CUMPLIMIENTO DE LA SUBPARTE C

Estándares de Seguridad para Protección del “EPHI”

bizuit

HIPAA
Health Insurance Portability and Accountability Act

Definiciones

EPHI: Electronic Protected Health Information, either patient administrative or clinic information.

En Español: Datos Electrónicos Protegidos en Salud, tanto clínicos como administrativos.

ESTÁNDAR DE SEGURIDAD

- Asegurar confidencialidad, integridad y disponibilidad del EPHI
- Proteger contra amenazas y peligros
- Proteger contra mal uso y divulgaciones
- Implementar apropiadamente en concordancia con el ambiente operacional

SUBPARTE C

Estándares de Seguridad para la Protección del EPHI

Regla	Descripción
§ 164.308	Salvaguardias Administrativas
§ 164.310	Salvaguardias Físicas
§ 164.312	Salvaguardias Técnicas
§ 164.314	Requerimientos Organizacionales
§ 164.316	Políticas, procedimientos y requerimientos de documentación

§164.308: Administración de la Seguridad

Implementa políticas y procedimientos para prevenir, detectar, contener y corregir violaciones de seguridad

Especificación	Implementación
Análisis de Riesgo	Evaluar minuciosamente los riesgos potenciales y vulnerabilidades a la confidencialidad, integridad y disponibilidad del EPHI.
Gestión del Riesgo	Implementar medidas de seguridad para reducir riesgos y vulnerabilidades en forma apropiada.
Políticas para Sanción	Definir apropiadamente sanciones y aplicarlas a quienes violen las políticas de seguridad and confidencialidad.
Revisión de la Actividad del Sistema	Implementar procedimientos de revisión regular de los registros de actividad del sistema, como logs, reportes de acceso e incidentes de seguridad.
Asignación del Responsable de la Seguridad	Identificar al oficial responsable de la implementación y aplicación de las políticas y procedimientos.

§164.308: Seguridad de Usuarios

Implementa políticas y procedimientos para que los usuarios cuenten con accesos y restricciones apropiadas.

Especificación	Implementación
Autorización	Implementar procedimientos para autorizar los accesos y restricciones a usuarios al EPHI.
	El módulo de Usuarios y Roles de BIZUIT® permite crear usuarios y asignarles los roles que correspondan.
Acreditación	Implementar procedimientos para validar que los accesos sean apropiados.
	Validar las interfaces de usuario de BIZUIT® para asegurar que cuenten con los accesos y restricciones apropiados.
Terminación	Implementar procedimientos para restringir los accesos al EPHI cuando un usuario sea desvinculado.
	El módulo de Usuarios y Roles para borrar o deshabilitar usuarios.

§164.308: Gestión de Accesos

Implementa políticas y procedimientos para autorizar accesos al EPHI

Especificación	Implementación
Aislar las funciones para autorizaciones	Implementar políticas y procedimientos para proteger el acceso a las funciones de autorización de accesos no autorizados por parte de usuarios de toda la organización. **Los módulos para administración de usuarios y roles están restringidos sólo a superusuarios.**
Autorización de Accesos	Implementar políticas y procedimientos para otorgar accesos al EPHI. Por ejemplo, mediante accesos a workstation, transacciones, programas, procesos, u otros mecanismos. **El módulo de Usuarios y Roles permite otorgar los permisos correspondientes.**
Access establishment and modificación	Implementar políticas y procedimientos para establecer, documentar, revisar y modificar los derechos de accesos a workstations, transacciones, programas o procesos. **El módulo de Usuarios y Roles en conjunto con la configuración de seguridad de los procesos permiten revisar y modificar los permisos de usuario que corresponda.**

§164.308: Entrenamiento de Seguridad y Comunicaciones

Implementa entrenamiento de seguridad y comunicaciones para los usuarios

Especificación	Implementación
Recordatorios de Seguridad	Realizar revisiones y actualizaciones periódicas de seguridad
	RESPONDE A POLÍTICAS INSTITUCIONALES
Protección de Software Malicioso	Implementar políticas y procedimientos para resguardar ataques, detectar y reportar software malicioso.
	RESPONDE A POLÍTICAS INSTITUCIONALES (antivirus)
Monitoreo de Accesos	Implementar políticas y procedimientos para monitorear log-in y reportes de discrepancias.
	El módulo "BIZUIT® System Audit" permite monitorear log-in y discrepancias
Gestión de Contraseñas	Implementar procedimientos para crear, mantener y resguardar contraseñas.
	El módulo de Usuarios y Roles permite administrar contraseñas

§164.308: Incidentes de Seguridad

Implementa políticas y procedimientos para gestionar incidentes de seguridad

Especificación	Implementación
Reporte y Respuesta	Identificar y responder a sospechas o incidentes de seguridad consumados; mitigarlos en la medida de lo practicable, y documentarlos, así como sus resultados.

RESPONDE A POLÍTICAS INSTITUCIONALES

§164.308: Plan de Contingencia

Implementa políticas y procedimientos para responder desastres, fallas y daños al EPHI

Especificación	Implementación
Respaldo de Datos	Implementar procedimientos para crear y mantener copias recuperables del EPHI. **Responde a políticas y procedimientos de respaldo de BD y de almacenamiento externo.**
Plan de Recuperación de Desastres	Implementar procedimientos para restaurar cualquier pérdida de datos. **Responde a políticas y procedimientos de restauración de BD desde almacenamiento externo.**
Plan de Operación de Emergencia	Implementar procedimientos para habilitar continuidad de los procesos de negocio críticos. **Redundancia horizontal/vertical de la plataforma y de BIZUIT®**
Procedimientos de Pruebas	Implementar procedimientos de pruebas periódicas de planes de contingencia. **Responde a políticas y procedimientos institucionales**
Análisis de Criticidad de Aplicaciones y Datos	Evaluar la criticidad de aplicaciones y datos específicos que soporten otros componentes del plan de contingencia. **Responde a políticas y procedimientos institucionales**

§164.310: Salvaguardas Físicas

Implementa políticas y procedimientos para limitar el acceso físico al EPHI

Especificación	Implementación
Control de Acceso a Instalaciones	Implementar políticas y procedimientos para limitar el acceso físico a las instalaciones en las que se almacena el EPHI o se ejecutan los sistemas que tienen acceso a él, asegurando autorizaciones apropiadas.
Uso Seguro de Workstations	Implementar políticas y procedimientos para especificar apropiadamente la ejecución de funciones.
	Implementar salvaguardas físicas para las estaciones de trabajo que acceden al EPHI, para permitir el acceso a usuarios autorizados.
Control de Dispositivos y Medios	Implementar políticas y procedimientos para administrar la recepción y remoción de hardware y medios electrónicos que contengan EPHI desde o hacia las instalaciones, así como su movimiento dentro de las instalaciones.

RESPONDE A POLÍTICAS INSTITUCIONALES

§164.312: Control de Acceso

Implementa políticas y procedimientos técnicos para permitir el acceso al EPHI mediante sistemas de información

Especificación	Implementación
Identificación unívoca de usuarios	Asignar un único nombre y/o número para identificar y trazar la identidad de usuarios. **El módulo de Usuarios y Roles permite la creación de usuarios con nombre unívoco.**
Acceso de Emergencia	Implementar procedimientos para acceder al EPHI durante una emergencia. No Aplica: dado que la transferencia de EPHI no puede ser accedida para operaciones CRUD.
Logoff Automático	Implementar procedimientos electrónicos para cerrar sesión después de un determinado tiempo de inactividad. **BIZUIT® dashboard permite "logoff" de una sesión luego de un tiempo configurable de inactividad.**
Encriptación y Desencriptación	Implementar mecanismos para encriptar y desencriptar el EPHI. **BIZUIT® puede encriptar/desencriptar datos en almacenamiento y transmisión.**

§164.312: Controles de Auditoría

Implementa procedimientos que registren la actividad

Especificación	Implementación
Controles de Auditoría	Implementar mecanismos de hardware, software y/o procedurales que registren y examinen actividad de los sistemas de información que contengan o usen el EPHI.
	**BIZUIT® registra toda la actividad general y detallada con traza en logs estructurados.** **Los Usuarios pueden examinar esta información usando BIZUIT® Dashboard y un superusuario.**

§164.312: Integridad

Implementa políticas y procedimientos para proteger el EPHI de alteraciones impropias

Especificación	Implementación
Autenticación	Implementar mecanismos para corroborar que el EPHI no sea alterado o destruido sin autorización.
	**BIZUIT® no permite modificaciones o eliminaciones físicas.** **BIZUIT® implementa versionado para modificaciones y deshabilitaciones para eliminación lógica de datos.** **BIZUIT® almacena y traza todas las operaciones.**

§164.312: Autenticación de Personas y Entidades

Implementa procedimientos para verificar una persona o entidad

Especificación	Implementación
Autenticación de Personas y Entidades	Implementa procedimientos para verificar que una persona o entidad que acceda al EPHI sea quien dice ser.

La capa de seguridad de BIZUIT® EventManager valida y autoriza todo acceso al sistema, ya sea de usuarios o de otras aplicaciones (escenario de integración).

Tanto GUI como Procesos de negocio o de integración corriendo sobre el motor de BIZUIT® son validados y autorizados antes de ejecutarse.

§164.312: Seguridad de Transmisión

Implementa medidas de seguridad para resguardar las transmisiones de EPHI

Especificación	Implementación
Controles de Integridad	Implementar medidas de seguridad para asegurar que ante cualquier modificación impropia de la transmisión electrónica del EPHI, el sistema sea capaz de detector la alteración.
	Toda transmisión de BIZUIT® puede ser encriptada por el canal (https and/o VPN) o por encriptación y firma del mensaje, de manera que cualquier alteración sea detectada.
Encriptación	Implementar un mecanismo para encriptar el EPHI cuando sea necesario.
	BIZUIT® puede encriptar y desencriptar datos, transporte o Comunicaciones tanto a otras aplicaciones como a la capa de presentación (https).

§164.314: Organizational Requirements

Especificación	Implementación
Contratos para Socios de Negocio	Todo socio de negocio (tanto interno como externo) que cree, reciba, mantenga o transmita el EPHI en nombre de las entidades cubiertas, acepte cumplir con los requerimientos aplicables de esta subparte, mediante la presentación explícita de estos términos en un contrato.
	Todo socio de negocio reportará cualquier incidente de seguridad del que tenga u obtenga conocimiento, incluyendo violaciones a EPHI no asegurado.
Planes Grupales de Salud	Implementar salvaguardas administrativas, físicas, y técnicas que protejan razonable y apropiadamente la confidencialidad, integridad, y disponibilidad del EPHI que se cree, reciba, mantenga, o transmita en nombre de un plan de Seguro grupal.
	Asegurar que cualquier agente a quién se le entregue esta información acepte proteger la información de manera apropiada.
	Reportar a la institución que provee el Seguro grupal, cualquier incidente de seguridad del que tome conocimiento.

ADHERE TO INSTITUTION POLICIES

§164.316: Documentación

Implementa políticas y procedimientos para mantener un registro escrito de acciones, actividades y evaluaciones

Especificación	Implementación
Limite de Tiempo	Retener la documentación por 6 años desde la fecha de creación o de la última fecha de activación, la que sea última.
Disponibilidad	Disponibilizar la documentación para aquellas personas responsables de implementar los procedimientos.
Actualizaciones	Revisar la documentación periódicamente, y actualizar según necesidad, en respuesta a cambios ambientales u operacionales que afecten la seguridad del EPHI.
Cumplimiento	**El diseño e Implementación gráfica con cero-código de BIZUIT® junto a su herramienta de auto-documentación permiten mantener la documentación en línea y actualizada en todo momento y cada vez que sea requerida.**