Sélection de requis

1. Protection des Données Personnelles (RGPD & LOPDGDD)

ID: PRIV-001

Titre : Obtention du consentement explicite
Description : Selon l'**article 6 du RGPD**, les patients doivent donner un consentement explicite avant tout traitement de leurs données médicales. Le consentement doit être **libre, spécifique, informé et révocable**.
Critères d'acceptation :

- Interface permettant aux patients de donner ou retirer leur consentement.
- Enregistrement des horodatages des consentements.
- Fourniture d'informations claires sur l'usage des données.
  Priorité : Haute
  Catégorie : Protection des données
  Source : RGPD, Art. 6
  Justification : Garantit la conformité légale et assure le respect des droits des patients sur leurs données personnelles.

ID: PRIV-002

Titre : Droit d'accès et de rectification des données
Description : Conformément aux **articles 15 et 16 du RGPD**, la plateforme doit permettre aux patients d'accéder à leurs informations de santé et de demander leur correction si elles sont inexactes.
Critères d'acceptation :

- Tableau de bord permettant aux patients d'afficher leurs données médicales.
- Fonctionnalité de demande de modification pour les informations incorrectes.
- Suivi et journalisation des modifications effectuées.
  Priorité : Haute
  Catégorie : Droits des utilisateurs
  Source : RGPD, Art. 15 et 16
  Justification : Assure la transparence et l'exactitude des informations médicales conformément à la législation.

ID: PRIV-003

Titre : Droit à l'oubli et suppression des données
Description : En vertu de **l'article 17 du RGPD**, les patients doivent pouvoir demander la suppression de leurs données personnelles lorsque celles-ci ne sont plus nécessaires ou

en cas de retrait du consentement.
Critères d'acceptation :

- Option accessible via le compte patient pour demander la suppression des données.
- Vérification de l'impact avant suppression définitive.
- Suppression des données dans un délai conforme aux obligations légales.
  Priorité : Haute
  Catégorie : Protection des données
  Source : RGPD, Art. 17
  Justification : Conformité aux exigences de protection des données et garantie de la confidentialité des patients.

---

2. Sécurité de l'Information (ISO 27001 & ENS)

ID: SEC-001

Titre : Chiffrement des données en transit et au repos
Description : Toutes les données médicales doivent être chiffrées en conformité avec **l'ISO 27001 et l'ENS** afin de garantir leur **confidentialité et intégrité**.
Critères d'acceptation :

- Chiffrement AES-256 des données stockées.
- Utilisation de TLS 1.2 ou supérieur pour les transmissions.
- Gestion centralisée des clés de chiffrement avec rotation périodique.
  Priorité : Haute
  Catégorie : Sécurité de l'information
  Source : ISO 27001, ENS, RGPD Art. 32
  Justification : Évite les violations de données et protège les informations sensibles.

ID: SEC-002

Titre : Authentification multi-facteurs (MFA)
Description : L'accès des **médecins, administrateurs et patients** doit être sécurisé via une **authentification multi-facteurs** pour prévenir les accès non autorisés.
Critères d'acceptation :

- Authentification à deux facteurs (TOTP, SMS ou application dédiée).
- Obligation du MFA pour les comptes à privilèges (administrateurs et médecins).
- Système de récupération sécurisé en cas de perte de facteur d'authentification.
  Priorité : Haute

Catégorie : Contrôle d'accès
Source : ISO 27001, ENS, RGPD Art. 32
Justification : Renforce la protection des comptes et réduit le risque d'intrusion.

ID: SEC-003

Titre : Journalisation et audit des accès
Description : Tous les accès et modifications des **dossiers médicaux** doivent être **journalisés** pour garantir la **traçabilité et détecter les accès suspects**.
Critères d'acceptation :

- Enregistrement des connexions, accès aux fichiers et modifications.
- Conservation des logs pendant **au moins 2 ans**.
- Détection et notification des accès non autorisés.
  Priorité : Haute
  Catégorie : Audit et conformité
  Source : ISO 27001, ENS, RGPD Art. 30
  Justification : Répond aux exigences de **traçabilité** et assure la **responsabilité des utilisateurs**.

---

3. Interopérabilité et Disponibilité

ID: INT-001

Titre : API standardisée pour intégration avec d'autres systèmes
Description : La plateforme doit disposer d'une **API RESTful** conforme aux **standards HL7 FHIR** pour assurer **l'échange de données médicales** avec d'autres systèmes de santé.
Critères d'acceptation :

- API documentée et sécurisée avec OAuth 2.0.
- Compatibilité avec **HL7 FHIR** pour interopérabilité avec autres hôpitaux.
- Contrôles stricts sur les accès et transactions.
  Priorité : Élevée
  Catégorie : Interopérabilité
  Source : IEEE 29148, RGPD Art. 20 (portabilité des données)
  Justification : Facilite l'échange sécurisé des dossiers médicaux.

ID: DISP-001

Titre : Haute disponibilité et récupération après sinistre
Description : Le système doit être conçu pour **minimiser les interruptions** et assurer la

récupération en cas de panne.
Critères d'acceptation :

- Architecture cloud avec redondance multi-zone.
- Mécanismes de sauvegarde **automatisés et chiffrés** toutes les 24h.
- Plan de reprise après sinistre (PRA) testé régulièrement.
  Priorité : Élevée
  Catégorie : Disponibilité
  Source : ISO 27001, ENS
  Justification : Essentiel pour garantir la continuité des soins et prévenir la perte de données.