Recommandations pour la direction de l'hôpital

Règlement Général de la Protection des Données

1. Principes de base

Le RGPD est un règlement européen daté de 2016 (UE 2016/679) qui définit les droits des citoyens et devoir des organisations en matière de données personnelles. En droit français, il prime sur la loi comme le précise les Articles 55 et 88-1 de la constitution de 1958, c'est-à-dire qu'il est au dessus des lois nationales ne peuvent en théorie le contredire. Le RGPD dispose de six grands principes que voici :

- Ne collecter que les données vraiment nécessaires pour atteindre votre objectif
- Soyez transparent
- Organisez et faciliter l'exercice des droits des personnes
- Fixez les durées de conservation
- Sécurisez les données et identifiez les risques
- Inscrivez la mise en conformité dans une démarche continue

Par principe, le traitement des données santé est interdit sauf dans des cas particuliers. Elles peuvent toutefois être traitées dans certaines conditions prévues par le RGPD dans son Article 9 Alinéa 2 ou bien des dispositions prévues par la loi, notamment l'article 44 de la Loi Informatique et Libertés en France. Le RGPD pose le cadre légal permettant la récolte des données légitimes où nécessaire au bon fonctionnement d'une organisation tout en permettant aux citoyens de garder la main et la possession de leurs données, les articles majeurs du RGPD concernant les procédures et cas de légalité de la récolte sont décrits et énumérés dans les articles.

RGPD UE2016/679 :

Article 6
Licéité du traitement

Un traitement de données n'est légal que s'il repose sur l'une des bases prévues par le RGPD. C'est-à-dire le consentement de la personne, l'exécution d'un contrat ou de mesures précontractuelles, le respect d'une obligation légale, la sauvegarde d'intérêts vitaux, l'exécution d'une mission d'intérêt public ou de l'autorité publique, ou encore l'intérêt légitime du responsable du traitement. Sous réserve de ne pas porter atteinte aux droits et libertés de la personne concernée.

Article 7
Conditions applicables au consentement

Le responsable du traitement doit pouvoir prouver que la personne a donné son consentement. Celui-ci doit être clair, distinct d'autres informations, formulé en termes simples et accessibles. La personne peut retirer son consentement à tout moment, aussi facilement qu'elle l'a donné, sans que cela remette en cause la légalité du traitement déjà effectué. Enfin, le consentement n'est valable que s'il est donné librement, sans être imposé comme condition à l'exécution d'un contrat ou à la fourniture d'un service lorsqu'il n'est pas nécessaire.

Article 9
Traitement des données sensibles

Le traitement de données personnelles sensibles, telles que les données de santé, génétiques, biométriques, les opinions politiques, convictions religieuses ou philosophiques, l'appartenance syndicale ou la vie sexuelle, est interdit par principe. Il peut toutefois être autorisé dans certains cas, si la personne concernée a donné son consentement explicite, si le traitement est nécessaire pour respecter une obligation légale, pour l'exécution d'une mission d'intérêt public, pour la sauvegarde des intérêts vitaux, pour la médecine préventive, les soins, la gestion des systèmes de santé ou encore pour la recherche scientifique, historique ou statistique, sous réserve des conditions prévues par le RGPD.

Loi n°78-17 Informatique et Libertés, 6 janvier 1978 :

Article 44
Traitement des données sensibles

L'article 44 précise que l'article 6 du RGPD (licéité du traitement) ne s'applique pas lorsque l'une des conditions du 2 de l'Article 9 du RGPD sont remplies. Cela concerne notamment : les traitements nécessaires à la médecine préventive, aux diagnostics médicaux, aux soins, ou à la gestion de services de santé par des professionnels soumis au secret médical, les traitements statistiques réalisés par les services statistiques officiels les traitements de données de santé justifiés par l'intérêt public, les traitements biométriques strictement nécessaires au contrôle d'accès dans les entreprises et administrations, la réutilisation d'informations publiques sans possibilité de réidentifier les personnes, et les traitements nécessaires à la recherche publique d'intérêt public, après avis de la CNIL.

Sources :

RGPD UE 2016/679 ¬

CNIL, « Le règlement général sur la protection des données - RGPD »
Wikipédia, « Règlement général sur la protection des données »
Parlement Européen, « Règlement - 2016/679 - FR - rgdp - EUR-Lex »

Constitution du 4 octobre 1958 de la cinquième République Française ¬

Légifrance, « Article 88-1 - Constitution du 4 octobre 1958 - Légifrance »
Légifrance, « Article 55 - Constitution du 4 octobre 1958 - Légifrance »

Loi Informatique et Libertés de 1978 ¬

Légifrance, « Article 44 - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - Légifrance »

Propositions techniques (sécurité des données & du réseau)

1. Sécurisation des données (au repos & en transit)

- Chiffrement au repos des bases et des sauvegardes (chiffrement disque/volume sur les serveurs et NAS de sauvegarde ; clés gérées dans un HSM/KMS interne, rotation semestrielle).
- Chiffrement en transit systématique (TLS 1.2+ avec HSTS) pour l'applicatif interne, les exports et les échanges avec les organismes externes (API/mTLS ou SFTP chiffré).
- Contrôle d'accès fort (RBAC + MFA) : rôles alignés sur les fonctions (ex. *Médecin*, *Chef de service*, *ARC/Data manager*, *DPO*), authentification MFA pour tout accès aux données de santé.
- Journalisation inviolable (WORM/immutabilité) des consultations, insertions, exports et suppressions ; conservation conforme (au moins 12 mois en prod, plus long si exigence légale interne).
- Pseudonymisation/anonymisation pour la recherche : séparation stricte entre données identifiantes (Patients…) et données d'étude ; l'ID patient réel n'est jamais transmis hors clinique, on expose un identifiant d'étude dérivé. Ceci se fonde sur la présence d'Études, Inclusions et d'un Organisme centralisateur dans le modèle.
- DLP (Data Loss Prevention) : blocage des exports non autorisés, filigrane et traçage des fichiers sortants, interdiction des supports USB non approuvés.
- Cycle de vie & minimisation : purges planifiées des jeux d'étude arrivés en fin d'utilité ; masquage/cryptage des colonnes les plus sensibles (nom, prénom, date de naissance, n° dossier).

2. Sécurisation réseau

- Segmentation en VLAN/segments :
  - *Bloc clinique/soins* (SIH, imagerie, labo),
  - *IoMT* (dispositifs médicaux) isolé,
  - *Bureautique/administratif*,
  - *Invités*,
  - *Zone DMZ* (accès externes, API vers organismes). Pare-feu inter-VLAN avec règles de moindre privilège.
- NAC 802.1X (postes & équipements), inventaire et profilage des dispositifs médicaux ; Wi-Fi WPA2-Enterprise/WPA3-Enterprise avec VLAN attribué par rôle.
- IDS/IPS (sur la DMZ et le cœur), pare-feu applicatif (WAF) pour les applis web, VPN pour l'accès distant (MFA obligatoire).
- DNS filtrant + Egress filtering (sortants), listes d'autorisation pour destinations partenaires (organismes).

3. Sécurité applicative & base de données (alignée sur l'annexe)

En regard du schéma fourni (Patients, Maladies, Études, Inclusions, Organes, Stades, Médecins, etc.), mettre en place :

- RBAC en base : rôles SQL par profil (ex. *medecin_r*, *arc_rw*, *chef_service_r*, *dpo_audit*) ; pas d'accès direct "*superuser*" en routine.
- Vues sécurisées & masquage :
  - Vues cliniques (soins) : accès nominatif autorisé.
  - Vues recherche : colonnes identifiantes masquées (nom, prénom, dateNaisPat) et remplacement par un id pseudonymisé dans Inclusions/Études.
- Contraintes & intégrité (en plus de celles déjà listées) : triggers d'audit (qui/quoi/quand), refus d'UPDATE sur identifiants patients hors procédure dédiée, contrôle de l'index unique (existant) pour éviter doublons *patient-maladie* et *patient-étude*.
- Validation applicative contre l'OWASP Top 10, revue de code obligatoire, tests d'intrusion annuels.

4. Sauvegardes, PRA/PCA

- Sauvegardes 3-2-1 (copie locale + copie hors site + copie immuable), tests de restauration trimestriels, PRA avec objectifs RTO/RPO définis (ex. RTO 4 h / RPO 1 h pour SI critique).
- PCA : plan de continuité pour activités cliniques critiques (accès en lecture seule dégradé si l'app principal est indisponible).

5. Gouvernance, procédures & sensibilisation

- PSSI (Politique de Sécurité du SI) approuvée par la direction ; registre des traitements ; DPA/clauses contractuelles pour tout prestataire manipulant les données d'étude.
- Gestion des incidents : playbooks (ransomware, fuite, indisponibilité), chaîne d'alerte, exercices semestriels.
- Sensibilisation continue (phishing simulé, e-learning RGPD, bonnes pratiques).

6. Spécifiques "Études/Organismes"

- Création d'un data mart de recherche séparé, alimenté par ETL : seules les données minimales utiles à l'étude y sont chargées, pseudonymisées ; les flux sortants vers l'Organisme passent par la DMZ et sont chiffrés et journalisés. Ce point répond à la logique d'Études/Inclusions/Organismes décrite dans l'annexe.

Plan de mise en œuvre (synthèse)

- 0–30 jours : segmentation réseau & durcissement accès (MFA, NAC), chiffrement TLS, PSSI & registre, rôles applicatifs initiaux.
- 30–60 jours : vues masquées/pseudonymisation, DLP, SIEM/logs WORM, sauvegardes immuables, WAF/IDS-IPS.
- 60–90 jours : PRA/PCA testé, tests d'intrusion, data mart recherche & flux sécurisés vers organismes, formation continue.

Ces propositions couvrent les volets "sécurité des données" et "sécurité du réseau" demandés par la question 3 du document, tout en tenant compte du modèle de données fourni en annexe (patients, études, inclusions, organismes, etc.).