epihc | ETHICAL PRINCIPLES IN HEALTH CARE™

En colaboración con el
Gobierno de Japón

Resumen del módulo 7

epihc.org

PRINCIPIO ÉTICO 7 – PROTECCIÓN DE LA INFORMACIÓN DEL PACIENTE

EL POR QUÉ, EL CÓMO Y TU DEBER

ESCENARIO

INFORMACIÓN PRIVADA DE CELEBRIDADES A LA QUE SE ACCEDIÓ

APRENDIZAJES CLAVE, DEBERES Y OBLIGACIONES CRÍTICAS

1. Eduque y sensibilice continuamente a todo el personal sobre los riesgos de protección de datos, en particular los derivados de la recepción de correos electrónicos.
2. Avise a los pacientes, al personal y a otras personas si sus datos han sido vulnerados y compartidos.
3. Actúe con honestidad y responsabilidad, prohibiendo prácticas que perjudiquen a los pacientes y manejar cualquier amenaza o riesgo real o percibido para los datos de pacientes, personal y clientes con urgencia, transparencia y sensibilidad.
4. Mantenga medidas de seguridad administrativas, técnicas y físicas adecuadas para garantizar que:
   a. Los registros, documentos e informes de la organización (físicos, digitales o electrónicos) se mantengan precisos, completos y protegidos contra manipulaciones.
   b. La información médica se mantenga confidencial.
   c. La información está protegida contra pérdida o mal uso.
   d. La confidencialidad de los registros de pacientes, personal y clientes se mantenga de acuerdo con los estándares legales y éticos aplicables.
   e. El personal se abstenga de hablar sobre los pacientes y sus condiciones en áreas públicas.
   f. Los datos no se vendan ni se moneticen sin el consentimiento de quienes contribuyen a ellos.

SUS DEBERES Y OBLIGACIONES

NOTAS PARA GERENTES

Seguir las buenas prácticas no es negociable!

CASO LEGAL

VIOLACIÓN DE DATOS DE LOS REGISTROS DE PACIENTES

1. Comprenda el marco regulatorio que rige la protección de datos.
2. Revise las estructuras de gobernanza, las políticas formales y los procedimientos que respaldan el uso y la protección de los datos y se alinean con el marco regulatorio.
3. Evalué las brechas en los procesos de gobernanza y hacer recomendaciones sobre cómo cerrar estas brechas en la protección de datos y apoyar las mejores prácticas según los Principios de Datos de la OMS.
4. Escale las áreas de riesgo significativo, particularmente en relación con la violación de datos, al Comité de Riesgos de la Junta.
5. Desarrolle protocolos y procedimientos para ciberataques y fugas de datos.
6. Garantice que los servicios a los pacientes cumplan con los más altos estándares de mecanismos de protección de datos.
7. Considere cómo las distintas partes interesadas con diferentes tareas e intereses desempeñan un papel en los tipos de violaciones de datos, los facilitadores y los impactos.
8. Considere los factores institucionales que contribuyen al incumplimiento organizacional de las medidas de protección de datos y cómo los reguladores y las partes interesadas de las organizaciones de atención médica pueden abordar colectivamente estos factores.
9. Proteja la propiedad intelectual, incluidas marcas comerciales, derechos de autor y patentes, de proveedores y otras partes interesadas.

NOTAS PARA ALTOS EJECUTIVOS Y MIEMBROS DEL CONSEJO DIRECTIVO

¡Fingir ignorancia no es una defensa válida!