Guide Hygiène Cyber sécurité et RGPD

Index

Julien ROUSSELLE
Responsable de la Sécurité des Systèmes d'Information
Centre Hospitalier Universitaire Amiens-Picardie
Groupement Hospitalier de Territoire : Somme Littoral Sud

I. Mots de passe

14 caractères minimum et complexes
Choisir des mots de passe complexes combinant :
majuscules, minuscules, chiffres, caractères spéciaux
Pas facilement identifiable
Différent dans chaque application et entre
l'environnement professionnel et personnel
A changer régulièrement
Ne pas le stocker en clair, ni sur un post it,
ni dans un fichier Excel, … voir les gestionnaires de mots de passe proposés ci-après

Rappel sur les méthodes pour un mot de passe complexe :
Il existe 3 grandes méthodes :

Méthode phonétique :
J'ai acheté 3 CD pour cent euros cet après-midi
ght3CD%E7am

Méthode des premières lettres :
Un tiens vaut mieux que deux tu l'auras
1tvmQ2tl'A

Méthode graphique :
Password
P@$$wØR[)

Aspects réglementaires des mots de passe :

ANSSI : https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf

CNIL et Légifrance :
https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires
https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe
https://www.nextinpact.com/news/100871-choisir-bon-mot-passe-regles-a-connaitre-pieges-a-eviter.htm

Feriez-vous cela ?

Alors ne faites pas ça !

Il existe plusieurs solutions pour sécuriser et archiver ses mots de passe :

Gestionnaires de mots de passe

Keepass, validé par la CNIL et l'ANSSI
https://keepass.info/download.html

Attention au faux Keepass, le sujet étant d'actualité, comme le RGPD
https://www.cyberveille-sante.gouv.fr/cyberveille/908-un-nouveau-malware-baptise-keypass-fait-son-apparition-2018-08-13

Attention aux fausses démarches RGPD : exemple avec RGPD France qui est une arnaque
https://www.tendancehotellerie.fr/articles-breves/technologie/10001-article/arnaque-au-rgpd-mefiez-vous-de-france-rgpd-org

Double authentification

Exemple avec le DMP : identifiant / mot de passe + envoi d'un SMS ou mail pour authentification forte : 2 facteurs pour une authentification forte

AUTHY

https://authy.com/

A privilégier aussi dans l'environnement personnel

Le couple identifiant / mot de passe n'est pas suffisant en terme de sécurité, le risque de piratage est important.

Solutions alternatives :

- ✓ Dashline : https://www.dashlane.com/
- ✓ Fichier Excel avec chiffrement, voir le détail dans les pages suivantes

II. Messagerie

Attention aux Hameçonnages ou Phishing

Ne jamais ouvrir les pièces jointes avec extensions :
.pif, .bat, .com, .exe, .lnk…

Ne jamais cliquer sur un lien dans un email
vous demandant de vous identifier

Survoler le lien avec la souris, sans cliquer,
juste pour vérifier l'adresse Web

LE PHISHING

Les bonnes pratiques

- Restez vigilant
- Vérifiez l'adresse mail et le nom de l'expéditeur sont cohérents entre eux
- Evitez de cliquer sur des liens contenus dans des mails
- Si vous cliquez sur le lien, vérifiez la cohérence entre l'adresse web officielle et officieuse du site
- Méfiez-vous de mails d'expéditeurs inconnus
- Evitez de cliquer sur les pièces jointes contenues dans les mails d'expéditeurs inconnus

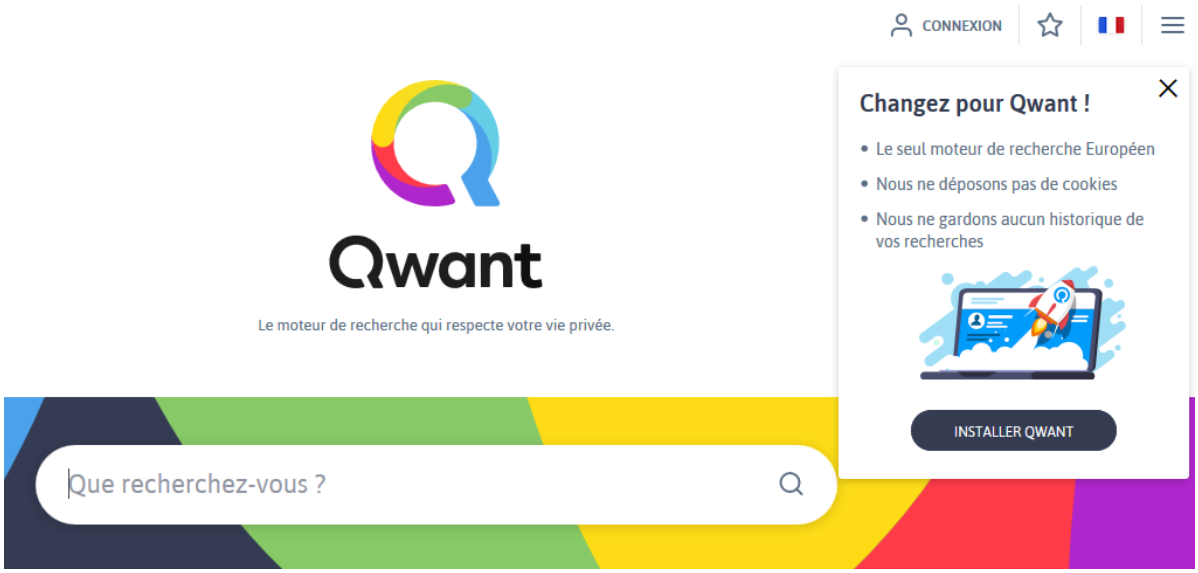
III. Internet

La protection de vos données commence par le bon navigateur Internet avec le bon moteur de recherche et de la vigilance avec quelques bons reflexes

Navigateur : utiliser Firefox et changer le moteur de recherche par défaut qui est ~~Google~~

Source : prism-break.org contre la NSA, contre l'écoute de masse

Moteurs de recherche respectant la protection des données :
https://www.qwant.com/



https://www.startpage.com/ avec les résultats de ~~Google~~ en anonyme

D'autres solutions valides, sécurisées et pour de bonnes actions :

- ✓ https://www.lilo.org/fr/
- ✓ https://www.ecosia.org/?c=fr

- ✓ Attention aux solutions gratuites
- ✓ **Sinon le produit, c'est VOUS !**
- ✓ Logiciel à prendre sur les sites des éditeurs
- ✓ **HTTPS (le S pour Sécurisé) et/ou le cadenas**
- ✓ Vérifier l'adresse des sites
- ✓ **Vigilance avec les Cookies**
- ✓ Consulter les Mentions légales ou CGU/CGV
- ✓ **Lire les protections sur les données**

IV. Réseaux

Attention aux Wifi gratuits et Hotspot
Privilégier le réseau de l'établissement ou la 4G
Vigilance sur les solutions collaboratives en ligne :
Utiliser les outils institutionnels :

- ✓ Partages bureautiques
- ✓ Sharepoint pour partager des documents en interne et sur le GHT
- ✓ Doodle hébergé en Suisse
- ✓ EventBride au Pays Bas et USA, restez vigilant
- ✓ Sinon des solutions payantes : Sarbacane, à étudier au cas par cas, consulter l'équipe conformité et sécurité numérique, la DSN : services numériques

Attention aux réseaux sociaux
Le RGPD s'attaque aux GAFAM : Google, Amazon, Facebook, Apple et même Microsoft
Et la suite : Twitter, LinkedIn, Instagram, Snapshat, … qui ne respectent pas la protection de vos données personnelles

PRUDENCE SUR LES RÉSEAUX SOCIAUX ET INTERNET

Les bonnes pratiques

- Choisissez un **mot de passe fort**
- **Evitez de donner trop de détails** sur votre vie autant professionnelle que personnelle
- Définissez vos paramètres de confidentialité pour **limiter l'accès à votre compte**
- Gardez à l'esprit **qu'Internet est une place publique**
- **Vérifiez** régulièrement ce qu'Internet dit de vous
- Si vous constatez que des informations nuisibles à votre entreprise circulent sur Internet, **prévenez** le support informatique

V. Matériel informatique

Faire les mises à jour, attention aux fausses mises à jour

Effectuer des sauvegardes régulières

Clé USB, disque dur externe, carte mémoire
Ne pas brancher une clé USB inconnue
Si c'est votre matériel, pensez à les chiffrer par défaut, voir le chapitre suivant

Smartphones, tablettes : ce sont des ordinateurs
Il faut aussi les mettre à jour
Conserver votre IMEI, référence matériel en cas de vol
Taper *#06# pour récupérer ce numéro

IOT (objets connectés), équipements biomédicaux
Faire des audits de sécurité et vulnérabilité
https://www.av-test.org/fr/internet-of-things/

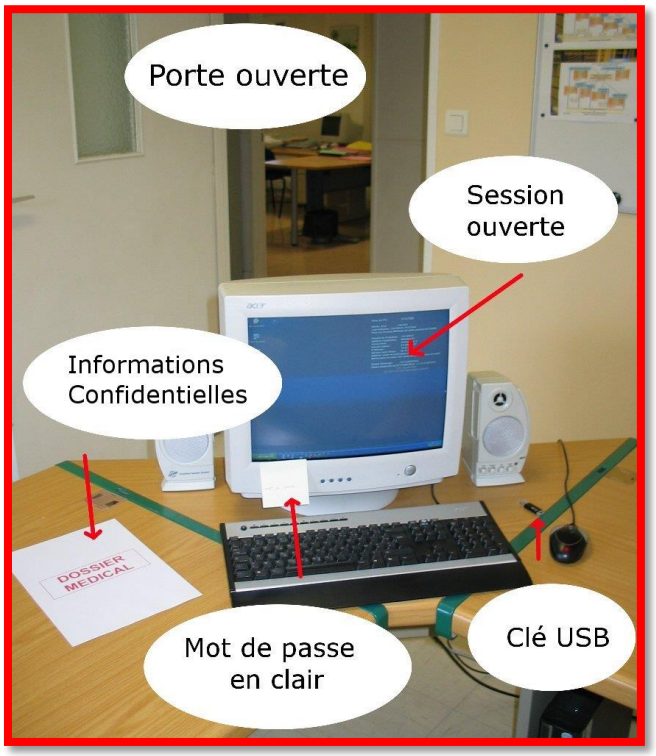
Vérifier les contrats et clauses avec les prestataires

Changer les mots de passe par défaut

VOTRE ENVIRONNEMENT DE TRAVAIL

- **Les bonnes pratiques**
  - Ne partagez pas vos mots de passe
  - Verrouillez votre session lors de toute absence
  - Bureau propre : rangez les documents dans un lieu fermé à clé (caisson, armoire)
  - Récupérez immédiatement vos impressions confidentielles aux imprimantes
  - Utilisez les poubelles sécurisées pour jeter les documents sensibles (ex : réponse à Appel d'Offre)
  - Utilisez les partages réseaux avec des droits restreints pour échanger des fichiers confidentiels
  - Chiffrer les fichiers confidentiels lors d'envois par mail
  - Si vous possédez un PC portable, attachez-le à votre bureau avec un câble en acier
  - En cas de doute sur vos équipements, faîtes-les analyser et ne les connectez pas au réseau

Ce qu'il ne faut pas faire



Dès que je quitte mon poste, je verrouille manuellement ma session au moyen de la commande Windows + L

VI. Chiffrement des données sur tous les supports

Dans le monde de la Santé et pour les professionnels : MSSanté et ApiCrypt

Pour tous les autres cas : 7-Zip, VeraCrypt, Bitlocker

Fichiers **Clés USB** **Intégré à Windows 10**

https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires

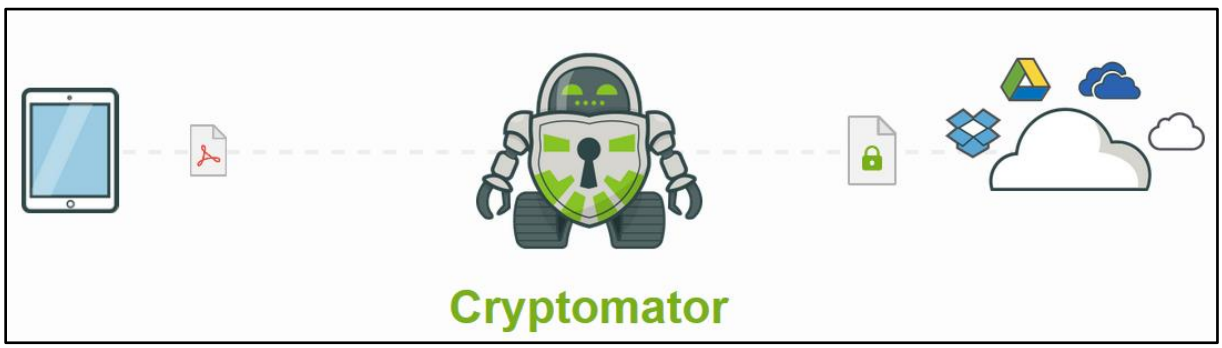
Sous Mac OS :
https://macquebec.com/techniques-de-cryptage-de-donnees-avec-os-x/

Autres solutions :

https://fr.wikipedia.org/wiki/AxCrypt

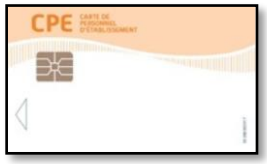
https://cryptomator.org/

Dans le nuage, Cloud



VII. A distance, en déplacement

Télétravail



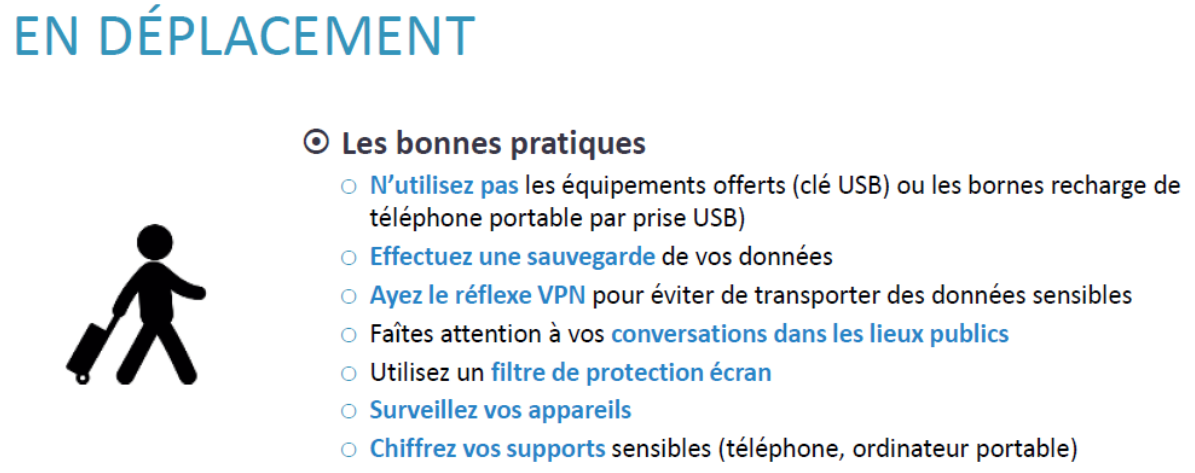
Avec VPN et CPE / CPS

Ordinateur chiffré Windows 10 avec connexion sécurisée à l'établissement

Nomadisme

Attention aux vols ou pertes
A signaler à votre hiérarchie et aux autorités

Vous avez un smartphone, une tablette, un ordinateur ? Alors vous êtes concerné par les cyber-risques, pas besoin d'être un geek ! Vol d'informations professionnelles et personnelles, de données bancaires, piratage de vos comptes sur les réseaux sociaux, usurpation d'identité... ça peut faire mal !
(Extrait de TutosRisques sur le cyber)



VIII. Droits et devoirs

Prendre en compte les nouveaux droits du RGPD :

- ✓ **Information**
- ✓ **Opposition**
- ✓ **Accès**
- ✓ **Rectification**
- ✓ **Effacement**
- ✓ **Déréférencement**
- ✓ **Portabilité**
- ✓ **Intervention humaine**
- ✓ **Limitation du traitement**

Vigilance avec la recherche DRCI (Direction Recherche Clinique et Innovation)
Notes d'information et gestion du consentement
Vérifier la partie anonymisation et le chiffrement

Inventaire des logiciels et fichiers auprès du Référent Informatique et Libertés de chaque service et dans le GHT qui remettra à l'équipe conformité, au DPO

Mentions légales à mettre à jour dans tous les traitements (modèles sur la CNIL)
Mettre à jour les conventions et marchés avec les avenants RGPD

Intégrer les clauses RGPD dans les chartes, politique sécurité, clauses de confidentialité et règlement intérieur

Importance d'une bonne gouvernance pour la mise en œuvre réussie du RGPD :

- ✓ Commissions Habilitation et Sécurité
- ✓ Commissions Projets Informatiques
- ✓ RGPD et Sécurité Numérique
- ✓ Tenue du dossier patient
- ✓ Identito Vigilance
- ✓ Qualité sur le SI

IX. En cas de problème, d'incident ou de violation de données

Contacter votre hiérarchie,
le support informatique,
le RIL,
le RSSI
ou
le DPO.

En cas de virus sur votre ordinateur, débrancher le du réseau ou arrêter le.

Pensez aux modes dégradés pour anticiper les incidents

PDF

Téléphone

Fax

Papier

Incident
Tout incident grave sur le SI ou pour la continuité des soins doit être signalé par la qualité et/ou le DPO, RSSI, RIL
https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/choixSignalementPS

Violation
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Points de vigilance, contrôles de la CNIL : Vidéo protection, badges, RH, recherche
60 % des plaintes

X. Bonnes pratiques et aller plus loin

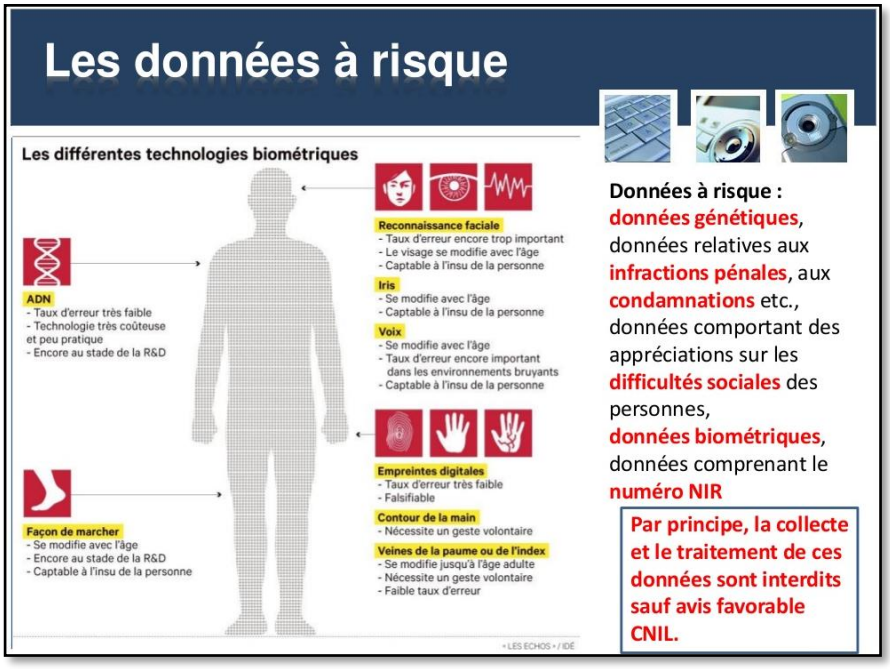
Privacy by Design et Security by Desgin : la protection et la sécurité dès le début des projets, choix de nouvelles applications
Registre des traitements avec le modèle dans la GED ou sur le site de la CNIL
https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

Nouveau traitement, application : toute gestion de données personnelles doit faire l'objet d'une déclaration auprès du DPO et saisie dans le registre PrivaCIL

Les données sensibles sont celles qui font apparaître, directement ou indirectement, les **origines raciales** ou **ethniques**, les **opinions politiques**, **philosophiques** ou **religieuses** ou l'**appartenance syndicale** des personnes, ou sont relatives à la **santé** ou à la **vie sexuelle** de celles-ci.

Par principe, la collecte et le traitement de ces données sont interdits sauf autorisation CNIL.

Ne pas oublier la sécurité, la transparence, l'inventaire des prestataires et sous-traitants.
Dans le cas des données sensibles ou à risques, vous devez vous rapprocher du DPO, il faut peut-être faire une demande d'autorisation à la CNIL



Analyse de risque et évaluation du niveau de protection des données
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Les traitements qui remplissent au moins **deux des critères suivants** doivent faire l'objet d'une analyse d'impact (AIPD) ou PIA :

- évaluation/*scoring* (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, *etc.*) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

Sensibilisation
Référents informatique et liberté et en lien avec la qualité et l'identito vigilance

Vigilance sur les nouveaux risques :

- ✓ **objets connectés (IOT)**
- ✓ **intelligence artificielle**
- ✓ **BigData**

Mémo

Fiche		Mesure	
1	Analyser les risques	**Recensez** les fichiers et données à caractère personnel et les traitements	❑
		Déterminez les menaces et leurs impacts sur la vie privée des personnes	❑
		Mettez en œuvre des **mesures de sécurité adaptées** aux menaces	❑
2	Authentifier les utilisateurs	Définissez un identifiant ***(login)*** unique à chaque utilisateur	❑
		Adoptez une **politique de mot de passe utilisateur rigoureuse**	❑
		Obligez l'utilisateur à **changer son mot de passe après réinitialisation**	❑
3	Gérer les habilitations & sensibiliser les utilisateurs	**Définissez des profils d'habilitation**	❑
		Supprimez les permissions d'accès obsolètes	❑
		Documentez les procédures d'exploitation	❑
		Rédigez une **charte informatique** et annexez-la au **règlement intérieur**	❑
4	Sécuriser les postes de travail	**Limitez le nombre de tentatives d'accès** à un compte	❑
		Installez un «**pare-feu**» *(firewall)* logiciel	❑
		Utilisez des **antivirus régulièrement mis à jour**	❑
		Prévoyez une procédure de **verrouillage automatique de session**	❑
5	Sécuriser l'informatique mobile	Prévoyez des **moyens de chiffrement** pour les **ordinateurs portables** et les unités de stockage amovibles (**clés USB**, CD, DVD…)	❑
6	Sauvegarder et prévoir la continuité d'activité	Effectuez des **sauvegardes régulières**	❑
		Stockez les supports de sauvegarde dans un endroit sûr	❑
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	❑
		Prévoyez et testez régulièrement la **continuité d'activité**	❑
7	Encadrer la maintenance	**Enregistrez les interventions** de maintenance dans une **main courante**	❑
		Effacez les données de tout matériel avant sa **mise au rebut**	❑
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	❑

Fiche		Mesure	
8	Tracer les accès et gérer les incidents	Prévoyez un **système de journalisation**	❑
		Informez les utilisateurs de la mise en place du système de journalisation	❑
		Protégez les équipements de journalisation et les informations journalisées	❑
		Notifiez les personnes concernées des accès frauduleux à leurs données	❑
9	Protéger les locaux	**Restreignez les accès** aux locaux au moyen de **portes verrouillées**	❑
		Installez des **alarmes anti-intrusion** et vérifiez-les périodiquement	❑
10	Protéger le réseau informatique interne	**Limitez les flux réseau au strict nécessaire**	❑
		Sécurisez les accès distants des appareils informatiques nomades par **VPN**	❑
		Utilisez le protocole SSL avec une clé de 128 bits pour les **services web**	❑
		Mettez en œuvre le protocole WPA - AES/CCMP pour les réseaux WiFi	❑
11	Sécuriser les serveurs et les applications	Adoptez une **politique de mot de passe administrateur rigoureuse**	❑
		Installez sans délai les **mises à jour critiques**	❑
		Assurez une **disponibilité** des données	❑
12	Gérer la sous-traitance	Prévoyez une **clause spécifique** dans les contrats des sous-traitants	❑
		Assurez-vous de l'**effectivité des garanties** prévues (audits de sécurité, visites...)	❑
		Prévoyez les **conditions de restitution** et de destruction des données	❑
13	Archiver	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	❑
		Détruisez les archives obsolètes de manière sécurisée	❑
14	Sécuriser les échanges avec d'autres organismes	**Chiffrez** les données avant leur envoi	❑
		Assurez-vous qu'il s'agit du **bon destinataire**	❑
		Transmettez le **secret** lors d'un envoi distinct et via un canal différent	❑

Pour aller plus loin :

Cyberveille sante	https://www.cyberveille-sante.gouv.fr/
Kit de sensibilisation	https://www.cybermalveillance.gouv.fr/
Hack academy	https://www.hack-academy.fr/home
Prism Break	https://prism-break.org/fr/all/
ANSSI	http://www.ssi.gouv.fr/
SecNumacadémie	https://secnumacademie.gouv.fr/
CNIL	https://www.cnil.fr/professionnel
Medef	https://rgpd.medef.com/

https://www.medef.com/fr/content/guide-pratique-sur-la-protection-des-donnees-personnelles

Gouvernement https://www.gouvernement.fr/risques/tutos-risques#risquescyber

Lexique :

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

CGU / CGV : Conditions Générales d'Utilisation ou de Vente

CNIL : Commission Nationale Informatique et Libertés

CPE / CPS : Carte ou badge de Personnel d'Etablissement ou Professionnel de Santé

DPO / DPD : Délégué à la Protection des Données personnelles dpo@chu-amiens.fr

GED : Gestion Electronique de Document

GHT : Groupement Hospitalier de Territoire

Hotspot : point d'accès sans fil

IMEI : numéro permettant d'identifier de manière unique un appareil mobile

RGPD : Règlement Européen Général de Protection des Données

RIL : Référent Informatique et Libertés

RSSI : Responsable de la Sécurité des Systèmes d'Information

VPN : Réseau Privé Virtuel, réseau chiffré sur Internet

Wifi : Réseau sans fil