Protection des données de santé

Hey ! Je suis Cylia, votre tutrice de Santé Publique/Santé Numérique. Ici on s'attaque à mes cours de SN, les notions de ce cours sont importantes et elles tombent souvent à l'examen donc je te surveille on ne les met pas de côté !

Plan du cours :

---

1. Concepts et champs légaux d'application

A. Données à caractère personnel

Donc une **Donnée à caractère personnel** c'est :
(selon l'article 2 de la Directive 95/46/CE du Parlement Européen et du Conseil du 24 Octobre 1995)

- ★ Toute information relative à **une personne physique** identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont **propres** (identité physique, physiologique, psychique, économique, culturelle ou sociale).
- ★ Pour déterminer si une personne est identifiable, il faut considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne

Toute information relative à une personne identifiée ou susceptible de l'être.

Exemple : *Numéro de sécurité sociale, numéro d'ordre renvoyant à une liste nominative même établie sur papier, prélèvement biologique, identifiant, identification par recoupement d'information.*

B. Utilisation des données

Ces informations **médicales personnelles** sont une **ressource essentielle** dans les domaines de l'épidémiologie, de la maîtrise des dépenses de santé, du commerce et des assurances.
C'est parce qu'elles intéressent beaucoup de monde qu'elles doivent être protégées.
Par exemple, les épidémiologistes font des études pour l'intérêt de l'ensemble de la population. Cependant ils n'ont pas de malades et n'ont donc pas à savoir qui est qui c'est le **principe du secret médical** *(notion vu en éthique)*.

On peut partager ce secret médical... Mais avec qui ?
Ce sont **les ordonnances de 1996** qui précisent qu'en dehors des soignants, seuls les inspecteurs de l'action sanitaire et social et les médecins conseils ont accès au secret médical.

C. Traitement des données

Il faut caractériser ce qu'est un fichier avant ça ;
Fichier : tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

La notion de traitement (Article 2) c'est des opération ou un ensemble d'opérations portant sur des données personnelles, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction
Exemples : *Constitution de fichiers, de bases, toute procédure, de télétransmissions d'informations quel que soit le moyen de télécommunications (réseaux, cartes Vitale, Internet...)*
Oui ça fait beaucoup mais ne vous inquiétez pas...

D. Traitement informatique

Le ttt (*Traitement*) informatique c'est :

- ★ une catégorisation
- ★ une concentration des données + importantes
  - *S'il y a une défaillance de la protection, il existe donc un DANGER +++ car on peut avoir accès à TOUTES les informations en même temps.*
- ★ Il y a une **puissance du ttt**
  - ***Identification** des personnes par recoupement*
- ★ **Interconnexion** et **dispersion**
  - *Une donnée isolée est potentialisée s'il y a une relation possible avec d'autres informations*
- ★ **Portabilité** et **appropriation**

On passe sur un petit tableau donc je le met sur l'autre page pour pas qu'il soit coupé <3

E. Notions de responsable et destinataire

RESPONSABLE *(article 3 - I)*	**QUI ?** La personne, l'autorité publique, le service ou l'organisme qui détermine les **finalités** et les **moyens nécessaires** à sa mise en œuvre, sauf désignation expresse par les dispositions législatives ou réglementaires. **OÙ ?** Il est établi sur le territoire français (installation stable, quelle que soit sa forme juridique, filiale, succursale...) où il a recours à des moyens de traitement situés en zone française.
DESTINATAIRE *(article 3 - II)*	**QUI ?** Toute personne **habilitée** à recevoir une **communication des données** autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. *Explication : On ne peut pas être responsable et destinataire à la fois ! Par exemple, vous écrivez un article, vous êtes au courant du contenu de l'article comme vos collaborateurs, vous n'êtes donc pas des destinataires. Lorsque l'article sera publié, les lecteurs seront des destinataires.* Les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication ne constituent pas des destinataires

F. Données médicales

L'expression « **données médicales** » se réfère à toutes les données à **caractère personnel** relatives à la **santé** d'une personne. Elle se réfère également aux **données ayant un lien manifeste et étroit avec la santé ainsi qu'aux données génétiques.**

Annexe de la recommandation R (97) 5 du 13 février 1997 relative à la protection des données médicales

G. Données de santé

Les **données de santé**, comme les données relatives aux origines raciales, à l'opinion politique, à la vie sexuelle, sont des données sensibles dont le **traitement est en principe interdit** (*Article 8*).
En principe c'est tout le temps vrai sauf qu'il existe des exceptions qu'on va voir ...

Des dérogations sont prévues (*Art 8. II*) **:**

- ★ Consentement **exprès** des personnes sauf disposition contraire.
- ★ Les traitements nécessaires aux fins de **médecine préventive**, des **diagnostics**, de **l'administration de soins** ou de traitements ou de la **gestion de services de santé** qui est mis en œuvre par un professionnel de santé ou par une personne tenue au secret.
- ★ Les traitements de données de santé à des fins de **recherche médicale**.
- ★ Les traitements de données sensibles susceptibles de faire l'objet, à bref délai, d'un procédé d'anonymisation reconnu conforme par la CNIL.
- ★ Les traitements de **données sensibles**, justifiés par **l'intérêt public** et **autorisés par la CNIL** ou par décret en CE après avis de la CNIL. *Mais c'est quoi la CNIL ?? ATTENDEZ*

2. Cadre légal

FRANCE	**Loi du 6/01/78 :** loi Informatique, Fichiers et Libertés (IFL), relative au développement, à l'utilisation et la **protection des fichiers informatiques et manuels**++ Institution de la **CNIL** *(Commission Nationale Informatique et Libertés)* par cette loi : **Autorité administrative indépendante** +++ chargée de veiller au respect de la loi. Elle protège la vie privée et les libertés individuelles ou publiques. Cette loi a subi plusieurs modifications mais seule la **modification de 2004** est **importante** : ➔ *modification en 92 : dispositions pénales* ➔ *modification en 94 : traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé* ➔ *modification en 99 : traitements des données personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins ou de prévention* ➔ *modification en 2000 : collecte, enregistrement et conservation des informations nominatives* ➔ *modification en 2004 : droits de la personne renforcés, allègement des formalités déclaratives auprès de la CNIL, contraintes nouvelles pour les transferts de données hors UE, nouveaux pouvoirs de la CNIL : sanctions et labellisation, institution du « correspondant CNIL » (le CIL : correspondant Informatique et Libertés)* ***Textes :*** ★ ***Code de déontologie* = Article 4** ★ ***Code pénal* = Article 226-13** ★ ***Code de la santé publique***
EUROPE	Recommandations du conseil de l'Europe du 3/01/81 relatives aux banques de données médicales automatisées. **Directive du 24/10/95 :** vise à réduire les divergences entre législations nationales sur la protection des données personnelles au sein de l'Europe. **Règlement de la protection des Données (RGPD) du 25 mai 2018**

*Dans cette partie sur la réglementation, faites bien la **différence** entre **France** et **Europe** ! Essayez de retenir les **objectifs**, les **directives** des lois.*

3. Principes de la loi IFL

A. Protection des données

★ **La confidentialité des informations :**

Seuls les utilisateurs habilités dans les conditions normalement prévues doivent avoir accès aux informations

★ **L'intégrité des informations :**

Les informations sont modifiables uniquement par les utilisateurs habilités dans les conditions d'accès normalement prévues.

★ **La disponibilité des informations :**

Les informations peuvent en permanence être employées par les utilisateurs habilités dans les conditions d'accès et d'usage normalement prévues.

B. Déclaration

Avec la loi du 6/01/78 (**IFL**), tout fichier informatisé nominatif de façon directe ou indirecte doit être déclaré à la CNI .+++

Le déclarant doit spécifier : ++++

- ➔ Les **objectifs** de la banque de données,
- ➔ L'organisme de **conservation**,
- ➔ L'organisme de **production** des données qui **contrôle** le droit d'accès,
- ➔ Les catégories d'informations traitées et les différents utilisateurs.

*On y différencie 2 types de déclarations ; les **déclarations normales** et les **déclarations simplifiées**.*

a) Déclaration Normale

Contenu de la déclaration : (*Article* 30)

L'identité du responsable, la ou les finalités du traitement, les interconnexions éventuelles, les données traitées, leur origine, les catégories de personnes concernées, la durée de conservation, le ou les services chargés de mise en œuvre, les destinataires des données, le service auprès duquel s'exerce le droit d'accès, les dispositions prises pour assurer la sécurité des données, le cas échéant, les transferts de données vers un État non membre de la Communauté européenne.

Description des mesures :

Des mesures **obligatoires** de protection des **fichiers informatiques** en découlent :

> **Identification et authentification** des utilisateurs
> Définition des **droits d'accès et d'utilisation**
> **Encryptage**
> Surveillance des **connexions**

> **Protections** des fichiers
> **Sauvegarde**
> **Sécurité** contre les virus et le piratage
> **Alimentation électrique** constante et protégée, etc…

b) *Déclaration Simplifiée*

La CNIL peut adopter des **normes simplifiées** pour les traitements les plus courants dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés. Il existe aujourd'hui **54 normes** (les normes sont sur le site de la CNIL ; *www.cnil.fr*) :

Le professeur en a mis des exemples donc je vous les met aussi

- ★ gestion de cabinets médicaux et paramédicaux (n°50)
- ★ gestion des pharmacies (n°52)
- ★ gestions des LABM (n°53)
- ★ gestion des centres d'optique (n°54)
- ★ gestion du personnel (n°46),
- ★ contrôle d'accès (n°42)
- ★ gestion des membres des associations (n°23)
- ★ utilisation de services de téléphonie fixe et mobile sur les lieux de travail (n°47),

Si le traitement envisagé correspond en tous points à une norme, un engagement de conformité suffit.

C. La finalité

★ **Une finalité** (*Article 6-2*) doit être :

- **Déterminée**
- **Explicite**
- **Légitime**, correspondant aux missions de l'organisme

Les données traitées doivent être **adéquates, pertinentes** et **non excessives** par rapport aux finalités pour lesquelles elles sont collectées (*Article 6-3°*).
Tout **détournement de finalité est passible de sanctions pénales** (*Article 226-21 code pénal*) : 5ans d'emprisonnement, 300 000 euros d'amende.
(Ici vous retenez simplement qu'on peut être sanctionné)
Exemples : *Les fichiers obligatoires (publics) ne peuvent être utilisés à des fins politiques ou commerciales / zones commentaires (« timide, menteur », …), fichiers bancaires…*

D. Obligation de sécurité

★ Il appartient au **responsable du traitement** de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la **sécurité des données** et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès (*Article 34 de la loi modifiée*).

★ **Respect de l'intégrité et de la confidentialité des données :** empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès.
★ Une **obligation** qui pèse sur le responsable du traitement

Les mesures de sécurité **physique** et **logique** doivent être adaptées à la nature des données et aux risques présentés par le traitement *(ex: chiffrement des données sur Internet)* :

IDENTIFICATION	➔ processus par lequel une « entité » informe le système distant de son **identité** ➔ Généralement l'identifiant se compose du nom de l'utilisateur, ou d'un numéro d'utilisateur, ou de tout autre identifiant qui permet au système de savoir avec "qui" il va entrer en communication *(ex : login / carte à puce, carte vitale)*
AUTHENTIFICATION	➔ élément qui caractérise une personne ou une « entités » et autorise l'accès au système *(ex : Mot de passe, emprunte digitale)* ➔ L'authentification est un **outil essentiel de la confidentialité** : celui qui accède à une donnée est bien celui qui est autorisé à le faire
GESTION DES ACCÈS	➔ tableau des habilitations
PRECAUTIONS ELEMENTAIRES	★ L'accès à l'application doit être protégé par des mots de passe individuels, alphanumérique d'une longueur de 6/7 caractères au moins. Évitez les mots de passe trop courants (évitez initiales, nom, prénom, SESAM etc.). Changez les régulièrement ★ Éteindre le PC en cas d'absence, déconnexion automatique, écran de veille protégé par un mot de passe ★ En cas de connexion à l'Internet : antivirus ; « parefeu » (firewall)/ séparation physique des réseaux ★ Effectuez régulièrement des sauvegardes (CD-Rom, disquettes) et conservez-les dans un lieu différent de la base de données.. ★ Lors de la numérisation et de la compression des images (imagerie médicale), utilisation de procédures normalisées permettent de garantir l'intégrité de ces données. ★ Lorsque des données de santé sont transférées via Internet, il convient de recourir à un dispositif de chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits, messagerie sécurisée...). ★ Mise en place de protocoles de transmission adaptés permettant de vérifier la conformité des données reçues à celles émises ★ Pour les applications en réseau : ○ Par-feu (firewall) ○ Maintenance des matériels : ne pas laisser emporter le disque dur si les données sont en « clair » ○ Limiter à tout prix le nombre d'informaticiens ayant le profil « super-utilisateur » ou « administrateur système » ○ En fonction des données traitées, traçabilité, journalisation des connexions

E. Les droits des personnes

I. DROIT À L'INFORMATION PRÉALABLE ET CONSENTEMENT ÉCLAIRÉ
II. DROIT DE CURIOSITÉ
III. DROIT D'ACCÈS DIRECT ET INDIRECT
IV. DROIT DE RECTIFICATION
V. DROIT À L'OUBLI

➔ **DROIT À L'INFORMATION (ARTICLE 32) : LE DROIT D'ÊTRE INFORMÉ**

- de l'identité du responsable
- de la finalité poursuivie par le traitement
- du caractère obligatoire ou facultatif des réponses, des conséquences à leur égard
- d'un défaut de réponse des destinataires des données
- de l'existence d'un droit de s'opposer pour des raisons légitime au traitement, un droit
- d'accès et de rectification *(et le cas échéant, des transferts à destination d'un État non membre de la Communauté européenne)*

➔ **DROIT D'OPPOSITION :**

Pour des **raisons légitimes** (*art.* 38), sauf si le traitement répond à une obligation légale :

- Discrétionnaire en matière de recherche médicale (*art.* 56) et d'utilisation des données à des fins de prospection commerciale

➔ **DROIT DE RECTIFICATION (ARTICLE 40)**

Modalités d'information : Affichettes dans les établissements de santé, à l'accueil des caisses, note d'information sur le site web de l'organisme, lettre de présentation de l'étude

➔ **DROIT À L'OUBLI :**

- Une durée de conservation **limitée** en adéquation avec la **finalité** poursuivie par le traitement (*Article* 6-5). La durée de conservation doit être **mentionnée** dans le dossier de formalité et limitée.

On fait la distinction entre la conservation en ligne des données et l'archivage. Au-delà de cette durée les données ne peuvent être conservées qu'en vue de leur traitement à des fins historiques, statistiques ou scientifiques (Article 36)
Les traitements des archives publiques sont dispensés des formalités préalable.

Super, tu as fait la plus grosse partie ! Il y a beaucoup de définitions c'est vrai mais tout est assez logique. Si tu as des doutes, reprends les parties précédentes et n'essaye pas de tout retenir du premier coup ... En premier essaie de bien comprendre !

4. Accès au dossier médical

A. Mesures de protection

Protection des données médicales :
Ex : suppression des feuilles de température et des prescriptions au lit du malade, ...

- ★ Mesures de protection des informations nominatives au niveau du circuit et du stockage du dossier médical. (*Ex : suppression des éléments nominatifs ou distinctifs*)
- ★ Procédures de destruction des documents nominatif

B. Propriété du dossier

Le patient **(loi du 4 mars 2002 dite Kouchner)** C'EST IMPORTANT

- ★ Le médecin et l'établissement sont co-propriétaires du dossier médical.
- ★ Le médecin et l'établissement qui établissent et conservent le dossier en sont les dépositaires

C. Accès au dossier

Les personnes suivantes ont accès au dossier **(les informations du dossier)** :

- ★ Le patient lui-même : avec la loi du 4 mars 2002 qui garantit l'accès direct du patient à son dossier médical
- ★ La personne de confiance (parent, proche, médecin, ...)
- ★ Les ayants droits d'un patient décédé sous certaines conditions
- ★ Le médecin libéral et les médecins du service public hospitalier qui soignent le malade (en continuité des soins).

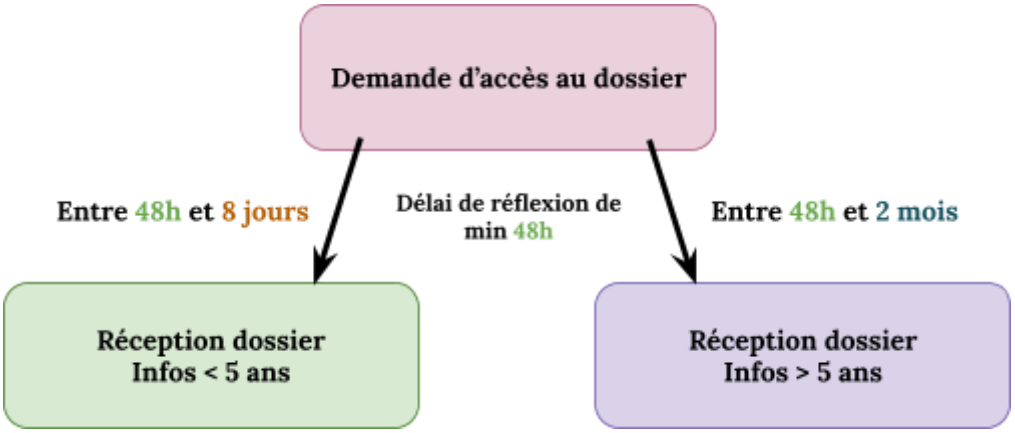
La loi du 4 mars 2002 a posé le principe de l'**accès direct du patient** à l'ensemble des informations de santé le concernant. Ce principe a été repris dans **l'article 43 de la loi «informatique et libertés» (IFL)**. Le décret du **29 avril 2002** a organisé cet accès.

- ★ Délai de communication entre 48h et 8 jours
- ★ Si les données remontent à plus de cinq ans, le délai est porté à deux mois

La présence d'une tierce personne peut être recommandée. L'accès aux données se fait, au choix du demandeur :

- ❖ Soit par consultation
- ❖ Soit par l'envoi des documents

Les frais de délivrance de ces copies ne sauraient excéder le coût de la reproduction et, le cas échéant, de l'envoi des documents



Un petit schéma récap <3

D. Communications des données

Ce dossier contient au moins les éléments suivants, ainsi classés :

1. Ce sont les informations formalisées recueillies lors des consultations externes dispensées dans l'établissement, lors de l'**accueil au service des urgences** ou au moment de l'**admission** et au **cours du séjour hospitalier**.
2. Ce sont les informations formalisées établies à la **fin du séjour**.
3. Ce sont les informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant de tels tiers.

Seules sont **communicables** les informations énumérées au 1. et au 2.

5. Autres dispositions

Le CIL ❤️

Il est défini depuis la refonte de la loi du 6 janvier 1978 en 2004 : **CIL (Correspondant Informatique et Libertés)**
Sa nomination permet un allègement des formalités. On a une dispense de déclaration des traitements.
Cependant ils existent des exceptions :

- ★ sauf les traitements relevant du régime de l'autorisation ou de la demande d'avis,
- ★ sauf lorsqu'il existe un transfert de données à destination d'un État non membre de la Communauté européenne.

La désignation est **facultative** et ouverte à **tout responsable de traitement.**

Le correspondant est chargé d'inscrire sur le registre qu'il tient à jour les traitements mis en œuvre par l'organisme.

- ➔ Il assure localement et de manière **indépendante**, une meilleure application de la loi et ainsi diffuse la culture informatique et libertés. ++
- ➔ Il permet de disposer de **relations privilégiées** avec la CNIL : service dédié, information ciblée et adaptée. ++

Le CIL a un rôle de :

- ★ **Conseil :** il est saisi pour avis avant la mise en œuvre de tout nouveau traitement, prépare les dossiers de formalités pour les traitements à risque
- ★ **Recommandation :** il traduit les termes de la loi en règles internes ou codes de conduite propres au secteur d'activité.
- ★ **Médiation :** il reçoit les plaintes et requêtes des personnes concernées par les traitements (droit d'accès notamment)
- ★ **Alerte :** il informe le responsable de traitement des manquements constatés.
- ★ **Information :** il dresse un bilan annuel qui est le reflet de son action (traitements examinés, recommandations émises…

6. Récapitulatif et évolution

★ **Code de la santé publique**

- Obligation de **confidentialité des données médicales**
- Droit d'être **informé**
- Droit d'**accéder aux informations**
- Obligation d'assurer la **sécurité du stockage des données.**

★ **Les 5 points clés de la loi IFL**

1. **Finalité**
   - Les données sont recueillies dans un **but précis, préalablement défini.**
2. **Proportionnalité et pertinence**
   - Seules les informations **pertinentes et nécessaires** au regard des objectifs sont utilisés
3. **Durée de conservation**
   - Pas de conservation **indéfinie** des informations personnelles
4. **Sécurité**
   - **Prendre les** mesures nécessaires pour garantir la sécurité des données
5. **Droit des personnes**
   - Information, accès, rectification, suppression et opposition / consentement sur leurs **données**

★ **COMPLÉTÉ 7.10.2016 (RÉPUBLIQUE NUMÉRIQUE)**

- **Droit à l'oubli** pour les mineurs,
- **Mort numérique :** directives de la personne sur ses données et droits des héritiers,
- **Portabilité des données**,
- En cas de violation des données, obligation d'information des personnes concernées,
- **Montant maximal des sanctions porté à 3 millions d'euros**.

★ CHAPITRE IX DE LA LOI IFL

Désormais applicable en matière de recherche, d'étude ou d'évaluation dans le domaine de la santé **(en complément de la loi Jardé)**.

2 GRANDES CATÉGORIES DE RECHERCHES :

- ➔ d'une part, les recherches impliquant la personne humaine,
- ➔ d'autre part, les recherches, études et évaluations n'impliquant pas la personne humaine.

Sont en particulier visées les recherches nécessitant exclusivement la réutilisation de données de santé à caractère personnel (par exemple celles issues de dossiers médicaux, de cohortes existantes ou du SNDS).

Les traitements de données à caractère personnel ayant pour finalité ces recherches sont soumis à l'autorisation de la CNIL

★ LES NOUVEAUTÉS RGPD (2018)

- Formalités allégées –> Accountability
- Désignation d'un délégué à la protection des données pour certaines entreprises
- Garantir la protection des données par défaut ou dès la conception
- Étude d'impact sur la vie privée
- Signalement des violations de données

Attention : Même avec la mise en œuvre du RGPD, il faut toujours déclarer !

RGPD

En cas de violation de données, il y a obligation de la personne concernée

➔ Il n'y a aucune nuance entre le RGPD et la loi du 7 octobre 2016 puisque le RGPD prévaut comme il est plus récent *(confirmé par le prof)*

C'EST FINIIII !!! Bravo d'être arrivé à la fin <33

PLACE AUX DÉDIS

Dédi à VOUS en 1er vraiment, bravo pour votre année jusqu' ici. Continuez à croire en vous, ne vous comparez pas. On va tout faire pour vous aider en SP/SN.

Dédi à mes amis du lycée/collège (les ancêtres) qui sont pas en med ; Hedra, Mathias, Thomas, Clément, Jonas, Claire... Bref, ils liront jamais la fiche mais c'est les meilleurs.

Dédi à ceux qui ont supporté la P1 en même temps que nous , Coco, Wael qui vont tout déchirer en Las2 et Zoltan l'année pro !!

Dédi à mon copain le mimi qui a fait une P1 avec moi, qui m'a supportée tout l'année, heureusement qu'il était là <3 Soyez pas seuls pendant votre P1 continuez à voir vos amis, etc... L'année est un marathon, pas un sprint donc prenez soin de vous.

Dédi à mon année de kiné qui m'attends, j'ai vraiment hâte !!

Dédi à la pré rentrée du Tut' (celle du S1) où je fais déjà mes fiches pour le S2.

Dédi à la Biocell du S1, je finis cette fiche pendant votre cours ça mérite. Z'êtes géniaux aussi (Grâce à St.Gigi 🧣)

Dédi à mes 2 co-tuts, Lau et Lyne, vous êtes des mimis.

Dédi à Lau spécialement parce que depuis le lycée c'est un amour, je suis super heureuse d'être au Tutorat avec toi !!

Dédi au super appartement que j'ai toujours pas même le 21 Août.

Dédi à mon chien !!! Je l'adore purée, il me manque.

Dédi aux rencontres du Tutorat, quelle équipe de fous.