Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA)

¿Qué es HIPAA?

- La *Regla de Privacidad* de HIPAA establece estándares sobre cómo se puede acceder, usar y divulgar la información en el Código de Bienestar e Instituciones (Welfare and Institutions Code o WRC por sus siglas en inglés) y define los derechos de los clientes con respecto a su información de la salud.

- La ***Regla de Seguridad*** de HIPAA exige que el WRC y el proveedor implementen y mantengan medidas de seguridad físicas y electrónicas para proteger la integridad de los datos y la confidencialidad de la información protegida de la salud. Algunos ejemplos son las cerraduras en las puertas, el cifrado de extremo a extremo del correo electrónico y las tarjetas de acceso. No sacar los archivos de los clientes del WRC o del sitio del proveedor.

La Ley Lanterman y la Confidencialidad

Código de Bienestar e Instituciones — WIC DIVISION 4.5. SERVICIOS PARA PERSONAS CON DISCAPACIDADES DEL DESARROLLO [4500 - 4885]

Título 17 Código de Regulación de California §4514. (Para Centros Regionales)

Toda la información y los archivos obtenidos en el curso de brindar admisión, evaluación y servicios bajo la División 4.1 (a partir de la Sección 4400), División 4.5 (a partir de la Sección 4500), División 6 (a partir de la Sección 6000) o División 7 (a partir de la Sección 7100) a personas con discapacidades del desarrollo será confidencial. La información y los archivos obtenidos durante la prestación de servicios similares a beneficiarios voluntarios o involuntarios antes de 1969 también serán confidenciales…

Términos - Información Médica Protegida (PHI)

- Información que identifica a un Cliente de cualquier forma, recopilada, creada, mantenida o recibida
- “Información médica protegida” - cualquier información de identificación individual del paciente, que incluye el nombre, domicilio, la fecha de nacimiento, el número de teléfono, el correo electrónico, el fax, el número de SSN, el número de la UCI, la fotografía, los nombres de los miembros de la familia o cualquier número o código que pueda identificar de forma única a una persona
- Puede ser electrónico, escrito u oral
- Incluyendo información personal, financiera y médica
- Esto se refiere a:
  - La salud o condición física o mental pasada, presente o futura
  - Tratamientos pasados, presentes o futuros

Identificadores Individuales de PHI

- Nombres;
- Domicilios - todas las subdivisiones geográficas más pequeñas que el estado, incluyendo la dirección postal, la ciudad, el condado, el distrito electoral, el código postal y sus códigos geográficos equivalentes, excepto los tres primeros dígitos de un código postal si, según los datos actualmente disponibles públicamente de la Oficina del Censo:
- La unidad geográfica formada al combinar todos los códigos postales con los mismos tres dígitos iniciales contiene más de 20,000 personas; y
- Los tres dígitos iniciales de un código postal para todas esas unidades geográficas que contengan 20,000 o menos se cambian a 000.
- Todos los elementos (excepto el año) de las fechas directamente relacionadas con una persona (incluyendo la fecha de nacimiento, la fecha de admisión, la fecha del dado de alta, la fecha de fallecimiento y todas las edades mayores de 89 años);
- Números de teléfonos;
- Números de FAX;
- Direcciones de correo electrónico (correo electrónico)

Identificadores Individuales de PHI

- Números de Seguro Social;
- Números de archivos médicos;
- Números de beneficiarios del plan de salud;
- Números de cuenta;
- Nombre de usuario o dirección de correo electrónico de la cuenta en línea, en combinación con una contraseña o una pregunta y respuesta de seguridad;
- Números de certificado/licencia;
- Identificadores y números de serie del vehículo, incluyendo los números de matrícula;
- Identificadores de dispositivos y números

de serie;

- URL Web;
- Direcciones del IP;
- Identificadores biométricos, por ejemplo, huellas dactilares y de voz, escaneos retinianos, etc.;
- Imágenes fotográficas de rostro completo y cualquier imagen comparable; y
- Cualquier otro número, característica o código de identificación único (por ejemplo, UCI)

WRC/ Responsabilidades de los Proveedores

- Obtenga un consentimiento firmado cada vez que tratemos de obtener ***o*** divulgar su PHI a alguien ajeno a nuestra agencia
- No puede usar ni divulgar más información que no sea la permitida por contrato o consentimiento
- Use las medidas de seguridad adecuadas para proteger su PHI
  - Administrativo - p. ej., funciones/accesos asignados
  - Físico - p. ej., habitaciones cerradas con llave/gabinetes archivadores
  - Técnico - p. ej., cifrado electrónico

WRC/ Responsabilidades de los Proveedores

- Denuncie al Departamento de Discapacidad del Desarrollo (Department of Developmental Disabilities o DDS por sus siglas en inglés) cualquier uso o divulgación ilegal de su PHI tan pronto como tengamos conocimiento de ello, por ejemplo, robos de computadoras portátiles y correos electrónicos u otras Violaciones de Datos
- Asegúrese de que los agentes a los que divulguemos/recibamos PHI sigan las mismas reglas que estamos obligados a seguir
- Permitir que las personas a las que se refiere el PHI accedan a su propio PHI
- Permitir que las personas modifiquen su PHI

WRC/ Responsabilidades de los Proveedores

- Permita que las personas reciban un registro de las divulgaciones de PHI – por lo que los archivos de los consentimientos son muy importantes
- Poner los archivos relacionados con PHI a disposición del Secretario de Salud y Servicios Humanos de California
- Devolver o destruir todo PHI tras la rescisión del contrato
- Autorizar la rescisión del contrato si ocurre una infracción

Sanciones:

- HIPAA prevé multas civiles y penales por el uso y la divulgación indebidos de los PHI.
- La Ley de California tiene multas y sanciones adicionales
- HIPAA exige que los empleadores apliquen sanciones que pueden incluir la terminación del empleo por violaciones de la privacidad

Sanciones:

- Cuando una persona divulga información a sabiendas y en violación de HIPAA:
  - Multas: No más de $50,000
  - Encarcelamiento: No más de 1 año
- Cuando se comete con falsos pretextos:
  - Multas: No más de $100,000
  - Encarcelamiento: No más de 5 años
- Cuando se comete con la intención de obtener un beneficio:
  - Multas: No más de $250 000
  - Encarcelamiento: No más de 10 años

¿Cómo Puedo Proteger PHI?

- Modele las mejores prácticas con proveedores, vendedores/ otros. Utilice el cifrado y recuérdeles que también utilicen el cifrado.
- No hable en la comunidad o en las áreas públicas de la oficina sobre un Cliente específico utilizando su nombre completo
- No deseche ninguna información que contenga identificadores de Clientes, incluyendo nombres, números o direcciones de la UCI o de la seguridad social; destruyala!
- No saque gráficos o dispositivos electrónicos de la oficina y los deje donde alguien pueda ver el nombre del Cliente o cualquier información.

¿Cómo Puedo Proteger PHI?

- No deje un correo de voz que incluya el PHI en un mensaje a menos que el Cliente lo haya autorizado específicamente
- No deje un fax o documento impreso que incluya el PHI en un área no segura
- Cuando usted encuentre un PHI desatendido, colóquela en una caja de objetos perdidos/encontrados o reenvíela al Oficial de Cumplimiento de HIPAA

¿Cómo Puedo Proteger PHI?

- No comparta su información de inicio de sesión electrónica con otras personas ni la deje en áreas expuestas
- Cierre la sesión por completo de su computadora o dispositivo electrónico cuando esté lejos de él

Mínimo Necesario

- HIPAA exige que la divulgación de PHI se limite al ***mínimo necesario*** para cumplir con la petición.
- Por ejemplo, si ayudas a un padre a pedir que se envíe a la escuela una evaluación psicológica del WRC. SOLO se enviará la evaluación psicológica (no otros archivos médicos, etc).

Acceso a los Archivos de Salud

- Un Cliente o su representante legal pueden pedir acceso para inspeccionar y copiar su PHI mediante la presentación de una petición por escrito.
- Las regulaciones Lanterman (4725) y Early Start (303.402) también otorgan a los Clientes el derecho de inspeccionar, revisar y obtener una copia precisa de cualquier archivo obtenido en el curso de la prestación de servicios.
- El proveedor debe permitir la inspección de manera oportuna, pero en ningún caso más de cinco (5) días hábiles después de recibir la petición por escrito.
- El proveedor debe hacer que las fotocopias estén disponibles de manera oportuna y, en cualquier caso, debe transmitir las copias dentro de los quince (15) días calendario posteriores a la recepción de la petición por escrito.

Modificación de los Archivos de Salud

- Los Clientes pueden pedir una modificación de sus archivos si consideran que el PHI es incorrecta o está incompleta mediante la presentación de una petición por escrito.
- El WRC no tiene que aceptar modificar el archivo, pero si rechazamos la petición, lo haremos por escrito.
- El WRC tiene sesenta (60) días calendario después de la recepción para decidir si acepta o rechaza la petición de modificación.

Petición de Restricciones

- El Cliente puede pedir restricciones sobre la forma en que el WRC usa o divulga el PHI.
- Por ejemplo, un Cliente adulto puede pedir que la información no se comparta con un hermano.
- El WRC no tiene que estar de acuerdo con la petición.
- El WRC debe documentar cualquier restricción con la que esté de acuerdo.

Petición de Comunicaciones Confidenciales

- Un Cliente puede pedir que el WRC se ponga en contacto con ellos de una manera determinada.
- El WRC debe atender cualquier petición razonable o legal.
- Es posible que el WRC no exija al Cliente que explique el motivo de la petición.
- Por ejemplo, un Cliente puede pedir que solo lo contacten en su casa y no en su lugar de trabajo.

Vendedores/Proveedores

- El WRC trabaja con muchos Vendedores/Proveedores que brindan servicios directos a los Clientes. Los Vendedores/Proveedores también están obligados a cumplir con las regulaciones de la HIPAA.

- *Cualquier* incumplimiento de la confidencialidad que ocurra con los Vendedores/Proveedores debe ser denunciado y abordado por el Oficial de Privacidad de la HIPAA. El DDS tiene requisitos especiales de notificación si se produce una infracción de este tipo.

- Consulte los Centros de Servicios de Medicare y Medicaid para conocer las regulaciones en: http://hhs.gov/ocr/hipaa/

Cifrado

- Los Vendedores/Proveedores deben utilizar un cifrado de extremo a extremo (E2EE), que es un método de comunicación segura que evita que terceros accedan a los datos mientras se transfieren de un sistema o dispositivo final a otro. En E2EE, los datos se cifran en el sistema o dispositivo del remitente y solo el destinatario previsto puede descifrarlos.
- Los Vendedores/Proveedores deben tener un acuerdo de socio comercial (business associate agreement o BAA por sus siglas en ingles) vigente con cada uno de sus socios para mantener la seguridad del PHI y el cumplimiento general de HIPAA.

Servicios de Cifrado de Correo Electrónico Conforme con HIPAA

- Barracuda
- Egress
- Hushmail
- kIdentillect
- LUXSCI

Servicios para Compartir Archivo Conforme con HIPAA

- Box
- Citrix ShareFile
- Microsoft OneDrive
- Google Workspace
- Kiteworks

Herramientas Recomendadas Para el Cifrado de Discos

- Bitlocker (Windows)
- FileVault (mac OS)
- Sophos
- TrueCrypt