

# **Capacitación básica en privacidad y seguridad para HIPAA 2009**

¿Qué es la Ley de Transferibilidad y Responsabilidad de Seguros Médicos (**HHealth Insurance Portability and Accountability Act, o “HIPAA”)?**

## **HIPAA es una ley federal aprobada para:**

- Proteger la privacidad de los datos personales y médicos de los pacientes
- Ofrecer seguridad física y electrónica de los datos personales de salud
- Simplificar la facturación y otras transacciones con Códigos Estandarizados y Transacciones
- Especificar nuevos derechos de los pacientes para la aprobación del acceso/uso de sus datos médicos

## **¿Se aplica la ley HIPAA a usted?**

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

---

## **Responda a estas preguntas**

- 1. HIPAA es una ley federal aprobada para proteger la privacidad de los datos personales y de salud de los pacientes y para preservar la seguridad física y electrónica de esos datos.**
  - a. Verdadero
  - b. Falso
- 2. ¿Quiénes deben cumplir la ley HIPAA?**
  - a. Médicos
  - b. Médicos y otros proveedores de atención a pacientes
  - c. Sólo supervisores y otros administradores
  - d. Todos los miembros del personal de la Universidad

## ¿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 sus datos PHI

\*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 realizar el trabajo.



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

## ¿Qué datos del paciente debemos proteger?

### Debemos proteger los datos personales y de salud de los pacientes que...

- sean creados, recibidos o mantenidos por un proveedor de servicios de salud o un plan de salud
- sean escritos, orales o electrónicos
- e incluyan por lo menos uno de los 18 identificadores personales en relación con los datos de salud

### Información Médica Protegida (PHI): 18 identificadores definidos por HIPAA

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Nombre   | <input checked="" type="checkbox"/> Número de registro médico  |
| <input checked="" type="checkbox"/> Dirección postal                                 | <input checked="" type="checkbox"/> Número de beneficiario del plan de salud                               |
| <input checked="" type="checkbox"/> Todos los elementos de las fechas excepto el año | <input checked="" type="checkbox"/> Identificadores de dispositivos y sus números de serie                 |
| <input checked="" type="checkbox"/> Número de teléfono                               | <input checked="" type="checkbox"/> Identificadores de vehículos y sus números de serie                    |
| <input checked="" type="checkbox"/> Número de fax                                    | <input checked="" type="checkbox"/> Identificadores biométricos  |
| <input checked="" type="checkbox"/> Dirección de correo electrónico                  | <input checked="" type="checkbox"/> (huellas dactilares y de voz)  |
| <input checked="" type="checkbox"/> Dirección URL                                    | <input checked="" type="checkbox"/> Fotos faciales y otras imágenes comparables                            |
| <input checked="" type="checkbox"/> Dirección IP                                     | <input checked="" type="checkbox"/> Cualquier otro número, código o característica de identificación única |
| <input checked="" type="checkbox"/> Número de seguro social                          |  |
| <input checked="" type="checkbox"/> Números de cuenta                                |  |
| <input checked="" type="checkbox"/> Números de licencia                              |  |

---

## Responda a estas preguntas

### 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)

### 4. ¿En qué circunstancias puede usted contar a otras personas la información PHI que oye en su trabajo?

- Sólo si sabe que al paciente no le va a importar
- Una vez que ya no trabaje en la organización
- Después de que un paciente ha muerto
- Cuando su trabajo lo requiere

## 5. La Información Médica Protegida (PHI) incluye:

- a. nombre, dirección, fecha de nacimiento, número de seguro social, dirección de correo electrónico
- b. registros médicos, diagnósticos, tratamientos, resultados de pruebas
- c. datos de facturación, informes del censo, autorizaciones de referencia
- d. todas las opciones anteriores

## Para que la Universidad utilice o divulgue la información PHI

- La Universidad debe dar a cada paciente un Aviso de Prácticas de Privacidad que:
  - Describa la forma en que 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 de 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)

**Pero**, para fines que no sean el tratamiento, pagos, operaciones... 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))

---

## Responda a estas preguntas

### 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 Autorización

### 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 usted?

- 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.

**8. Después de que un paciente recibe el Aviso de Prácticas de Privacidad, ¿cuándo puede la Universidad acceder a la información PHI o divulgar esa información?**

- a. Para el tratamiento de un paciente
- b. Para el pago de cuentas
- c. Para las operaciones de atención de la salud
- d. Todas las opciones anteriores.

**Con todas las leyes estatales y federales, ¿qué datos del paciente deben protegerse?**

**Todos los datos personales y de salud 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.**

**Para el paciente, todos son datos confidenciales**

- Datos **personales** del paciente
- Datos **financieros** del paciente
- Datos **médicos** del paciente
  - Datos **PHI** escritos, orales y electrónicos

---

**Responda a estas preguntas**

**9. ¿Qué forma de datos PHI deben protegerse y mantenerse confidenciales bajo las leyes estatales y federales, así como bajo las políticas de la Universidad?**

- a. Escritos
- b. Orales
- c. Electrónicos
- d. Todas las opciones anteriores

# ¿Por qué yo?

**Yo no atiendo a los pacientes... ¿Necesito capacitación?**

**Yo no uso ni tengo contacto con la información médica o financiera de los pacientes...  
¿Necesito capacitación?**

Y...

**¿No es este simplemente un problema de informática (IT)?**

---

## ¿Quiénes usan PHI en UCLA?

- **Todas las personas** que trabajan con, o que ven, información de salud, financiera, o confidencial con identificadores PHI de HIPAA
- **Todas las personas** que usan una computadora o dispositivo electrónico que almacena o transmite información
- Por ejemplo:
  - Empleados del Sistema de Salud (Health System)
  - Empleados de la Faculty Group Practice
  - Empleados de la David Geffen School of Medicine
  - Personal del campus que trabaja en áreas clínicas
  - Personal administrativo con acceso a información PHI
  - Voluntarios
  - Estudiantes que trabajan con pacientes
  - Personal de investigación e investigadores
  - Personal de Contabilidad / Nómina salarial (Accounting / Payroll)
  - Casi **todos** – ¡en algún momento!

---

## Responda a estas preguntas

**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

¿Por qué es importante mantener la privacidad y la seguridad?

¿Cuándo debe usted:

- ver la información PHI?
- usar la información PHI?
- compartir la información PHI?

**Respuesta: Sólo cuando se requiere para el tratamiento, pago u operaciones de atención de la salud, o cuando las leyes lo permiten o lo requieren.**

---

### Responda a estas preguntas

**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. Informando de sospechas de incidentes de seguridad
- d. Todas las opciones anteriores

---

### HIPAA – Situación 1

*Yo trabajo en admisiones. Una amiga que trabaja en la sala de emergencia (ER) me dijo que vio a una famosa estrella de cine en el elevador. Mi amiga leyó en el diario que la estrella de cine tiene cáncer y me pidió que averiguara en qué piso está, ya que sabemos en qué pisos se da tratamiento a los pacientes de cáncer.*

**Hágase estas preguntas:**

- ¿Necesita saber en qué piso está la estrella de cine para hacer su trabajo?
- ¿Tiene su amiga necesidad de saber si la estrella de cine tiene cáncer para hacer su trabajo?
- ¿Querría usted que gente desconocida tuviera acceso a sus datos privados?

## Responda a estas preguntas

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.

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 disparaba 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

---

## HIPAA – Situación 2

*Soy empleada de archivos médicos. Mientras abría informes de laboratorio, vi los resultados de la prueba de embarazo de mi gerente. ¡El resultado era positivo! Esa noche, en una fiesta, la vi con algunos amigos, y la felicité por el embarazo. Después me enteré de que no sabía los resultados de la prueba. ¡Yo fui la primera en decírselo! -- ¿Hice bien?*

### Pregúntese:

- ¿Necesitaba leer los resultados de laboratorio para hacer su trabajo?
- ¿Es su tarea dar información a los pacientes sobre su salud, aunque la persona sea amiga o compañera de trabajo?
- ¿Es su tarea informar a otras personas sobre los resultados de las pruebas de una persona?
- ¿Debe un empleado de la Universidad mirar los datos médicos de otro empleado si eso NO es necesario para realizar sus tareas?
- ¿Cómo se sentiría si esto le hubiera sucedido a usted?

**No mire, lea, use o cuente a otros la información PHI de una persona, a menos que sea parte de su trabajo.**

## Responda a estas preguntas

**14. 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 usted?**

- a. Se trata de un médico, 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 la UC.
- d. Ninguna de las opciones anteriores.

**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.

## Recordatorios

- **Usarlo solamente si es necesario para hacer su trabajo**
- **Usar el mínimo necesario para hacer su trabajo.**
- **Seguir las políticas y procedimientos de UCLA Medical Sciences o del campus de UCLA en lo referente a confidencialidad y seguridad de la información.**

## Las violaciones de HIPAA pueden tener sanciones—

- **Sanciones penales**
  - Multas de \$50,000 a \$250,000
  - Hasta 10 años de prisión
- **Sanciones civiles monetarias**
  - Multas de \$100 a \$25,000/año
  - Más dinero si hay violaciones en múltiples años
- **Multas y sanciones – Violación de leyes estatales**
  - El personal puede ser multado por cada violación y se le puede notificar al consejo de concesión de licencias si corresponde

- Medidas correctivas y disciplinarias de UCLA
  - Sanciones que pueden llegar hasta la pérdida de privilegios y la pérdida del empleo

## **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

### **Los pacientes pueden tener problemas con...**

- Que se les pida **decir en voz alta** ciertos tipos de información confidencial o personal
- **Oír conversaciones** acerca de información PHI por parte del personal que cumple sus tareas
- Que se les pregunten sus datos privados en “**voz alta**” en lugares públicos, en
  - clínicas, salas de espera, áreas de servicio
  - pasillos, elevadores, vehículos de transporte, en la calle

## **Protección de la privacidad: Intercambios verbales**

- Los pacientes pueden considerar que las operaciones clínicas normales violan su privacidad (*divulgación incidental*)
- Pregúntese: “**¿Qué pasaría si fueran mis datos los que se están discutiendo en este lugar o de esta manera?**”

## **Divulgaciones incidentales y la ley HIPAA**

- “**Incidental**”: Un uso o divulgación que no puede razonablemente evitarse, tiene carácter limitado y ocurre como consecuencia de un uso o divulgación permitida. (§164.502(c)(1)(iii))
  - Ejemplo: discusiones durante los turnos de enseñanza; llamar a un paciente por su nombre en la sala de espera; hojas de entrada en hospitales y clínicas.

## Responda a estas preguntas

**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 telefónicos 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 del 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 tener información en el teléfono móvil que no cause problemas si se coloca en un sitio público.
- d. Todas las opciones anteriores.

---

## Divulgaciones incidentales y la ley HIPAA

- Los usos y divulgaciones incidentales están permitidos, siempre y cuando se utilicen medidas de seguridad razonables para proteger la información PHI y que se apliquen los estándares mínimos necesarios.
- ¡Esto suele ser malentendido por los pacientes!

## La información se puede perder...

---

### Responda a estas preguntas

Por favor marque la mejor respuesta con un signo de ✓.

**17. El acceso a cualquier sitio de Internet puede rastrearse para obtener su nombre y el lugar donde se encuentra.**

- a. Verdadero
- b. Falso

## Tenemos que proteger todo el ciclo de información PHI

- Entrada/creación
- Almacenamiento
- Destrucción
- Para cualquier formato

**Los recipientes trituradores de papel funcionan mejor cuando se pone el papel dentro del recipiente. Si el papel está fuera del recipiente, se transforma en:**

- × Chismes
- × Basura
- × Material público

## La información PHI electrónica también se puede perder o ser robada

- Laptops, PDA, teléfonos celulares perdidos o robados
- Discos zip, CD, disquetes, unidades flash perdidos o robados
- Los sistemas no protegidos fueron penetrados por hackers
- Envíos de correo electrónico a la dirección o a la persona equivocada (el mismo problema ocurre con el fax)
- El usuario no ha salido del sistema

**Sea consciente de que la información ePHI está por todas partes**

---

### Responda a estas preguntas

Por favor marque la mejor respuesta con un signo de √.

**18. De Florida (febrero de 2005): Un archivo adjunto a un correo electrónico con una lista no encriptada de pacientes de VIH fue enviado 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. Un oficial de Seguridad de Computación debe notificar a los 10 receptores y solicitarles borrar el archivo. 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.

**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. NO puede discutir ninguna información PHI con nadie, a menos que su trabajo lo requiera.

## “Buenas Prácticas de Computación” 10 protecciones para los usuarios

- Contraseñas
- Bloqueo de la pantalla
- Seguridad de la estación de trabajo
- Dispositivos portátiles
- Manejo de datos
- Antivirus
- Seguridad de Computación
- Correo electrónico
- Uso seguro de Internet
- Informar de los incidentes/violaciones de seguridad

## Buenas Prácticas de Computación #1 Contraseñas

Utilice contraseñas crípticas que no puedan adivinarse fácilmente, y protéjalas – no las escriba ni las comparta con nadie.

## “Buenas Prácticas de Computación” #2 Bloquee la pantalla

### Para una PC ~

- <ctrl> <alt> <delete> <enter>
- o
- <img alt="Windows logo" data-bbox="118 818 148 831"> <L>

### Para una Mac ~

- Configurar el salvapantallas con su contraseña      Crear un atajo para activar el

salvapantallas

- Usar una contraseña para arrancar o despertar su computadora.

### Buenas Prácticas de Computación #3 Seguridad de estaciones de trabajo

#### ❖ **Asegure físicamente el área y los datos cuando estén desatendidos**

### Buenas Prácticas de Computación #4 Seguridad de dispositivos portátiles

#### ❖ **No guarde 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!

#### **Copias de seguridad de los datos, pregúntese...**

- ¿Qué eficacia tendría usted si su correo electrónico, documentos de procesamiento de textos, hojas de cálculo de Excel y su base de datos de contacto fueran borrados?
- ¿Cuántas horas le llevaría reconstruir esa información?

### Buenas Prácticas de Computación #5 Manejo de datos

#### **Manejo de datos confidenciales**

- Saber dónde están guardados los datos.
- Destruir datos confidenciales que ya no se necesitan ~
  - **Triturar** o destruir de otra forma los datos confidenciales antes de deshacerse de ellos

- **Borrar/desmagnetizar** los datos antes de desecharlos o de reutilizar unidades de almacenamiento
- Proteger los datos confidenciales que mantiene ~
  - **Hacer una copia de seguridad** de los datos en un servidor departamental

## Buenas Prácticas de Computación #6 Antivirus

**Asegúrese de que su computadora tenga antivirus y todos los parches de seguridad necesarios.**

## Buenas Prácticas de Computación #7 Seguridad de Computación

**No instale programas desconocidos o no solicitados en su computadora**

## Buenas Prácticas de Computación #8 Correo electrónico

### **Practique el correo electrónico seguro**



No abra, reenvíe ni conteste mensajes de correo electrónico sospechosos



No abra archivos adjuntos sospechosos ni haga clic en direcciones de sitios webs desconocidos



Borre el spam





Antes de enviar mensajes electrónicos a los pacientes, confirme que el registro del paciente contenga el consentimiento para recibir correo electrónico.

## Buenas Prácticas de Computación #9 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 definir 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!

## Buenas Prácticas de Computación

### #10 Informar de los incidentes/violaciones de seguridad

**¿Cómo informar de los incidentes/violaciones de seguridad?** Informe de las pérdidas o robos de laptops, blackberries, PDA, teléfonos celulares, unidades flash, etc...

La pérdida o robo de cualquier dispositivo de computación **DEBE** reportarse inmediatamente al Departamento de Policía de UCLA. **Marque el 1-310-825-1491**

√ 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 se aplica también a las pérdidas o robos de información PHI en formato físico (papel, películas, etc.).

√ Si no se protege el acceso/uso/divulgación no autorizados se podrían imponer sanciones de hasta \$25,000 por paciente.

√ Puede también ponerse en contacto con el Oficial de Seguridad de Información de Medical Sciences.

Ann S. Chang, CISSP  
achang@mednet.ucla.edu  
(310) 825-7003

---

### Responda a estas preguntas

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

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

## RECURSOS

### ...Privacidad y Confidencialidad

- Su Supervisor/Gerente
- Oficina de Privacidad: (310) 835-7135  
Director de Privacidad: Carole A. Klove, RN, JD  
Correo electrónico: [cklove@mednet.ucla.edu](mailto:cklove@mednet.ucla.edu)
- Sitio web de HIPAA: <http://pmo.mednet.ucla.edu/>
- Investigación de HIPAA en UCLA: <http://oprs.ucla.edu/human/forms/HIPAA>
- Sitio web de UCOP HIPAA: <http://www.universityofcalifornia.edu/hipaa>

### ...Seguridad de la información

- Su Supervisor/Gerente
- La persona encargada de IT o CSC en su departamento
- Sitio web de HIPAA:  
<http://pmo.mednet.ucla.edu/>
- Oficial de Seguridad de Información de UCLA Medical Sciences:  
Ann S. Chang  
[achang@mednet.ucla.edu](mailto:achang@mednet.ucla.edu)  
(310) 825-7003



### Recordatorios sobre la seguridad de HIPAA

- |  |  |
|--|--|
| √ Proteja su computadora con una contraseña              | √ Mantenga la oficina segura   |
| √ Haga copias de seguridad de la información electrónica | √ Guarde los discos bajo llave   |
| √ Envíe mensajes de correo electrónico de forma segura   | √ Ejecute el programa antivirus <ul style="list-style-type: none"><li>○ Software antispam</li><li>○ Software antispyware</li></ul> |