REQUISITOS DE SEGURIDAD, PRIVACIDAD E INTEROPERABILIDAD PARA PLATAFORMA SaaS DE HISTORIAS CLÍNICAS ELECTRÓNICAS

Requisitos de Privacidad y Protección de Datos (CCPA y CPRA)

ID: PRIV-CCPA-001 Título: Derecho de Acceso del Consumidor
Descripción: Los pacientes tienen derecho a solicitar información sobre sus datos personales almacenados en la plataforma, incluyendo su origen, propósito y con quién han sido compartidos en los últimos 12 meses.
Criterios de Aceptación:

- Implementación de un portal de autoservicio para que los pacientes soliciten acceso a su información.
- Plazo de respuesta dentro de los 45 días. **Prioridad:** Alta
  Fuente: CCPA, Sección 1798.110
  Justificación: Asegura que los pacientes tengan visibilidad sobre sus datos médicos y quién accede a ellos, cumpliendo con el derecho de acceso estipulado en el CCPA y CPRA.

ID: PRIV-CCPA-002 Título: Derecho de Eliminación de Datos
Descripción: Los pacientes pueden solicitar la eliminación de sus datos personales, salvo excepciones legales que requieran su retención.
Criterios de Aceptación:

- Mecanismo accesible en la plataforma para solicitar la eliminación de datos.
- Confirmación de eliminación en un plazo de 45 días. **Prioridad:** Alta
  Fuente: CCPA, Sección 1798.105
  Justificación: Garantiza el derecho de los pacientes a la supresión de sus datos personales, excepto en los casos en los que la legislación requiera su conservación.

ID: PRIV-CCPA-003 Título: Transparencia en la Recolección de Datos
Descripción: Se debe informar claramente a los usuarios sobre los datos que se recopilan y su propósito antes de la recolección.
Criterios de Aceptación:

- Política de privacidad accesible en todas las plataformas digitales.
- Notificaciones claras en el momento de la recolección de datos. **Prioridad:** Alta
  Fuente: CPRA, Sección 1798.130
  Justificación: Asegura la transparencia en el procesamiento de datos de los pacientes y facilita la conformidad con las regulaciones de privacidad.

ID: PRIV-CCPA-004 Título: Derecho de Corrección de Datos
Descripción: Los pacientes tienen derecho a solicitar la corrección de sus datos personales si son inexactos.
Criterios de Aceptación:

- Implementación de un proceso para solicitar correcciones.
- Confirmación de la corrección en un plazo de 45 días. **Prioridad:** Alta
  Fuente: CPRA, Sección 1798.106
  Justificación: Asegura la exactitud de la información médica almacenada, reduciendo el riesgo de errores en los registros clínicos.

ID: PRIV-CCPA-005 Título: Evaluación de Terceros
Descripción: Las organizaciones deben asegurarse de que terceros que reciben datos personales cumplen con las obligaciones de privacidad y seguridad.
Criterios de Aceptación:

- Contratos con proveedores que incluyan cláusulas de protección de datos.
- Auditorías periódicas a terceros. **Prioridad:** Alta
  Fuente: CPRA, Sección 1798.140
  Justificación: Protege la información médica cuando es compartida con terceros, asegurando que cumplan con las normativas de privacidad.

ID: PRIV-CCPA-006 Título: Medidas de Seguridad Apropiadas
Descripción: Implementar medidas de seguridad razonables para proteger los datos personales de accesos no autorizados o usos indebidos.
Criterios de Aceptación:

- Uso de cifrado para datos sensibles.
- Monitoreo de accesos y auditorías periódicas. **Prioridad:** Alta
  Fuente: CCPA, Sección 1798.150
  Justificación: Garantiza la confidencialidad e integridad de los datos médicos almacenados en la plataforma.

ID: PRIV-CCPA-007 Título: Registro de Actividad y Detección de Código Malicioso
Descripción: Implementar sistemas de registro de actividad para detectar accesos no autorizados o intentos de manipulación de datos.
Criterios de Aceptación:

- Registro de todas las modificaciones y accesos a datos médicos.
- Implementación de herramientas para detección de código malicioso. **Prioridad:** Alta

Fuente: CPRA, Sección 1798.185
Justificación: Mejora la seguridad del sistema y permite la identificación temprana de posibles amenazas.

ID: PRIV-CCPA-008 Título: Derecho a la Exclusión de la Venta de Datos
Descripción: Los consumidores deben tener la posibilidad de optar por no vender sus datos personales a terceros.
Criterios de Aceptación:

- Implementación de un enlace "Do Not Sell My Personal Information" en la página principal.
- Registro de solicitudes de exclusión y aplicación efectiva. **Prioridad:** Alta
  Fuente: CCPA, Sección 1798.120
  Justificación: Protege la privacidad de los pacientes evitando que sus datos sean vendidos sin su consentimiento.

ID: PRIV-CCPA-009 Título: Retención de Datos Mínima Necesaria
Descripción: Los datos personales solo deben conservarse el tiempo necesario para cumplir con el propósito para el cual fueron recopilados.
Criterios de Aceptación:

- Definición de plazos de retención claros y documentados.
- Eliminación automática de datos una vez cumplida su finalidad. **Prioridad:** Media
  Fuente: CPRA, Sección 1798.100
  Justificación: Minimiza el riesgo de exposición de datos innecesarios y mejora la gestión de información médica.

ID: PRIV-CCPA-010 Título: Evaluaciones Periódicas de Cumplimiento
Descripción: Las empresas deben realizar auditorías periódicas para garantizar el cumplimiento del CCPA y CPRA.
Criterios de Aceptación:

- Revisión anual de políticas de privacidad.
- Documentación de auditorías internas. **Prioridad:** Alta
  Fuente: CPRA, Sección 1798.185
  Justificación: Asegura la actualización continua de las políticas de privacidad y su cumplimiento normativo.

ID: PRIV-CCPA-011
Título: Derecho a la Portabilidad de Datos

Descripción: Los pacientes deben tener la capacidad de solicitar una copia de sus datos médicos en un formato estructurado, de uso común y legible por máquina.
Criterios de Aceptación:

- Provisión de una funcionalidad en la plataforma para exportar datos en formatos estándar como JSON, XML o CSV.
- Garantía de que la portabilidad de los datos se complete dentro de los 45 días posteriores a la solicitud del paciente.
  Prioridad: Alta
  Fuente: CCPA, Sección 1798.100(d)
  Justificación: Permite a los pacientes transferir sus datos médicos entre proveedores de salud sin restricciones indebidas.

ID: PRIV-CCPA-012
Título: Protección Contra la Discriminación por Ejercicio de Derechos
Descripción: Se debe garantizar que los pacientes no sean discriminados por ejercer sus derechos de privacidad, incluyendo el derecho de acceso, eliminación y exclusión de venta de datos.
Criterios de Aceptación:

- Se prohíbe denegar servicios o modificar precios a pacientes que ejercen sus derechos de privacidad.
- Implementación de mecanismos internos para prevenir y mitigar la discriminación.
  Prioridad: Alta
  Fuente: CCPA, Sección 1798.125
  Justificación: Garantiza que los pacientes no sean penalizados por ejercer sus derechos de protección de datos.

ID: PRIV-CCPA-013
Título: Notificación de Brechas de Seguridad
Descripción: Se debe notificar a los pacientes en caso de una brecha de seguridad que comprometa sus datos personales.
Criterios de Aceptación:

- Comunicación a los afectados en un plazo no mayor a 72 horas tras la detección de la brecha.
- Inclusión de detalles sobre la naturaleza de la brecha, los datos comprometidos y las acciones correctivas tomadas.
  Prioridad: Alta
  Fuente: CCPA, Sección 1798.150
  Justificación: Refuerza la confianza de los usuarios en la plataforma y asegura el cumplimiento con regulaciones de seguridad de datos.

ID: PRIV-CCPA-014
Título: Consentimiento Explícito para el Uso de Datos Sensibles
Descripción: Antes de recopilar o procesar datos de salud, la plataforma debe obtener el consentimiento explícito del paciente.
Criterios de Aceptación:

- Implementación de mecanismos de aceptación explícita antes de la recopilación de datos médicos.
- Registro del consentimiento con fecha y hora, permitiendo la revocación en cualquier momento.
  Prioridad: Alta
  Fuente: CPRA, Sección 1798.121
  Justificación: Asegura que los pacientes tengan control sobre el uso de su información médica sensible.

ID: PRIV-CCPA-015
Título: Evaluación de Impacto en la Privacidad (PIA)
Descripción: Antes de implementar nuevas funcionalidades o cambios en el sistema, se debe evaluar su impacto en la privacidad de los datos de los pacientes.
Criterios de Aceptación:

- Realización de una evaluación de impacto en la privacidad para cualquier nueva función que implique procesamiento de datos personales.
- Documentación de medidas de mitigación para reducir los riesgos identificados.
  Prioridad: Media
  Fuente: CPRA, Sección 1798.185
  Justificación: Permite anticipar y reducir riesgos relacionados con la privacidad en el desarrollo de nuevas funcionalidades.