Selección de Requisitos para la Plataforma SaaS

1. Requisitos de Privacidad y Protección de Datos

PRIV-001 - Obtención de Consentimiento Explícito
Descripción: Antes de procesar datos personales de los pacientes, se debe obtener su consentimiento explícito de manera libre, informada, específica e inequívoca.
Criterios de Aceptación:
- Implementación de una casilla de verificación no pre-marcada.
- Registro de la fecha y hora del consentimiento.
Prioridad: Alta
Categoría: Consentimiento del Usuario
Fuente: RGPD, Art. 6

PRIV-002 - Retiro del Consentimiento
Descripción: Los pacientes deben poder retirar su consentimiento en cualquier momento con la misma facilidad con la que lo otorgaron.
Criterios de Aceptación:
- Implementación de una opción de revocación en la misma interfaz donde se otorgó.
- Eliminación o cese del tratamiento de datos tras el retiro del consentimiento.
Prioridad: Alta
Categoría: Consentimiento del Usuario
Fuente: RGPD, Art. 7

PRIV-003 - Derecho de Acceso
Descripción: Los pacientes deben poder acceder a su historial médico digital y recibir una copia en un formato estructurado y claro.
Criterios de Aceptación:
- Provisión de una interfaz accesible para solicitar datos.
- Garantía de entrega dentro del plazo máximo estipulado (30 días).
Prioridad: Alta
Categoría: Derechos de los Usuarios

Fuente: RGPD, Art. 15

PRIV-004 - Derecho de Rectificación
Descripción: Los pacientes pueden solicitar la corrección de información inexacta en su historial médico.
Criterios de Aceptación:
- Implementación de un mecanismo para modificación de datos personales con registro de cambios.
- Confirmación de la aplicación de los cambios en un plazo máximo de 30 días.
Prioridad: Alta
Categoría: Derechos de los Usuarios
Fuente: RGPD, Art. 16

PRIV-005 - Principio de Minimización
Descripción: Solo deben recopilarse los datos estrictamente necesarios para la finalidad médica establecida.
Criterios de Aceptación:
- Controles para evitar la recolección de datos innecesarios.
- Eliminación automática de datos no esenciales.
Prioridad: Media
Categoría: Minimización y Retención de Datos
Fuente: RGPD, Art. 5.1(c)

PRIV-008 - Evaluaciones de Impacto en la Privacidad (EIPD)
Descripción: Se deben realizar evaluaciones de impacto en la privacidad para identificar y mitigar riesgos en tratamientos de datos de alto riesgo.
Criterios de Aceptación:
- Realización de la EIPD antes de iniciar el tratamiento.
- Implementación de medidas correctivas si se identifican riesgos significativos.
Prioridad: Alta
Categoría: Responsabilidades del Responsable y Encargado del Tratamiento
Fuente: RGPD, Art. 35

2. Requisitos de Seguridad de la Información

SEG-001 - Cifrado de Datos en Reposo y en Tránsito

Descripción: Los datos médicos y personales deben ser cifrados con estándares robustos para evitar accesos no autorizados.

Criterios de Aceptación:

- Uso de cifrado AES-256 o equivalente.
- Implementación de cifrado de extremo a extremo en comunicaciones.

Prioridad: Alta

Categoría: Seguridad de la Información

Fuente: RGPD, Art. 32, ISO 27001

SEG-002 - Control de Acceso Basado en Roles

Descripción: Se deben establecer roles y permisos diferenciados para médicos, administrativos y pacientes con acceso restringido a la información según necesidad.

Criterios de Aceptación:

- Definición de perfiles de acceso para cada tipo de usuario.
- Implementación de doble factor de autenticación para médicos y administradores.

Prioridad: Alta

Categoría: Seguridad de la Información

Fuente: ENS, ISO 27001

SEG-003 - Registro de Actividad y Auditoría

Descripción: Todo acceso y modificación de datos debe ser registrado en un log de auditoría para garantizar la trazabilidad de la información.

Criterios de Aceptación:

- Registro de usuario, fecha, acción y datos modificados.
- Disponibilidad de auditoría para inspecciones de seguridad.

Prioridad: Alta

Categoría: Seguridad de la Información

Fuente: ENS, ISO 27001

SEG-004 - Protección contra Ciberataques

Descripción: Implementación de medidas de seguridad para prevenir ataques de malware, phishing

y accesos no autorizados.
Criterios de Aceptación:
- Firewalls perimetrales y segmentación de red.
- Detección y respuesta ante incidentes de seguridad (SIEM).
Prioridad: Alta
Categoría: Seguridad de la Información
Fuente: ENS, ISO 27001

3. Requisitos de Interoperabilidad y Disponibilidad

INT-001 - Interoperabilidad con Sistemas Hospitalarios
Descripción: La plataforma debe integrarse con sistemas de información hospitalaria (HIS) y bases de datos médicas.
Criterios de Aceptación:
- Implementación de API RESTful para comunicación con terceros.
- Soporte para estándares HL7 y FHIR.
Prioridad: Alta
Categoría: Interoperabilidad
Fuente: ENS, ISO 27001

INT-002 - Respaldo y Recuperación de Datos
Descripción: Se debe garantizar la continuidad del servicio mediante copias de seguridad automáticas y recuperación ante desastres.
Criterios de Aceptación:
- Backup incremental cada 24 horas y full backup semanal.
- Tiempo máximo de recuperación < 4 horas (RTO).
Prioridad: Alta
Categoría: Disponibilidad
Fuente: ISO 27001

INT-003 - Exportación de Datos en Formatos Estándar
Descripción: Los datos de los pacientes deben ser exportables en formatos interoperables para facilitar la migración entre sistemas.

Criterios de Aceptación:

- Exportación en JSON y XML bajo estándar FHIR.

- Función de descarga para pacientes y profesionales.

Prioridad: Media

Categoría: Interoperabilidad

Fuente: ENS, ISO 27001