer aux usagers et une difficulté à détecter des manipulations ou dérives.



INFORMATION

L'utilisation de l'IA peut menacer la bonne information des personnes en diffusant rapidement des contenus faux ou biaisés, parfois difficilement vérifiables, fragilisant ainsi le débat démocratique.



L'IA FORTE

Ou **ia générale** : IA qui présenterait des capacités cognitives supérieures à celles d'un humain sur de multiples domaines. Pas de consensus entre opportunité exceptionnelle et danger non maîtrisé.

QUELQUES ENJEUX ÉTHIQUES ET JURIDIQUES DE L'IA

Pourquoi faut-il réglementer ?



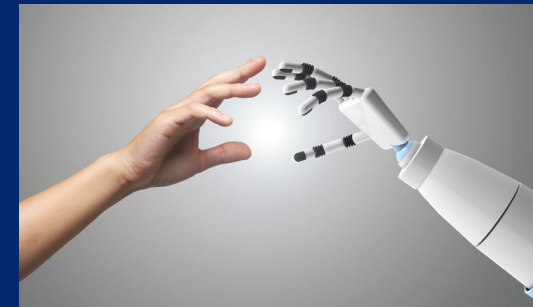
RESPONSABILITÉ

Qui est responsable des décisions de l'IA ?
Le concepteur, le fournisseur de la solution ou l'utilisateur ?



AUTOMATISATION

L'automatisation présente de nombreux risques : perte de contrôle sur la décision, erreur non détectée, etc.



SUPERVISION

L'IA ne doit pas se substituer au jugement professionnel : la garantie humaine reste indispensable. Mais à quel degré ? Trop faible elle est symbolique, trop lourde, elle réduit l'intérêt de l'outil.

QUELQUES ENJEUX ÉTHIQUES ET JURIDIQUES DE L'IA

Des risques augmentés pour les personnes vulnérables



BIAIS

L'IA peut présenter des biais : dans ces données, dans son l'algorithme ou encore dans son usage. Ces biais peuvent mener à des décisions inéquitables notamment pour les publics vulnérables.



MANIPULATION COGNITIVE

L'IA pourrait être utilisé pour manipuler des personnes ou des groupes vulnérables pour induire des comportements non souhaités et influencer les choix.



DÉTRESSE PSYCHOLOGIQUE

L'IA générative peut influencer des personnes vulnérables à commettre des actes portant atteinte à leur santé (allant jusqu'au suicide). La survalidation des IAG ou "sycophancy" peut conforter dans les idées délirantes



RAPPORT DE L'OMS : ÉTHIQUE ET GOUVERNANCE DE L'IA EN SANTÉ, juin 2021

6 principes éthiques

INTELLIGENCE ARTIFICIELLE (IA) & SANTÉ

LES 6 GRANDS PRINCIPES DE L'OMS POUR UNE IA RESPONSABLE

Protéger l'autonomie de l'être humain

Garantir la maîtrise humaine
des systèmes de soins de santé
et des décisions médicales.
Protéger la vie privée et la confidentialité.
Recueillir le consentement éclairé
des patients via des cadres juridiques
appropriés.



Garantir la transparence, la clarté et l'intelligibilité

Avant la conception ou le déploiement
d'une IA, publier des informations
suffisantes et facilement accessibles
pour permettre un débat public
constructif.



Promouvoir le bien-être et la sécurité des personnes ainsi que l'intérêt public

Concevoir l'IA dans le respect
des obligations réglementaires
pour des utilisations bien définies.
Contrôler la qualité et l'amélioration
de la qualité dans l'utilisation de l'IA.



Encourager la responsabilité et l'obligation de rendre des comptes

Utiliser l'IA dans des conditions
appropriées, par des personnes
formées et au service de l'humain.



Garantir l'inclusion et l'équité

Favoriser l'accessibilité,
la non-discrimination et la diversité
des capacités dans le respect des
codes relatifs aux droits humains



Promouvoir une IA réactive et durable

Soutenir des évolutions sociales
positives et s'assurer que l'IA réponde
aux attentes et aux besoins.
Renforcer la responsabilité écologique.
Anticiper et accompagner les
bouleversements en matière d'emploi
et de formation.



OMS : Organisation Mondiale de la Santé.

1. World Health Organization. Ethics and governance of artificial intelligence
for health. Who guidance. 2021

PRINCIPE : PROMOUVOIR UNE IA RÉACTIVE ET DURABLE



Ethik - IA
Garantie Humaine de l'

Durabilité

Le SIA doit également être en cohérence avec l'effort de durabilité des systèmes de santé et être conçu de manière à minimiser son empreinte écologique et accroître leur efficacité énergétique.

- L'IA frugale est l'une des 4 priorités de la seconde phase de la **Stratégie Nationale pour l'Intelligence Artificielle (SNIA)**.
- Le **Conseil Economique, Social, et Environnemental (CESE)** dans un avis rendu en septembre 2024, recommande de concentrer les financements publics en matière de recherche et d'innovation sur les IA à finalité directement environnementale et sur les IA frugales.
- **L'Office Parlementaire d'Evaluation des Choix Scientifiques et Technologiques(OPECST)** érige l'objectif d'une **IA frugale en « impératif »**.
- **L'Ecolab du Commissariat Général au Développement Durable (CGDD)** et **l'Association Française de NORMalisation (AFNOR)** ont publié un référentiel pour évaluer et réduire l'effet d'un service d'IA sur l'environnement.



3

Ethik - IA
Garantie Humaine de l'

Points essentiels du cadre réglementaire de l'AI Act

Objectifs du règlement :

- IA sûres et respectueuses des **droits fondamentaux** et valeurs de l'UE
- Favoriser le **marché économique** : réglementer sans freiner l'innovation
 - Promouvoir une IA de confiance : rassurer les utilisateurs
 - Règles harmonisées → faciliter les échanges et le développement
 - Compétitivité sur le marché mondial : imposer les règles aux SIA qui voudraient s'implanter en UE

Cibles :

- Fournisseurs, déployeurs et autres parties prenantes physiquement présents ou établis au sein de l'UE
- Fournisseurs, déployeurs et autres parties prenantes non établies au sein de l'UE mais dont les résultats générés par les systèmes d'IA sont utilisés dans l'UE



Article 3.1 de l'AI Act :

Un "système d'IA" est un **système automatisé** qui est conçu pour fonctionner à **différents niveaux d'autonomie** et peut faire preuve d'une **capacité d'adaptation après son déploiement**, et qui, pour des objectifs explicites ou implicites, **déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties** telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent **influencer les environnements physiques ou virtuels**.



FOURNISSEUR

Développe ou fait développer un SIA sous son propre nom ou sa propre marque.



MANDATAIRE

A reçu et accepté un mandat d'un fournisseur pour s'acquitter en son nom des obligations et des procédures.



IMPORTATEUR

Met sur le marché un SIA qui porte le nom ou la marque d'un fournisseur établi dans un pays tiers



DISTRIBUTEUR

Fait partie de la chaîne d'approvisionnement, et met un système d'IA à disposition sur le marché de l'Union.

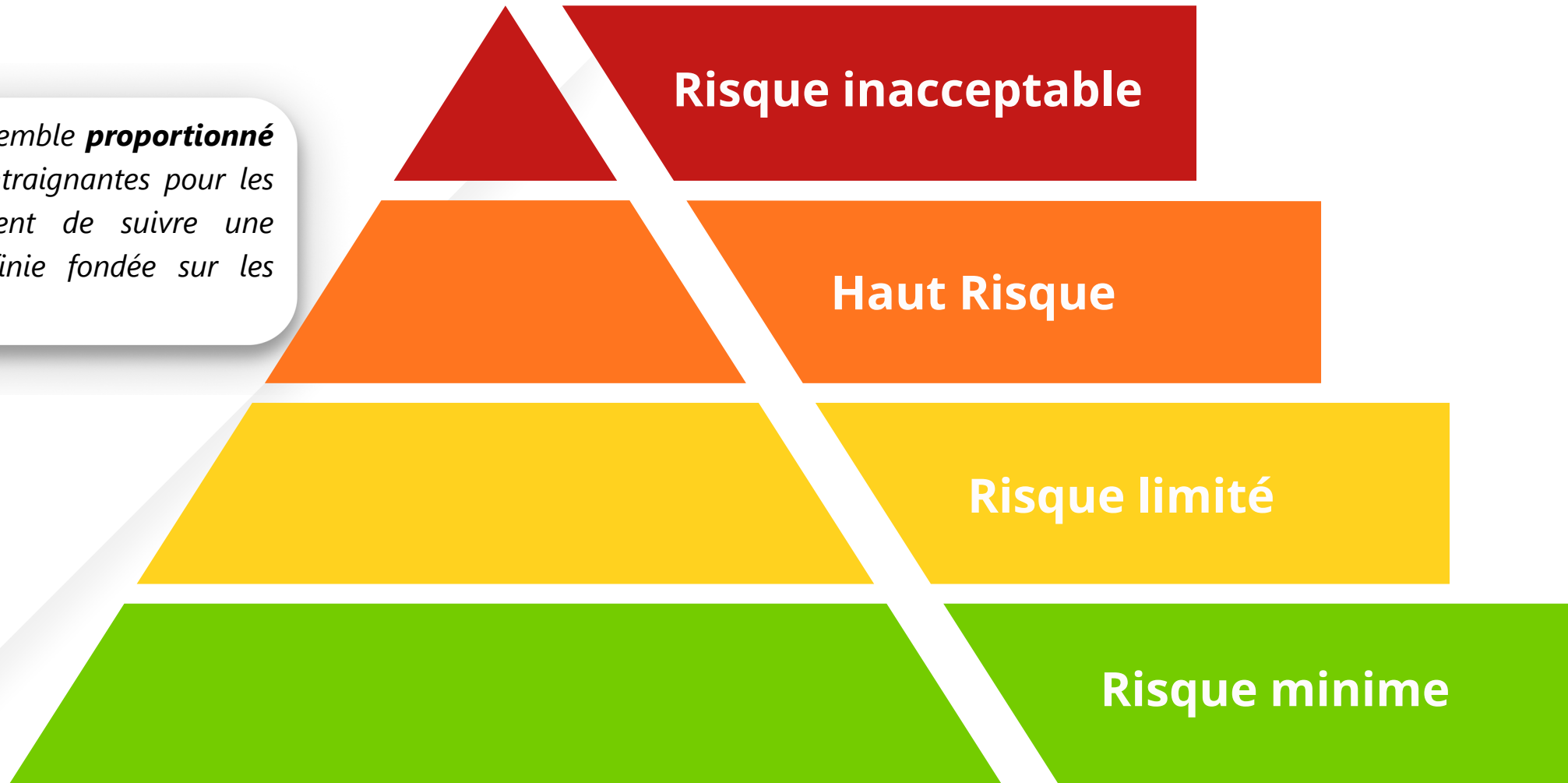


DÉPLOYEUR

Utilise sous sa propre autorité un système d'IA à titre professionnel.



« afin d'introduire un ensemble **proportionné et efficace** de règles contraignantes pour les systèmes d'IA, il convient de suivre une approche clairement définie fondée sur les risques »



PRINCIPE : GARANTIR LA TRANSPARENCE, LA CLARETE ET L'INTELLIGIBILITE

Les technologies d'IA devraient être intelligibles ou compréhensibles pour tous : développeurs, professionnels utilisant les SIA, patients, etc.

L'OMS encourage une information en amont de la conception et du déploiement de l'IA pour permettre un débat public sur la conception, le déploiement et l'utilisation de l'IA.

L'**AI ACT** met en exergue :

- la formation des **professionnels**
- l'information des **patients**.



AI ACT : FORMATION DES PROFESSIONNELS

OBLIGATIONS APPLICABLES AUX SYSTÈMES D'IA INDÉPENDAMMENT DE LEUR NIVEAU DE RISQUE

Article 4 de l'AI Act :

Les fournisseurs et déployeurs s'assurent d'un niveau suffisant de maîtrise de l'IA pour leur personnel et autres personnes s'occupant du fonctionnement et de l'utilisation des systèmes

Maîtrise de l'IA = Les **compétences**, les **connaissances** et la **compréhension** qui permettent aux fournisseurs, aux déployeurs et aux personnes concernées (...) de procéder à un **déploiement des systèmes d'IA en toute connaissance de cause**, ainsi que de **prendre conscience des possibilités et des risques que comporte l'IA**, ainsi que des préjudices potentiels qu'elle peut causer.



La réglementation des SIA à haut risque

Article L4001-3 CSP (loi de bioéthique)

Le patient est informé de l'usage d'un dispositif médical comportant un traitement de données algorithmique dont l'apprentissage a été réalisé à partir de données massives.

Il peut, le cas échéant, être averti de l'interprétation qui en résulte.
Les données le concernant utilisés pour ce traitement lui sont accessibles.



AI ACT

Droit à l'explication des décisions individuelles prises à l'aide du SIAHR, lorsqu'elles produisent des effets juridiques ou significatifs que le patient perçoit comme ayant une incidence négative sur sa santé, sa sécurité ou ses droits fondamentaux.

Droit de demander au déployeur une explication claire et pertinente sur :

- Le rôle du SIA dans la procédure décisionnelle
- Les principaux paramètres de décision

PRINCIPE : Encourager la responsabilité et l'obligation de rendre des comptes



Ethik - IA
Garantie Humaine de l'



Il incombe aux parties prenantes de veiller à ce que les SIA soient utilisées dans des conditions appropriées et par des personnes dûment formées.

Des mécanismes efficaces doivent être mis en place pour permettre aux individus lésés par des décisions fondées sur des algorithmes de contester ces décisions et d'obtenir réparation.

Responsabilité du concepteur

- Informer les utilisateurs (documentation, notice d'utilisation, capacités et limites du système, etc.)
- Concevoir le système correctement (qualité des données, cybersécurité, etc.)

En cas de dommage ?

Remonter la chaîne des responsabilités.

Responsabilité du déployeur

- Utiliser correctement le système (conformément à la notice, dans le respect du périmètre et de la finalité du système, etc.)
- Maintien de la compétence
- Informer les patients

En cas de dommage ?

Remonter la chaîne des responsabilités.



PRINCIPE : PROTÉGER L'AUTONOMIE DE L'ÊTRE HUMAIN

Les individus doivent rester maîtres des systèmes de soins et des décisions médicales.

Comment garantir que l'humain garde la main ?

- Par le biais de formations sur l'éthique et le juridique : responsabilité, information des patients, biais cognitifs
- En démystifiant :
 - Apprendre à ne pas humaniser les systèmes d'IA
 - Connaître les capacités mais aussi les limites
- Est-ce que le contrôle humain est toujours pertinent ?



Ethik - IA
Garantie Humaine de l'



Article 26 : le déployeur

Les utilisateurs de systèmes d'IA **ont en charge la mise en oeuvre du contrôle humain** permise par le fournisseur.

Ils ont la faculté

- **d'organiser leurs propres ressources et activités aux fins de la mise en oeuvre des mesures de contrôle humain.**
- **d'appréhender les capacités, limites et risques engendrés par le système d'IA à haut risque**, ce qui leur permet de suspendre son utilisation, conformément à l'article 14.

4

Ethik - IA
Garantie Humaine de l'

Garantie Humaine et gouvernance IA :
quel cadre pour les pharmaciens d'officine ?

Mettre en place une gouvernance de l'IA en officine

Ce guide propose un cadre simple pour déployer l'IA en officine de manière sécurisée, avec des rôles clairs, une lecture des risques et une supervision humaine.

Étape 1. Organiser le pilotage

Le pharmacien titulaire porte la démarche

Il peut aussi assurer le rôle de référent IA

Un appui RGPD peut être sollicité si besoin

Étape 2. Recenser les usages de l'IA

Lister les outils déjà utilisés ou envisagés

Préciser leur finalité et les données mobilisées

Identifier les bénéfices attendus et les points de vigilance

Exemples : gestion des stocks, rédaction interne, analyse documentaire, alertes métier

Étape 3. Classer par niveau de risque

Usage acceptable

Exemples : tri de mails non médicaux, rédaction interne

Règle : aucune donnée patient identifiable

Usage sensible

Exemples : gestion des stocks (données métier), alertes

Règle : validation préalable et contrôle humain

Usage critique

Exemples : outil influençant une décision de santé

Règle : analyse renforcée ou exclusion de l'usage

Étape 4. Poser les règles d'usage

Définir une finalité précise

Limitier les données au strict nécessaire

Interdire les outils non validés pour les données patients

Maintenir une supervision humaine systématique

Assurer la traçabilité des usages

Étape 5. Évaluer les fournisseurs

Vérifier l'hébergement et la sécurité

Examiner les garanties contractuelles et le cadre RGPD

Évaluer les impacts et les limites de la solution

Point de vigilance : données de santé, sous-traitance, réutilisation des données, localisation de l'hébergement

Étape 6. Former l'équipe et suivre

Former l'équipe aux bons usages de l'IA

Savoir repérer les erreurs, biais et hallucinations

Prévoir une revue régulière des outils et incidents

Actualiser les règles si les usages évoluent

 **Rythme conseillé :** un point tous les 3 mois



L'IA assiste l'officine, mais la décision finale et la responsabilité restent humaines.

La gouvernance de l'IA en officine : sécuriser le parcours de soins

LES ÉTAPES DE LA GOUVERNANCE DE L'IA



Piloter et recenser les usages

Désigner un responsable et lister chaque outil utilisé au sein de l'officine.



Évaluer les risques et les fournisseurs

Classer les outils par niveau de risque et vérifier la conformité des fournisseurs.



Former l'équipe et suivre les impacts

Former l'équipe aux bons usages de l'IA et suivre les résultats dans le temps.



HÔPITAL

Source d'informations et point de départ du parcours

L'OFFICINE AU CŒUR DU PARCOURS COORDONNÉ

Le point de contrôle humain

L'officine valide les suggestions de l'IA pour sécuriser la dispensation des médicaments.

La coordination hôpital-ville

Le pharmacien facilite la continuité du traitement entre l'hôpital et la ville.

La garantie pour le patient

Le patient bénéficie d'une information claire et d'une décision finale toujours humaine.



VILLE

Acteurs de ville coordonnés



PATIENT

Bénéficiaire d'une prise en charge coordonnée et informée

Idee centrale : L'Officine encadre les usages de l'IA, garde la décision humaine et sécurise la relation avec le patient dans le parcours hôpital-ville.

L'IA peut assister le parcours, mais la confiance repose sur l'information du patient, la coordination des acteurs et la responsabilité humaine.

Ethik - IA
Garantie Humaine de l'

MERCI !



Françoise Tran

Responsable de projet innovation



ftran@ethik-ia.fr



URPS Pharmaciens
Centre-Val de Loire





Table Ronde

Animée par
Françoise Guegan & Vanessa Auroux

Participants

Elisa BENAZECH
Patrice LAIGLE
Cyril LEROSSIGNOL
Ugo SCHURIG
Françoise TRAN

**Posez toutes vos
questions !**

Alors... Deux boîtes de Rinoxel et un peu
d'empathie... Pour l'empathie, voyez
avec ma collègue.

