

HIPAA 2009
Capacitación en Privacidad y Seguridad
Prueba y CLAVE DE RESPUESTAS

Nombre: _____ Núm. de ID de empleado: _____ **LA PRUEBA HA SIDO EVALUADA**
Unidad/Depto.: _____ Gerente: _____ **Y CORREGIDA POR: _____**
Fecha: _____

1. **HIPAA es una ley federal aprobada para proteger la privacidad de la información personal y médica de los pacientes y proveer su seguridad física y electrónica.**
- Verdadero
 - Falso
 - HIPAA NO es una ley federal.
 - HIPAA permite que todo empleado de atención médica vea los expedientes de los pacientes.

Respuesta: a – Verdadero
Consultar la Página 2:

HIPAA es una ley federal aprobada para:

- **Proteger la privacidad de la información personal y médica de los pacientes.**
- **Ofrecer seguridad física y electrónica de la información médica personal.**
- **Simplificar la facturación y otras transacciones con códigos y transacciones estandarizados.**
- **Especificar nuevos derechos de los pacientes a aprobar el acceso/uso de su información médica.**

2. **¿Quiénes deben cumplir la ley HIPAA?**
- Médicos
 - Médicos y otros proveedores de atención a pacientes
 - Sólo supervisores y otros administradores
 - Todos los miembros del personal de la Universidad

Respuesta: d – Todos los miembros del personal de la Universidad
Consultar la Página 3:

La Ley de Transferibilidad y Responsabilidad de Seguros Médicos (HIPAA) requiere que UCLA capacite a todos los miembros de su personal acerca de las políticas de HIPAA de la Universidad y los procedimientos específicos requeridos por HIPAA que pueden afectar el trabajo que usted hace para UCLA Medical Sciences, que incluye el UCLA Hospital System, la Faculty Group Practice y la David Geffen School of Medicine (DGSOM), que aquí se denominan colectivamente como “la Universidad”.

3. **¿Qué significa PHI?**
- Physical Health Injuries (Lesiones físicas)
 - Patient and Hospital Incidents (Incidentes de pacientes y hospitales)
 - Personal and Health Information (Información personal y de salud)
 - Protected Health Information (Información médica protegida)

Respuesta: d – Información médica protegida
Consultar la Página 6:

Información de salud con identificadores = Información Médica Protegida (PHI)

HIPAA

Capacitación en Privacidad y Seguridad

Posprueba y Clave de respuestas

4. **Entre los ejemplos de Información Médica Protegida (PHI) se incluyen:**
- a. Nombre, dirección, fecha de nacimiento, número de seguro social, dirección de correo electrónico
 - b. Registros médicos, diagnósticos, tratamientos, resultados de pruebas
 - c. Registros de facturación, registros de investigación, autorizaciones de referencia
 - d. Todas las opciones anteriores

Respuesta: d – Todas las opciones anteriores
Consultar la Página 7

5. **¿En qué circunstancias puede usted acceder a la información PHI y compartir esa información?**
- a. Sólo si sabe que al paciente no le va a importar
 - b. Una vez que ya no trabaje en la organización
 - c. Después de que un paciente ha muerto
 - d. Sólo si es parte de su trabajo, y solamente se puede compartir con personas que necesitan la información

Respuesta: d – Sólo si es parte de su trabajo, y solamente se puede compartir con personas que necesitan la información

6. **Bajo HIPAA, los pacientes tienen ciertos derechos contenidos en los siguientes documentos:**
- a. Declaración de Confidencialidad
 - b. Aviso de Prácticas de Privacidad
 - c. Condición al ser Admitido
 - d. Formulario de Divulgación de Información

Respuesta: b – Aviso de Prácticas de Privacidad

Consultar la Página 10

La Universidad debe dar a cada paciente un Aviso de Prácticas de Privacidad que:

- **Describa cómo la Universidad puede usar y divulgar la información médica protegida del paciente (PHI) e**
- **Informe al paciente de sus derechos de privacidad**

7. **El mejor amigo de su hermana ha sido sometido a una operación de triple bypass en el centro médico. Su hermana le pide que averigüe el pronóstico. ¿Qué debe hacer?**
- a. Preguntarle a una enfermera del piso cómo está el paciente y pasarle la información a su hermana.
 - b. Ingresar en Essentris y PCIMS y pasarle la información a su hermana.
 - c. Explicar que hacer preguntas o mirar los registros del paciente es una violación de la privacidad del paciente.
 - d. Ninguna de las opciones anteriores.

Respuesta: c -- Explicar que hacer preguntas o mirar los registros del paciente es una violación de la privacidad del paciente.
Consultar la Página 5 y la Página 11

HIPAA

Capacitación en Privacidad y Seguridad

Posprueba y Clave de respuestas

¿Cuáles son los requisitos de HIPAA?

- ✿ Proteger la privacidad y la seguridad de la Información Médica Protegida (PHI) de las personas
- ✿ Requerir el uso del “mínimo necesario”
- ✿ Ampliar los derechos de las personas respecto al uso* de su información médica protegida

*El uso incluye el acceso o la búsqueda del registro de un paciente en cualquiera de los sistemas de la Universidad o en los archivos en papel que no se requiera para hacer su trabajo.

A menos que las leyes lo requieran o lo permitan, la Universidad debe obtener la autorización del paciente para usar, divulgar o acceder solamente al mínimo necesario:

- 🔒 Autorización del paciente - permite a la Universidad divulgar información con otros fines (§164.508)
- 🔒 Mínimo necesario se aplica a todos los usos y divulgaciones de pagos y de todas las operaciones de atención de la salud (§164.502(b), §164.514(d))

8. ¿Cuándo puede la Universidad usar o divulgar la información PHI?

- a. Para el tratamiento de un paciente, si el paciente ha recibido el Aviso de Prácticas de Privacidad de la Universidad.
- b. Para el pago de cuentas, si el paciente ha recibido el Aviso de Prácticas de Privacidad de la Universidad.
- c. Para actividades de enseñanza, si el paciente ha recibido el Aviso de Prácticas de Privacidad de la Universidad.
- d. Todas las opciones anteriores

Respuesta: d – Todas las opciones anteriores.

Consultar la Página 10

- 🌿 La Universidad debe dar a cada paciente un Aviso de Prácticas de Privacidad que:
 - Describa cómo la Universidad puede usar y divulgar la información médica protegida del paciente (PHI) e
 - Informe al paciente de sus derechos de privacidad
- 🌿 La Universidad debe intentar obtener la firma del paciente acusando recibo del Aviso, SALVO en situaciones de emergencia. Si no se obtiene la firma, la Universidad debe documentar la razón por la que no se obtuvo.
- 🌿 45 CFR164.520(a)(b)

9. ¿Qué forma de datos del paciente deben protegerse y mantenerse confidenciales bajo las leyes estatales y federales, así como bajo las políticas del sistema de salud?

- a. Escritos
- b. Orales

HIPAA

Capacitación en Privacidad y Seguridad

Posprueba y Clave de respuestas

- c. Electrónicos
- d. Todas las opciones anteriores

Respuesta: d – Todas las opciones anteriores.
Consultar la Página 14

Todos los datos personales y médicos que existen para todas las personas, en cualquier forma:




-  Escritos
-  Orales
-  Electrónicos

Esto incluye la información médica protegida por HIPAA y la información confidencial bajo las leyes estatales.

10. Debido a que tengo acceso a datos confidenciales de los pacientes como parte de mi trabajo, puedo ver los registros de cualquier persona, aunque no sea mi paciente, siempre y cuando no comunique los datos a nadie más.
- a. Verdadero
 - b. Falso
 - c. También puedo compartir dicha información con mi familia y amigos cercanos.
 - d. Puedo obtener acceso a información impresa, como expedientes médicos, en cualquier momento, pero no a los registros electrónicos.

Respuesta: b -- Falso

Consultar la Página 5
¿Cuáles son los requisitos de HIPAA?

-  Proteger la privacidad y la seguridad de la Información Médica Protegida (PHI) de las personas
-  Requerir el uso del “mínimo necesario”
-  Ampliar los derechos de las personas respecto al uso* de su información médica protegida

*El uso incluye el acceso o la búsqueda del registro de un paciente en cualquiera de los sistemas de la Universidad o en los archivos en papel que no se requiera para hacer su trabajo.

11. Usted puede proteger los datos de los pacientes de la siguiente manera:
- a. Protegiendo la información verbal o escrita
 - b. Utilizando métodos seguros de computación
 - c. Informar de las sospechas de incidentes de seguridad
 - d. Todas las opciones anteriores

Respuesta: d – Todas las opciones anteriores

HIPAA

Capacitación en Privacidad y Seguridad

Posprueba y Clave de respuestas

Cómo puede usted proteger la información de los pacientes: PHI / ePHI /Confidencial

- Atención a la comunicación verbal
- Protecciones del material impreso
- Métodos seguros de computación
- Informar de las sospechas de incidentes de seguridad

12. Una estudiante de UCLA de 19 años es ingresada a la sala de emergencia por lesiones sufridas en un accidente automovilístico. La estudiante está en situación estable, pero despierta y alerta. Su padre llama desde Minnesota para pedir información sobre el estado de la paciente. Usted puede:

- a. Informar al padre de la paciente sobre su condición y estado general.
- b. No dar ninguna información al padre.
- c. Obtener el consentimiento de la paciente para dar información que va más allá de la condición y el estado general.
- d. Opciones a y c.

Respuesta: d – Opciones a y c
Consultar las Páginas 10 y 11

- La Universidad debe dar a cada paciente un Aviso de Prácticas de Privacidad que:
 - Describa cómo la Universidad puede usar y divulgar la información médica protegida del paciente (PHI) e
 - Informe al paciente de sus derechos de privacidad
- La Universidad debe intentar obtener la firma del paciente acusando recibo del Aviso, SALVO en situaciones de emergencia. Si no se obtiene la firma, la Universidad debe documentar la razón por la que no se obtuvo.
- 45 CFR164.520(a)(b)

A menos que las leyes lo requieran o lo permitan, la Universidad debe obtener la autorización del paciente para usar, divulgar o acceder solamente al mínimo necesario:

- Autorización del paciente - permite a la Universidad divulgar información con otros fines (§164.508)
- Mínimo necesario se aplica a todos los usos y divulgaciones de pagos y de todas las operaciones de atención de la salud (§164.502(b), §164.514(d))

13. Un reportero viene a la sala de emergencia y le dice al médico encargado que hay sospechas de que el accidente en el que la chica de 19 años fue herida fue causado por un francotirador que tiraba sobre la autopista, y que está preparando un reporte para el noticiero de la noche. Quiere saber el nombre de la paciente y su estado para el reporte. Usted puede darle esta información.

- a. Verdadero
- b. Falso
- c. Cualquier empleado puede hablar con los medios noticieros.
- d. Sólo se puede dar el nombre del paciente.

HIPAA

Capacitación en Privacidad y Seguridad

Posprueba y Clave de respuestas

Respuesta: b -- Falso

Se requiere una autorización específica para divulgar el nombre y la condición. La pregunta debe remitirse al departamento de relaciones con los medios.

14. Su supervisor (un médico) está muy ocupado y le pide que ingrese en el sistema de información clínica usando la ID y contraseña del médico para obtener algunos informes de pacientes. ¿Qué debe hacer?

- a. Se trata de su jefe, por lo cual está bien hacerlo.
- b. Ignorar el pedido y esperar a que el médico se olvide.
- c. Negarse al pedido y mencionar las Políticas de Seguridad de Datos de UC.
- d. Ninguna de las opciones anteriores

**Respuesta: c – Negarse al pedido y mencionar las Políticas de Seguridad de Datos de UC
Uso de Buenas Prácticas de Computación**

15. Un compañero de trabajo tiene que salir para hacer unas diligencias breves y deja la computadora ingresada en el sistema de información confidencial. Usted tiene que consultar información usando la misma computadora. ¿Qué debe hacer?

- a. Desconectar a su compañero y volver a ingresar con su propia ID y contraseña.
- b. Para ahorrar tiempo, seguir trabajando con la ID de su compañero.
- c. Esperar a que el compañero regrese antes de desconectarlo; o tomarse un descanso largo hasta que el compañero regrese.
- d. Dejar la computadora de su compañero ingresada en el sistema y usar otra computadora.

Respuesta: a -- Desconectar a su compañero y volver a ingresar con su propia ID y contraseña.

Use Buenas Prácticas de Computación – Siga las políticas y procedimientos de UCLA Medical Sciences o del campus de UCLA en lo referente a confidencialidad y seguridad de la información.

16. Todo el contenido del teléfono móvil (blackberry) de una persona famosa ha aparecido en Internet, incluidos los mensajes electrónicos privados, las direcciones y los números de teléfono de la libreta de teléfonos. Parece que la red móvil ha sido atacada por hackers. Un médico tiene información similar en su blackberry, incluida una foto de un paciente (obtenida con el consentimiento del paciente) para descargar a una presentación educativa. ¿Cómo puede este médico proteger esta información de la mejor manera?

- a. Descargar la foto inmediatamente después de tomarla, y borrar la imagen del teléfono.
- b. No tomar fotos de pacientes en este tipo de dispositivo.
- c. Solamente mantener información en el teléfono móvil que no cause problemas si se coloca en un sitio público.
- d. Todas las opciones anteriores.

Respuesta: c – Solamente mantener información en el teléfono móvil que no cause problemas si se coloca en un sitio público.

Uso de Buenas Prácticas de Computación

HIPAA

Capacitación en Privacidad y Seguridad

Posprueba y Clave de respuestas

- ❌ No tenga datos confidenciales en dispositivos portátiles
- ❌ Haga copias de seguridad de sus datos
 - Haga copias de seguridad con regularidad, idealmente por lo menos una vez al día.
 - Haga copias de los datos en el servidor seguro de su departamento o en medios removibles como un CD-RW o un lápiz de memoria USB.
 - Guarde los datos de seguridad en forma segura y separados del equipo. Recuérdelo, ¡sus datos son valiosos!

17. El acceso electrónico a los datos de los pacientes puede rastrearse para identificar su ID de usuario y su computadora, y define los documentos y el tiempo que ha pasado accediendo a los registros.

- a. Verdadero
- b. Falso
- c. El ID de usuario y la computadora no se pueden rastrear.
- d. Ninguna de las opciones anteriores.

Respuesta: a – Verdadero

Practicar un uso seguro de Internet

- El acceso electrónico a los datos de los pacientes puede rastrearse para identificar su ID de usuario y su computadora, y define los documentos y el tiempo que ha pasado accediendo a los registros.
- El acceso a sitios con contenido cuestionable a menudo ocasiona spam o virus.
- Y vale la pena repetirlo...
¡No descargue programas desconocidos o no solicitados!

18. Un archivo adjunto a un correo electrónico con una lista no encriptada de pacientes de VIH fue enviada por error a 10 personas fuera de la organización (nombres, MRN, SSN y diagnóstico). ¿Qué medidas se deben tomar?

- a. El usuario debe notificar inmediatamente a Servicios de Computación.
- b. El personal de servicios de computación debe actuar inmediatamente respecto a este aviso.
- c. Los líderes de UCLA deben notificar a los 10 receptores. Se debe documentar y notificar el incidente y las medidas correctivas en un plazo no superior a 5 días al Departamento de Salud Pública de California y a los pacientes afectados y representantes legales.
- d. Todas las opciones anteriores.

Respuesta: d – Todas las opciones anteriores

Buenas Prácticas de Computación

Informar de los incidentes/violaciones de seguridad

- Además, informe inmediatamente de cualquier cosa inusual, sospechas de incidentes de seguridad, o violaciones de seguridad a su Coordinador de Soporte de Computación y a su supervisor. Las áreas de la Universidad deben llamar al Despacho de Ayuda de MCCS, al (310) 794-4357.
- Esto también se aplica al robo o pérdida de información PHI en formato físico (papel, película, etc.).
- Puede también ponerse en contacto con el Oficial de Seguridad de Información de Medical Sciences.

HIPAA

Capacitación en Privacidad y Seguridad

Posprueba y Clave de respuestas

- ❌ Si no se protege el acceso/uso/divulgación no autorizados se podrían imponer sanciones de hasta \$25,000 por paciente.
- ❌ **Ann S. Chang, CISSP**
achang@mednet.ucla.edu
(310) 825-7003

19. Yo no trabajo con pacientes ni tengo acceso a registros médicos, pero veo a los pacientes que pasan frente a mi escritorio en la clínica. ¿No puedo hablar sobre los pacientes con mis compañeros de trabajo, familiares y amigos, aunque no tenga nada que ver con mi trabajo?

- a. Solamente puede hablar de los pacientes con sus compañeros de trabajo.
- b. Solamente puede hablar de los pacientes con sus familiares y amigos.
- c. Puede hablar de los pacientes con sus compañeros de trabajo, familiares y amigos.
- d. Usted **NO** puede discutir ninguna información de los pacientes con nadie, a menos que necesiten la información para realizar su trabajo.

Respuesta: d -- Usted NO puede discutir ninguna información de los pacientes con nadie, a menos que necesiten la información para realizar su trabajo.

Consultar las Página 5 y 11:

¿Cuáles son los requisitos de HIPAA?

- ❌ **Proteger la privacidad y la seguridad de la Información Médica Protegida (PHI) de las personas**
- ❌ **Requerir el uso del “mínimo necesario”**
- ❌ **Ampliar los derechos de las personas respecto al uso* de su información médica protegida**

***El uso incluye el acceso o la búsqueda del registro de un paciente en cualquiera de los sistemas de la Universidad o en los archivos en papel que no se requiera para hacer su trabajo.**

A menos que las leyes lo requieran o lo permitan, la Universidad debe obtener la autorización del paciente para usar, divulgar o acceder solamente al mínimo necesario:

- ❌ **Autorización del paciente - permite a la Universidad divulgar información con otros fines (§164.508)**
- ❌ **Mínimo necesario se aplica a todos los usos y divulgaciones de pagos y de todas las operaciones de atención de la salud (§164.502(b), §164.514(d))**

20. ¿De qué medidas de protección de seguridad de estaciones de trabajo es responsable USTED de usar y/o proteger?

- a. ID del usuario
- b. Contraseña
- c. Salir de los programas que acceden a información PHI cuando no los esté usando.
- d. Todas las opciones anteriores

Respuesta: d – Todas las opciones anteriores
Consultar la Página 44

“Buenas Prácticas de Computación”
10 Protecciones para los usuarios

- 1. Contraseñas**
- 2. Bloquear la pantalla**
- 3. Seguridad de la estación de trabajo**
- 4. Dispositivos portátiles**
- 5. Manejo de datos**
- 6. Antivirus**
- 7. Seguridad de Computación**
- 8. Correo electrónico**
- 9. Uso seguro de Internet**
- 10. Informar de las sospechas de incidentes de seguridad**

DECLARACIÓN DE CONFIDENCIALIDAD

La protección de la información médica y de otros datos confidenciales es un derecho protegido por las leyes y que se hace cumplir por medio de multas, sanciones penales y también por la política del UCLA Health System.

La protección de la información confidencial es una obligación fundamental de todos los empleados, personal docente clínico, médicos residentes (*house staff*), estudiantes y voluntarios.

Su firma de esta declaración lo comprometerá con esa obligación, y **SERÁ** usada como prueba de que usted entiende las obligaciones y hechos básicos referentes a la privacidad.

Léala cuidadosamente.

Al firmar esta declaración, usted acepta:

1. Acepto proteger la privacidad y la seguridad de la información confidencial en todo momento, tanto durante como después de terminar mi empleo en la Universidad de California.
2. Acepto a) acceder a la información confidencial en el grado mínimo necesario para mis tareas asignadas y b) divulgar dicha información únicamente a las personas autorizadas a recibirla.
3. Acepto que entiendo lo siguiente:
 - a. El UCLA Health System hace un seguimiento de todas las ID de usuario usadas para acceder a registros electrónicos. Esas ID permiten descubrir el acceso inapropiado TANTO a los registros de empleados como a los de los pacientes.
 - b. El acceso inapropiado y la divulgación no autorizada de información protegida será motivo de medidas disciplinarias, que pueden incluir hasta la terminación del empleo, y pueden ser causa de un informe a las autoridades a cargo de otorgar licencias profesionales, del cumplimiento de las leyes de privacidad y del enjuiciamiento de actos criminales. La Oficina de Integridad de Información Médica (OHII) podrá imponer sanciones a **personas** o proveedores de atención médica de **\$2,500 a \$25,000 por incumplimiento**.
 - c. Las ID de usuario no se pueden compartir. El uso inapropiado de mi ID (**por mí o por otra persona**) es **mi** responsabilidad y me expone a consecuencias graves.

Firma: _____

Nombre en letra de molde: _____

Fecha: _____

Iniciales del Supervisor o Jefe _____

DECLARACIÓN DE CONFIDENCIALIDAD

INFORMACIÓN SUPLEMENTARIA

La Información Médica Confidencial incluye, sin limitarse a:

Cualquier información individualmente identificable en poder o derivada de un proveedor de atención de la salud, referente al historial médico de un paciente, su condición o tratamiento mental o físico, así como los registros, resultados de pruebas, conversaciones, registros de investigación e información financiera de los pacientes y/o sus familiares. (Nota: esta información se define en las Reglas de Privacidad como “información médica protegida”.) Los siguientes son ejemplos, sin limitarse a:

- Los registros médicos físicos y psiquiátricos incluyen material en papel, fotos, video, informes de diagnóstico y terapéuticos, muestras de laboratorio y patológicas;
- Registros de seguro y facturación de los pacientes;
- Datos computarizados de los pacientes, en computadoras centrales y departamentales, y mensajes alfanuméricos de radio para buscar personas;
- Observación visual de los pacientes que reciben atención médica o acceden a servicios; e
- Información verbal provista por un paciente o referente a un paciente.

La Información Confidencial de Empleados y Negocios incluye, sin limitarse a:

- Teléfono y dirección del empleado;
- Nombre del cónyuge u otros familiares;
- Número de Seguro Social o registros de retención impositiva;
- Información relacionada con la evaluación del rendimiento;
- Otra información obtenida de los registros de la Universidad que, en caso de divulgarse, constituiría una invasión injustificada de la privacidad; o
- Divulgación de información confidencial de negocios que causaría daño al UCLA Health System.

Provisiones reglamentarias relevantes:

- Las actividades y la información de revisión por funcionarios de igual nivel y de gestión de riesgos están protegidas por el Código de Evidencia de California sección 1157 y el privilegio de las comunicaciones entre abogado y cliente.
- La Ley Federal de Transferibilidad y Responsabilidad de Seguros Médicos (“HIPAA” o la “Regla de Privacidad”) (45 Código de Reglamentaciones Federales, Parte 160 et seq.) define las normas federales para la protección de la información médica.
- La Ley de Confidencialidad de Información Médica de California (Código Civil de California § 56 et seq.) y la Ley Lanterman-Petris-Short (Código de Bienestar e Instituciones de California § 5000 et seq.) gobiernan la divulgación de información identificable de los pacientes por parte de los hospitales y otros proveedores de atención médica.
- La Ley de Prácticas de Información del Estado (Código Civil de California, secciones 1798 et seq.) gobierna la adquisición y el uso de datos referentes a personas.

- **Los proyectos de ley SB541 y AB211 establecen que el acceso, revisión, visionado o divulgación no autorizados de información personal o información médica protegida sean notificados al Departamento de Salud y al paciente en un plazo no superior a 5 días a partir de su detección. Se podrán imponer sanciones y multas monetarias contra UCLA y contra el miembro del personal específico y el incidente podrá ser notificado al consejo de concesión de licencias del miembro del personal (p. ej., el Consejo Médico o de Enfermería).**