CONSIDERACIONES PARA EL SISTEMA INFORMÁTICO PARA EL OTORGAMIENTO PRESTACIONES DE TELECONSULTA Y TELEREHABILITACIÓN

1.- Toda prestación de teleconsulta y telerehabilitación (teleconsulta y telerehabilitación sincrónica) debe ser realizada a través de un software o página web dispuesto especial y exclusivamente para ello, con soporte para acceder a ficha médica electrónica del beneficiario y con la integralidad para emitir receta médica electrónica con firma electrónica avanzada del profesional y un medio de validación electrónica.

2.- El software deberá asegurar que la prestación remota de salud resguarde el ámbito técnico de la prestación.

3.- El software debe velar por tomar todas las medidas de seguridad de la información para que esta interacción directa médico beneficiario se realice de forma segura cuidando la privacidad del beneficiario y mantener resguardado el registro de la ficha.

4.- La institución es responsable que la prestación sea realizada por el profesional seleccionado por el beneficiario personalmente. En caso de alguna modificación de quién realice la prestación esta deberá ser informada al beneficiario quién optará aprobar o rechazar dicho cambio.

5.- El software debe garantizar el correcto uso de la información clínica del beneficiario y mantener el resguardo de ella con aspectos tecnológicos para su resguardo. El acceso a la ficha electrónica del beneficiario debe ser previa validación a través de autentificación de dos factores.

6.- La venta y cobro de la prestación debe ser directo en la plataforma del prestador de teleconsulta y telerehabilitación, ya sea integrándose a FONASA o por medio de alguna de las empresas que tienen este soporte.

7.- El software debe cumplir con lo dispuesto en el anexo técnico adjunto a la presente declaración, elaborado por FONASA.

ANEXO TÉCNICO

El presente apartado tiene la finalidad de establecer los lineamientos técnicos que debe cumplir la empresa solicitante, en adelante el Operador Tecnológico del software de teleconsulta y telerehabilitación en base a las buenas prácticas de desarrollo, calidad y seguridad que permitan asegurar la adecuada entrega del servicio.

Los estándares técnicos y funcionales de la información y seguridad que permitan la funcionalidad de un software de teleconsulta y telerehabilitación deberán aplicarse sin excepción a todas las soluciones presentadas para la prestación del servicio.

Los ámbitos del lineamiento definido en este documento son los siguientes:

- Usabilidad y Accesibilidad
- Seguridad y control
- Aseguramiento de Calidad de servicio del SW
- Pruebas de Seguridad de la información, carga y estrés
- Requerimientos de Auditoria
- Requerimientos técnicos específicos
- Aspectos generales de validación

1. Usabilidad y Accesibilidad

Respecto de los requerimientos y entregables de usabilidad el sistema de teleconsulta y telerehabilitación debe cumplir con:

- Manual de usuario (beneficiario/prestador) para el uso del servicio.
- Guía rápida de uso y resolución de problemas de baja complejidad (por ejemplo, Preguntas Frecuentes).
- Debe contemplar mecanismos de accesibilidad para personas con discapacidad, siguiendo estándares y normas como por ejemplo la WCAG 2.1. Estos mecanismos deberán ser explicitados y entregados en la documentación del software para su verificación.
- Debe contar con una Mesa de Ayuda que permita resolver problemas de usabilidad, operación y accesibilidad del uso de la herramienta.

2. Seguridad y control

En términos generales, los Operadores Tecnológicos que presten servicios de teleconsulta y telerehabilitación deberán contar con políticas, procedimientos y controles dirigidos a resguardar la Seguridad de la Información (confidencialidad, integridad y

disponibilidad) que permitan dar cuenta de una gestión sistemática al respecto. Pueden considerarse los estándares y normas de la serie/familia ISO 27000, en particular ISO 27001/2 e ISO 27799, así como también el Marco de Ciberseguridad del National Institute of Standards and Technologies (NIST).

Para efectos de requerimientos de seguridad específicos definidos en este anexo, se debe cumplir al menos con los siguientes ítems:

- Control de Accesos
  - El sistema debe contar con una matriz de roles con segregación de funciones que asegure que los accesos a distintos niveles y detalles de información estén resguardados.
  - El software debe poseer un control de accesos, al momento de la atención, para que los usuarios puedan acceder válidamente a los recursos de la aplicación. Este control de acceso debe ser ejecutado tanto para el Prestador como para el Beneficiario de la prestación.
  - Para la identificación del beneficiario y prestador, éste lo deberá realizar a través la Clave Única del Estado, lo anterior implica la integración del software con dicho medio de validación de identidad digital o una autenticación de dos factores, sea uno de ellos un registro con clave y otro como código autorización personal enviado a su correo electrónico, mensaje de texto (SMS) al celular u otro medio.

  - Adicional a los puntos anteriores, el aplicativo debe permitir una identificación visual del prestador al momento de la prestación.
  - El sistema debe tener mecanismos de manejo de sesión establecidos que consideren:
    - El identificador de sesión debe ser único, suficientemente largo y aleatorio.
    - Se deben generar (o rotar) los identificadores de sesión durante la autenticación y re-autenticación.
    - Se debe implementar un timeout por inactividad que fuerce la re- autenticación al usuario. La duración de este timeout debe ser inversamente proporcional a la sensibilidad de los datos a proteger, vale decir, mientras más sensible, menor duración.

- Controles de ingreso de datos
  - El software debe tener controles para validar los datos de entrada al sistema de teleconsulta y telerehabilitación, con el fin de asegurar que son correctos y apropiados. Estos controles deben ser aplicados a todo ingreso de transacciones, datos permanentes y tablas de parámetros. Para implementar estos controles se deben considerar los siguientes lineamientos:
    - Detectar errores en los datos de entrada, como por ejemplo: valores fuera de rango, caracteres inválidos en campos de datos, datos faltantes o incompletos.
    - Determinar las responsabilidades de todos los usuarios involucrados.
    - Identificación de Datos, el sistema debe ser capaz de identificar los datos sensibles e implementar mecanismos de protección y encriptación adecuados en su almacenamiento, lo cuales deben ser informados como parte de la documentación del software para análisis del equipo de seguridad de la información de FONASA.
    - Todo el manejo de datos debe estar alineado con la normativa y legalidad vigente.

- Controles de Incidentes de seguridad
  Se deben incluir registros de incidentes de seguridad de la información, como pistas de auditoría sobre transacciones de archivos críticos para identificar usuario, fecha, hora, lugar de ejecución (IP, MAC, etc.), función realizada, y otros datos necesarios para un adecuado control.

- El sistema debe establecer controles para garantizar la integridad, disponibilidad, confidencialidad y cifrado de la información, a través de protocolos estándar definidos que deben ser entregados como parte de la documentación del aplicativo para análisis de equipo de seguridad de la información de FONASA.

- El sistema debe integrarse a un servicio de FONASA, en el cual debe informar el inicio de la atención en el momento que esta ocurra, identificando datos como identificador de la aplicación, versión de la aplicación, el folio del bono, RUT prestador, Rut paciente y el código de la prestación.

- El sistema debe proveer e implementar protocolos de comunicaciones de red que garanticen la integridad de los datos enviados.

- El sistema debe poseer copias de seguridad de los datos y documentación asociadas a las atenciones realizadas. Estas deben estar ubicadas en un sitio distinto al del sistema productivo.

- Para los datos en tránsito, las comunicaciones de los componentes que transporten información entre usuarios deberán siempre estar protegidas bajo el protocolo de comunicación TLS.

- El sistema deberá realizar consultas seguras a las bases de datos, esto a fin de evitar ataques por ejemplo del tipo SQL Injection, se sugiere utilizar como referencia la “Guía técnica para lineamientos para desarrollo de software del Estado”. Estos atributos serán verificados a través de pruebas de seguridad realizadas por el equipo de FONASA.

- El sistema debe tener un correcto manejo de errores y excepciones:
  - No exponer información sensible o privada en los mensajes de error.
  - Asegurarse de que una excepción o fallo no comprometa la seguridad por un error de programación en el sistema. Por ejemplo, causar una denegación de servicio o ejecución de código con privilegios incorrectos.
  - Registrar las excepciones adecuadamente en un log que permita ser auditable.

- El sistema debe tener claramente establecido un plan de recuperación de información frente a un incidente (sitio de contingencia, respaldo en línea, etc.). Lo anterior debe ser entregado como parte de la documentación del software y el servicio.

- La documentación del sistema debe contener la descripción de los procesos de respaldos de datos de pacientes, indicando su frecuencia y lugar de almacenamiento.

- El sistema debe tener un modo de contingencia frente a caída del sitio productivo el cual debe ser descrito e informado como parte de la documentación del servicio.

3. Aseguramiento y certificación de calidad

Al momento de que la institución presente su software de operación, este podrá ser sometido a pruebas de aseguramiento y posterior certificación de seguridad que valide la operación del mismo. Para lo anterior la institución responsable del software deberá entregar al momento de la solicitud de la inscripción:

- Plan de pruebas de usuario el cual debe contener todos los flujos operativos de la aplicación, entradas y salidas posibles. El plan de pruebas debe contener al menos lo siguiente:
  - Configuración de ambiente de pruebas
  - Casos de Prueba
  - Datos de prueba
  - Flujos
  - Criterios de aceptación.

- Diseño y navegación de la aplicación.

- Identificación de las circunstancias de uso del sistema en que este puede fallar (por ejemplo, establecimiento de la conexión, interrupción en la comunicación, calidad de la imagen, calidad del sonido, calidad del video, fallos de uso, etc.), y que medidas de prevención se han implementado ante estos escenarios para que puedan ser aprobadas por el equipo de aseguramiento de calidad de quien lo certifica.

4. Pruebas de Seguridad de la información, carga y estrés

El sistema presentado por la institución podrá ser sometido a diversas pruebas de seguridad y validación, carga y stress que garanticen su correcto funcionamiento en el contexto de la seguridad de la información y carga de utilización.

No obstante las pruebas que serán realizadas por el equipo certificador, es necesario que la Institución presente documentación relativa a sus propias validaciones de seguridad de información y pruebas de carga, al momento de la solicitud de la inscripción

En general se realizarán pruebas que den cuenta del cumplimiento de todos los lineamientos descritos en el punto 2 de este anexo.

5. Requerimientos de Auditoria

El sistema debe entregar datos de auditoria que permitan hacer trazabilidad de todas las transacciones que estén establecidas en el software de teleconsulta y telerehabilitación.

- Registro de eventos (hora, usuario, origen, transacción).
- Registro de tiempos de atención.
- Registro de incidentes de cualquier tipo que pueda tener la aplicación.
- Cantidad de usuarios registrados y cantidad de transacciones por cada uno de ellos.
- Cantidad de atenciones y detalle de ellas.
- Actualización de versiones de la aplicación con trazabilidad de cambios. Dependiendo del tipo de cambio realizado en la aplicación FONASA podrá solicitar certificar nuevamente la solución.

La información mencionada en este punto debe estar accesible en todo momento y a demanda de FONASA a fin de verificar el comportamiento de la aplicación de acuerdo con los lineamientos definidos.

6. Requerimientos Técnicos Específicos

El Operador Tecnológico debe entregar la siguiente información respecto de su software la cual será auditada y corroborada por los equipos técnicos que certifican:

- Diseño técnico de la aplicación (Lenguajes, bases de datos, métodos de encriptación, integración de componentes, entre otros)
- Datos referidos a la interoperabilidad de información en base a estándares definidos.
- Descripción de métodos posibles de integración vía webservices, SOAP, REST, APIs, etc.
- Descripción de arquitectura de la aplicación (descripción de capas, control de flujo, balanceo, implementación de alta disponibilidad lógica y física, cantidad de nodos por capa, etc.).
- Infraestructura que soporta la aplicación.
- Métodos de respaldo, replicación y contingencia (site principal y secundario)
- El resguardo de los datos debe estar supeditado a la legislación chilena vigente.

7. Aspectos Generales de validación

Si bien en este anexo se describen los aspectos básicos que debe cubrir la aplicación responsable de la atención, la Institución deberá documentar cada uno de estos puntos en un documento general de la aplicación donde describa como da cumplimiento a estos lineamientos.

Dichos documentos serán revisados y analizados para corroborar y certificar que se cumplen estos requisitos mínimos.

Según lo descrito en los puntos 3 y 4 de este documento, realizará las pruebas de uso, seguridad y carga de acuerdo con parámetros establecidos y a la documentación entregada como insumo por el propio operador tecnológico.

Sin perjuicio de lo anterior se podrá solicitar al Operador Tecnológico información adicional, reuniones técnicas o pruebas adicionales que permitan realizar la validación total del aplicativo.

Sin perjuicio de los puntos antes señalados, este es un documento inicial y podría ser modificado por FONASA previo aviso a la Institución en convenio.