



Ethique, cybersécurité et protection des données dans l'enseignement numérique des sciences de la santé

Pr ERIC NSEME

MÉDECIN LÉGISTE EXPERT – FMSB/UYI

Plan

- I. Introduction
- II. Données à protéger
- III. Cadre juridique camerounais
- IV. Cadre sécuritaire
- V. En pratique
- VI. Conclusion

I- Introduction

Importance du sujet

HIER

Amphithéâtre

Polycopiés

Dossiers papiers

Enseignement essentiellement en présentiel

AUJOURD'HUI

Visioconférences

Réseaux de communication, IA

Simulation

Enseignement présentiel + distanciel

Nouvelle réalité : **l'étudiant devient producteur, collecteur, détenteur et diffuseur de données.**

II- Données à protéger

Cas pratique

- ❑ Une étudiante partage dans un groupe WhatsApp : photographie d'une lésion + dossier clinique + résultats biologiques.
- ❑ Le nom est retiré, mais restent : âge, hôpital, date, photographie du visage et numéro de dossier partiel.
- ❑ Un étudiant réutilise l'image dans un PowerPoint.
- ❑ Un autre transmet les données à une IA générative pour obtenir un diagnostic différentiel.
- ❑ **Question : combien de problèmes éthiques et médico-légaux identifiez-vous ?**

Question :

Quels problèmes éthiques et médico-légaux identifiez-vous?

Trois questions dans trois disciplines

ÉTHIQUE

Est-ce souhaitable ?

Autonomie
Dignité
Confidentialité
Bienfaisance
Non-malfaisance
Justice

Éthique → pourquoi ?

PROTECTION

Est-ce légitime ?

Finalité
Nécessité
minimisation
Accès
Conservation
Responsabilité

Droit → dans quelles conditions ?

CYBERSÉCURITÉ

Est-ce protégé ?

Authentification
Accès
Chiffrement
Sauvegarde
Traçabilité
Incident

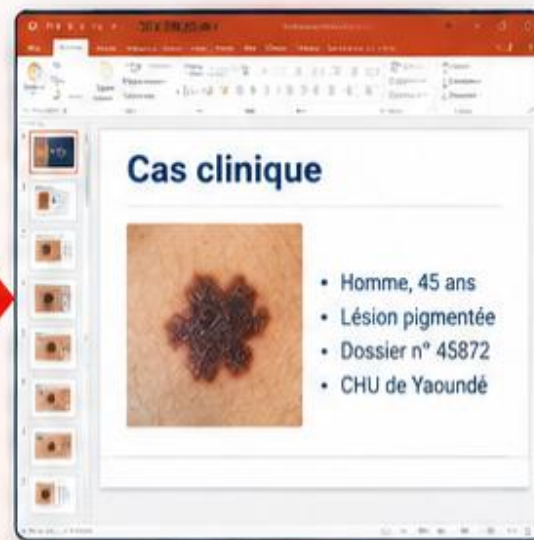
Sécurité → comment protéger ?

❌ Le cas du fil rouge – Version à risque (erreurs à éviter)

Une simple photo peut voyager très loin...
au-delà de ce que vous imaginez !



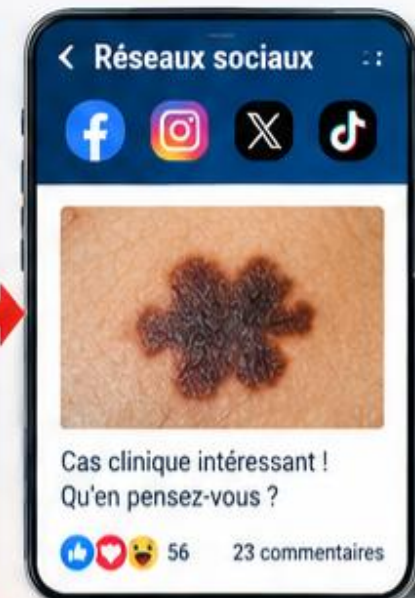
1. L'étudiante partage une photo d'une lésion avec des données cliniques dans un groupe WhatsApp.



2. Un autre étudiant utilise la photo dans une présentation PowerPoint.



3. La photo et les données sont envoyées à une IA générative.



4. La photo finit par être partagée sur les réseaux sociaux.



Les erreurs constatées

- ❌ Publication d'une image identifiable sur WhatsApp.
- ❌ Transmission du dossier à une plateforme non sécurisée.
- ❌ Envoi des données cliniques à une IA publique.
- ❌ Suppression du nom du patient jugée suffisante.
- ❌ Utilisation de la photo dans un cadre non autorisé.
- ❌ Risque de réidentification (âge, sexe, lieu, date, etc.).

Les données à protéger

PATIENTS

Dossier
Images
Biologie
Génétique
Voix
Données médico-légales

ÉTUDIANTS

Notes
Evaluations
Biométrie
Traces de connexion

ENSEIGNANTS

Cours
Examens
Corrections
Evaluations
Données personnelles

Une photographie clinique peut rester identifiable même sans le nom.

DONNÉE PÉDAGOGIQUE ≠ DONNÉE LIBRE

Le piège de la « désidentification »

SUPPRIMER LE NOM

≠

ANONYMISER

Ce qui peut être réidentifié

Âge + sexe + lieu + date + pathologie rare

Photographie + contexte clinique

Numéro de dossier + métadonnées

Deux notions

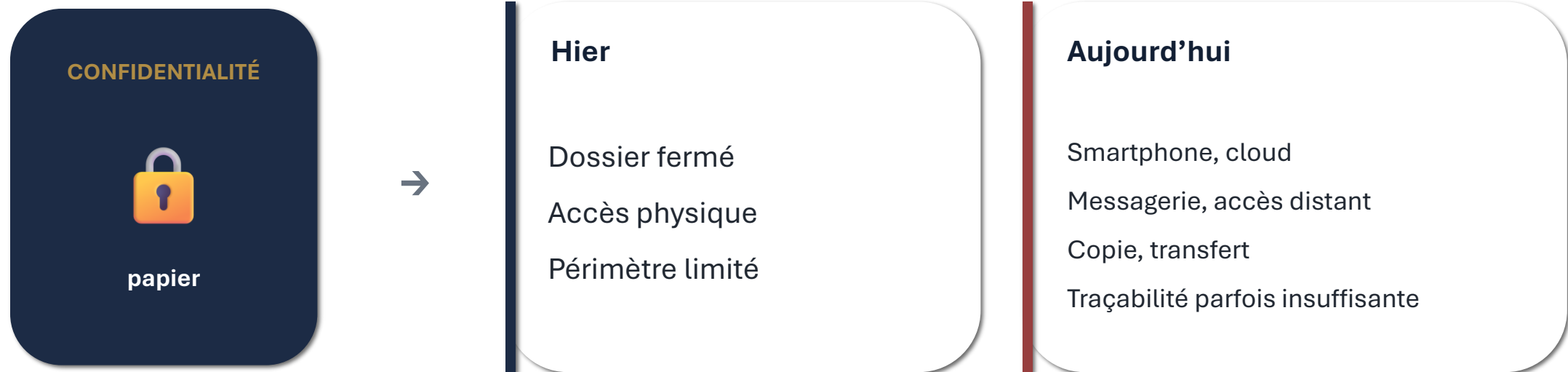
ANONYMISATION : réidentification
raisonnablement impossible

PSEUDONYMISATION : un code remplace
l'identité, mais le lien peut être retrouvé

Règle : raisonner sur le risque de réidentification, pas seulement sur la présence du nom.

III- Cadre juridique camerounais

Le secret médical change de support, pas de nature



Question : l'étudiant a-t-il besoin de connaître l'identité du patient pour apprendre ?

En pratique : l'étudiant ne doit avoir accès qu'au minimum nécessaire

Le cadre juridique camerounais

01

Vie privée & confidentialité

Principes constitutionnels et droits de la personne

02

Secret professionnel

Code pénal et déontologique

03

Cyber & communications

Loi n°2010/012 du 21 décembre 2010 et textes relatifs aux communications électroniques

04

Institution

Règles universitaires, hospitalières, contrats et procédures internes

IV- Cadre sécuritaire

Les 7 portes d'entrée du risque pour une faculté de médecine

1

PHISHING

2

IDENTIFIANTS

3

RANSOMWARE

4

TÉLÉPHONE

5

CLOUD

6

APPLICATIONS

7

SOCIAL

CHAINE D'EXPOSITION : PATIENT → ÉTUDIANT → SMARTPHONE → PLATEFORME → CLOUD → TIERS

**« Si la donnée était celle
de votre propre dossier médical... »**

La partageriez-vous de la même manière dans un réseau social
académique ou professionnel ?

IA générative

Usages pédagogiques

Cas cliniques
QCM
Simulation
Reformulation
Scénario
Apprentissage personnalisé

→ **Fort potentiel pédagogique**

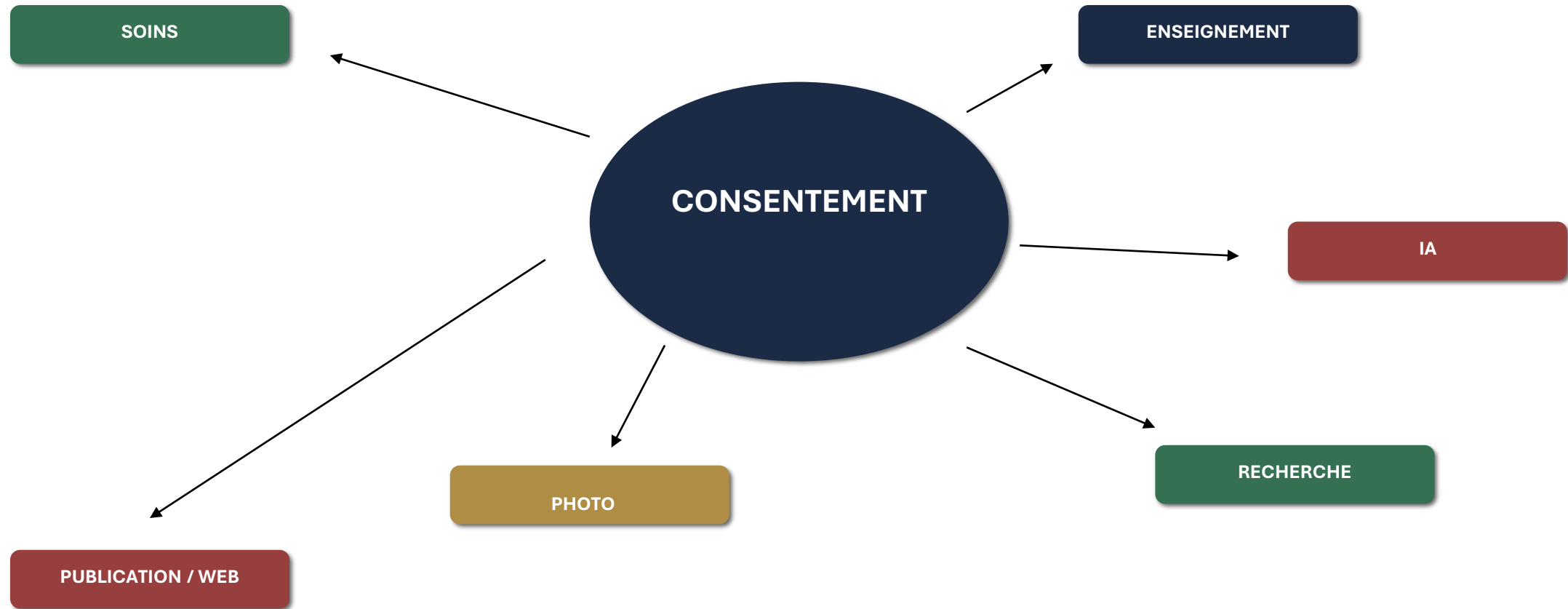
Zone rouge

Nom + dossier + photographie
Résultats biologiques identifiants
Contexte rare ou médico-légal

→ **Ne pas verser ces données dans une IA publique sans cadre approprié**

« Une IA n'est pas un coffre-fort parce qu'elle est facile à utiliser. »

Le consentement éclairé



Soins ≠ photographie ≠ enseignement ≠ recherche ≠ diffusion ≠ IA

V- En pratique

La règle des 5M



Avant de déposer une image clinique :

Puis-je ? Est-ce nécessaire ? Est-elle identifiable ? Qui y accède ? Combien de temps ?

10 mesures pour une faculté de médecine au plan numérique

- | | | | |
|----|---|----|-------------------------------------|
| 01 | Charte de l'enseignement numérique | 02 | Politique de protection des données |
| 03 | Pas de données identifiables sur plateformes personnelles | 04 | Espaces sécurisés pour cas réels |
| 05 | Formation cyber obligatoire | 06 | Authentification forte |
| 07 | Droits d'accès maîtrisés | 08 | Procédure de signalement d'incident |
| 09 | Cadre spécifique pour l'IA | 10 | Audit éthique + cyber périodique |

La cybersécurité n'est pas seulement une fonction informatique, c'est une responsabilité professionnelle.

Retour au cas

À éviter

- WhatsApp avec données identifiantes
- Dossier transmis à une plateforme publique
- Image réutilisée sans cadre
- Données cliniques identifiables dans IA

À privilégier

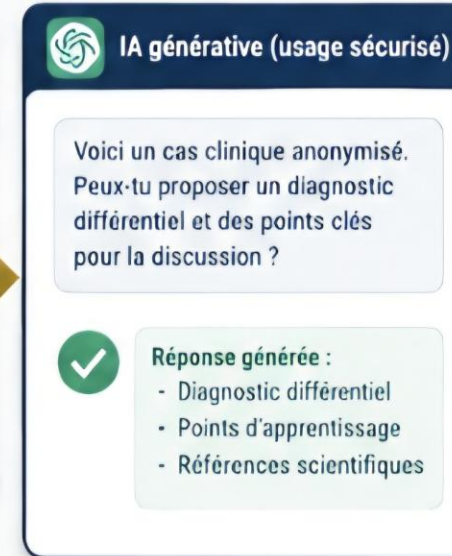
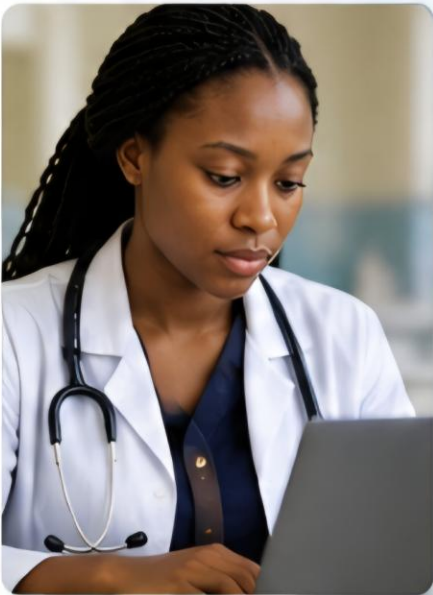
- Cas anonymisé correctement
- Image non identifiable
- Plateforme institutionnelle sécurisée
- IA avec données non identifiantes

Objectif : préserver simultanément VALEUR PÉDAGOGIQUE + CONFIDENTIALITÉ + SÉCURITÉ



Le même cas – Version sécurisée (bonnes pratiques)

Même objectif pédagogique...
mais avec des données protégées !



1. L'étudiante utilise un cas correctement anonymisé et une plateforme institutionnelle sécurisée.

2. L'image est anonymisée et ne contient aucune donnée personnelle.

3. La présentation est faite avec des données non identifiantes.

4. L'IA est utilisée uniquement avec des données non identifiantes.



Les bonnes pratiques

- ✓ Anonymiser correctement les images et métadonnées.
- ✓ Utiliser les plateformes institutionnelles.
- ✓ Obtenir le consentement si nécessaire.

- ✓ Limiter l'accès aux personnes habilitées.
- ✓ Former et sensibiliser les étudiants et enseignants.
- ✓ Toujours se poser la question : « Puis-je l'utiliser ? »

VI- En conclusion

En conclusion

ÉTHIQUE

Respecter la
personne

JURIDIQUE

Respecter
confidentialité et
règles applicables

PÉDAGOGIQUE

Mettre la technologie au
service de
l'apprentissage

CYBER

Protéger les données
collectées

Je vous remercie de votre aimable attention!
