Capacitación sobre Privacidad y Seguridad de la Información

Para:

CDPH Programa Comunitario de Pruebas Rápidas

Presentado por:

Departamento de Salud Pública

de California

Junio 2023

Temas de privacidad y seguridad de la información

Esta capacitación abordará lo siguiente:

- Clasificaciones de información
- Privacidad de la información
  - Leyes y normas de privacidad estatales y federales
  - Mínimo necesario
  - Uso y divulgación de PHI y PII
- Seguridad de la información
  - Medidas de seguridad administrativas
  - Medidas de seguridad físicas
  - Medidas de seguridad técnicas
- Incidentes de seguridad de la información y violaciones de privacidad
- Sanciones

Clasificaciones de Información

Clasificaciones de Información

Toda la información no es igual. A los fines de la seguridad y privacidad de la información, la información del Programa de Pruebas podría clasificarse de la siguiente manera:

- **Información que permite la identificación personal (Personally Identifiable Information, PII):** esta es información que identifica o describe a una persona. Los ejemplos incluyen nombre, fecha de nacimiento, número de seguro social, número de cuenta financiera, información médica identificable individualmente, raza, sexo, resultados de la prueba de COVID-19, etc.
- **Información confidencial**: solo personas autorizadas pueden tener acceso a la información. Se trata de información guardada por el Programa de Pruebas que está *exenta de divulgación*. Algunos ejemplos incluyen comunicaciones con el asesor legal.
- **Información pública**: información sobre el Programa de Pruebas y sus servicios que puede compartirse con todos. *Solo la gerencia de Departamento de Salud Pública de California (California Department of Public Health, CDPH) o la Oficina de Servicios Legales pueden determinar si la información es pública.*

La mayor parte de la **información confidencial** a la que accederá se considera información **personal**.

Si no está seguro de si la información es confidencial, trátela como tal hasta que la gerencia del CDPH o la Oficina de Servicios Legales lo informen lo contrario.

Privacidad de la Información

Privacidad de la Información

- Los problemas de privacidad existen en cualquier lugar y en cualquier momento en que se recoja, almacene o difunda **información personal** o **confidencial**. La privacidad es una preocupación, ya sea electrónica, verbal o física.

- Los problemas de privacidad de la información pueden surgir de una amplia gama de fuentes, incluida la información recopilada en Primary o mientras se evalúan personas.

- El desafío en la privacidad de la información es recopilar, almacenar y difundir información relacionada con las pruebas de COVID-19 mientras se protege la **información personal** y **confidencial**.

Leyes y Normas de Privacidad Estatales y Federales

- Las leyes y normas de privacidad se encuentran a nivel federal, estatal y local.

- El Programa de Pruebas del CDPH se rige principalmente por la Ley de Prácticas de Información (Information Practices Act, IPA) (sección 1798 del Código Civil de California, y siguientes) y la política estatal (sección 5300 del Manual Administrativo del Estado).

- El Programa de Pruebas no está cubierto por la Ley de Portabilidad y Responsabilidad de los Seguros Médicos (Health Insurance Portability and Accountability Act, HIPAA) de 1996. Sin embargo, su organización y parte de la información que usted posee podrían estarlo.

- La conclusión es que, independientemente de si la información está cubierta por la IPA, la HIPAA o la Ley de Privacidad y Derechos Educativos de la Familia (Family Educational Rights and Privacy Act, FERPA), la privacidad y protección de la **información personal** y **confidencial** es de suma importancia.

Ley de Prácticas de Información

- La Ley de Prácticas de Información (IPA) establece requisitos para todas las agencias estatales para la recopilación, el mantenimiento y la difusión de **información personal**.
- La IPA se estableció en 1977 y es una ley estatal para proteger la **información personal**, incluida la información médica.
- **Recuerde: la información médica incluye (¡pero definitivamente no se limita a!) los resultados positivos y negativos de la prueba para la detección de la COVID y si alguien es vacunado.**
- La IPA exige que se mantenga la confidencialidad de la **información personal**.

Información Personal en Virtud de la IPA

- **La información personal (Personal Information, PII)** es cualquier información mantenida por una agencia que identifica o describe a una persona. Algunos ejemplos incluyen:
  - Nombre.
  - Número de seguro social.
  - Información médica o información que implique una afección médica.
  - Información financiera (número de cuenta, débito o número de tarjeta de crédito, en combinación con cualquier código de seguridad, código de acceso o contraseña requeridos que permitirían el acceso a la cuenta financiera de una persona).
  - Número de licencia de conducir o número de tarjeta de identificación de California.
  - Información del seguro médico (puede incluir la fecha de nacimiento).
  - Declaraciones hechas por la persona o atribuidas a esta.
  - Dirección particular.
  - Número de teléfono particular.

Descripción General de la HIPAA

- La HIPAA es una reglamentación federal que protege la confidencialidad y la seguridad de la **información médica protegida (protected health information, PHI).** La HIPAA incluye normas de privacidad y seguridad.
- La HIPAA crea y protege los derechos de privacidad individuales para la **PHI** y regula el uso y la divulgación de esa información.
  - **La PHI** es “información médica que permite la identificación individual” en cualquier forma o medio, ya sea electrónico, en papel u oral, que se relaciona con lo siguiente:
    - La salud o afección física o mental pasada, presente o futura de la persona. O
    - la prestación de atención médica a la persona.
- Cuando existen leyes estatales o federales más estrictas para un programa específico con respecto al uso y la divulgación de la **PHI**, se deben cumplir esas leyes más estrictas.
- La siguiente diapositiva explica por qué hablamos sobre la HIPAA cuando la IPA rige el Programa de Pruebas.

Descripción General de la HIPAA (continuación)

- Como se indicó anteriormente, el Programa de Pruebas del CDPH no se rige por la HIPAA.

- La Oficina de Privacidad del CDPH ha realizado un análisis de los servicios prestados por el Programa de Pruebas y ha determinado que no se incluyen en la definición de "programa cubierto" establecida en la HIPAA. Por lo tanto, no se aplica la HIPAA.

- Sin embargo, varios conceptos dentro de la HIPAA, como la PHI (analizada anteriormente) o el mínimo necesario (analizado a continuación), son conceptos que debe comprender para poder usar, mantener y ayudar al CDPH a controlar de manera eficaz el intercambio indebido de información personal de las personas.

PII Frente a PHI

- La información de identificación personal (PII) y la información médica protegida (PHI) pueden parecer similares en la superficie, pero las distinciones clave los distinguen.
- Si bien la PII es un término general para cualquier información que pueda relacionarse con la identidad de una persona, la PHI se aplica específicamente a las entidades cubiertas por la HIPAA que poseen información médica identificable.
- La PII incluye, entre otros, números de Seguro Social, números de pasaporte, números de licencia de conducir, direcciones, direcciones de correo electrónico, fotos, datos biométricos o cualquier otra información que pueda rastrearse a una persona. La información médica, educativa, financiera y de empleo se incluye en la PII.
- Debido a que muchos socios del Programa de Pruebas pueden tener acceso tanto a la PHI como a la PII, todos los datos se tratan de la misma manera para agilizar los procesos.

Mínimo Necesario

El mínimo necesario es un concepto para garantizar que la **PHI** esté limitada en su uso y divulgación para minimizar los riesgos de seguridad. El acceso a la **PHI o PII** debe limitarse a la cantidad más pequeña necesaria para hacer su trabajo, lo que incluye:

- **Solicitud de la cantidad mínima de información necesaria.**
- **Uso de la cantidad mínima de información necesaria.**
- **Divulgación de la cantidad mínima de información necesaria.**

Mínimo Necesario (continuación)

- **RECORDATORIOS IMPORTANTES**:
  - Cuando envíe una solicitud de asistencia técnica al CDPH o Primary.Health, envíe solo la información mínima necesaria para expresar su inquietud.
  - **Los códigos QR** de las tarjetas de prueba de BinaxNOW se utilizan para identificar a las personas y proteger la PII.
  - **No** incluya ninguna información personal en las tarjetas de prueba, los mensajes de texto ni los correos electrónicos, incluidos el nombre, la fecha de nacimiento o la captura de pantalla que contenga PII.

Mínimo Necesario (continuación)

Recuerde, en caso de duda, pregunte al coordinador del centro de Pruebas del CDPH si no está seguro de que la divulgación esté permitida.

Intercambio interno de PII

- Solo comparta **PII** con otras personas en el Programa de Pruebas si la requieren para sus operaciones.
- **La PII** puede compartirse con asociados comerciales internos cuando se colabora con operaciones, p. ej., asuntos legales, contabilidad, auditorías e investigaciones.
- **NUNCA** reenvíe ni comparta números de Seguro Social.

Uso y Divulgación de PHI y PII

- **El uso** es compartir, aplicar, utilizar, examinar o analizar la **PHI** y la **PII**.
- **La divulgación** es la divulgación, transferencia, provisión de acceso o divulgación de cualquier otra manera de **PHI** e **PII** fuera del programa que contiene la información.
- Todos deben asegurarse de que la **PHI**, **la PII** y la **información confidencial** no se divulguen a entidades externas en violación de las leyes/reglamentaciones federales o estatales, ni de las políticas del CDPH.
- Si se solicita a un centro de pruebas que divulgue información personal a personas que no sean quienes pertenecen a la información, y ellos o sus gerentes están preocupados por la divulgación, deben comunicarse inmediatamente con el CDPH a CommunityRapidTesting@cdph.ca.gov y con la Oficina de Privacidad a privacy@cdph.ca.gov para obtener más orientación.
- **Las divulgaciones de datos que no sean de rutina deben ser aprobadas por el responsable de privacidad del CDPH y el responsable de seguridad de la información por escrito.**

Divulgación de PHI e Información Personal

- **Regla general**: no divulgue ninguna **PHI** ni **PII** a ninguna entidad externa a menos que lo apruebe el CDPH.
  - "Entidad externa" es cualquier persona a quien no pertenece la información personal.
    - Esto incluye al personal que no forme parte del Programa de Pruebas o que no tenga una necesidad comercial de acceder a la información.
  - Consulte a su gerente antes de divulgar dicha información o cuando tenga alguna pregunta.
  - Si no está seguro, no intente determinar si la información puede compartirse. Consulte a su gerente.

- **Divulgaciones comunes requeridas:** existen casos en los que se **requiere la divulgación de** PHI **o** PII, incluidos los siguientes:
  - A la persona a quien pertenece el registro; o al padre/la madre, el tutor, el guarda o el representante autorizado
  - Con autorización/consentimiento voluntario previo por escrito

Seguridad de la Información

Medidas de Seguridad Administrativas

Las medidas de seguridad administrativas incluyen políticas y procedimientos documentados para las operaciones diarias, la gestión de la conducta del personal, el acceso a los sistemas de información automática del Estado y a los dispositivos relacionados y la gestión de la selección, el desarrollo y el uso de controles de seguridad.

Medidas de Seguridad Físicas

- **Las medidas de seguridad físicas** son medidas de seguridad destinadas a proteger los sistemas de información electrónica y la información confidencial (de cualquier forma), así como los edificios y equipos relacionados con estas, de peligros naturales, peligros ambientales e intrusiones no autorizadas. Cuando se autoriza el trabajo remoto, las medidas de seguridad físicas son similares a proteger su propia casa o posesiones.
- Algunos ejemplos de medidas de seguridad físicas son:
  - Identificar a todos los empleados y visitantes.
  - Cerrar con llave los cajones, los gabinetes, las salas y los edificios.
  - Cerrar con llave las puertas y ventanas cuando no se encuentren en su hogar.
  - Destruir la información confidencial.
  - Tener precaución al imprimir, enviar por fax y correo electrónico.
  - Proteger los dispositivos informáticos móviles contra robos y usos indebidos.

Áreas Sin Supervisión

- **<u>Nunca</u>** debe dejar **sin supervisión información personal** o *confidencial*, donde personas no autorizadas puedan acceder a ella, incluso durante unos minutos, incluso durante el horario de trabajo.

- Otra persona autorizada para ver la información puede observar su información personal o confidencial si se encuentra en el área inmediata.

Asegurar la Información

- **La información personal y confidencial** DEBE protegerse fuera del horario de trabajo, incluso si el edificio es seguro. Por ejemplo:
  - Coloque los documentos en un cajón bajo llave o en un archivador bajo llave.
  - No deje información personal o confidencial sin seguridad en su oficina, a menos que esta esté bloqueada.
  - No deje información personal o confidencial visible encima o debajo de su escritorio.
  - No deje las llaves en gabinetes, cajones o puertas de oficina en un escritorio o en un lugar obvio.
  - **RECUERDE**: Esto incluye su escritorio y oficina en su casa si realiza teletrabajo.

Asegurar la Información (continuación)

- Los documentos en papel corren un mayor riesgo que los archivos electrónicos de ser violados porque no pueden ser cifrados.
  - **Nunca** imprima documentos ni retire documentación fuera del sitio a menos que sea absolutamente necesario.
  - **Nunca** tome notas manuscritas a menos que sea absolutamente necesario.
  - Los documentos deben triturarse o colocarse en un recipiente de destrucción confidencial cerrado lo antes posible cuando ya no sean necesarios.
  - Los documentos relacionados con el trabajo deben mantenerse separados de cualquier documento personal.
- Cuando se deje la información o los documentos sin supervisión, guárdelos en armarios cerrados, cajones cerrados o salas cerradas con llave. **No** deje la información sin supervisión en vehículos u otros lugares donde pueda verse o robarse.

Destrucción Confidencial

Cuando ya no necesite la **información personal o confidencial** para fines comerciales, tiene algunas opciones para eliminar/destruir esta información.

- **Documentos físicos**
  - Triture inmediatamente los documentos usted mismo.
  - Utilice recipientes de destrucción cerrados y confidenciales.
- **Documentos electrónicos**
  - Realice una eliminación o limpieza segura de la información.

No deseche **información personal o confidencial** en su hogar, fuera de su departamento o en cestos de basura/cestas de basura a menos que se trituren. Si no tiene una trituradora, no cree documentos en papel.

Los documentos confidenciales destruidos no deben almacenarse en cajas en cubículos u oficinas de los empleados.

Correo Electrónico/mensaje de Texto con Información Personal o Confidencial

- Verifique las direcciones de correo electrónico/números móviles de todos los destinatarios antes de enviarlos.

- Si descubre que envió el correo electrónico o mensaje de texto a la dirección de correo electrónico incorrecta, informe de inmediato el incidente a su supervisor e infórmelo a la oficina de privacidad y seguridad si el correo electrónico o mensaje de texto contiene PHI o PII, de modo que el abogado encargado de la privacidad pueda determinar si es necesario enviar por correo una carta de notificación de incumplimiento a las personas posiblemente afectadas. Los formularios pueden ser proporcionados por la oficina de privacidad.

Medidas de Seguridad Para la Comunicación Verbal

- Tome las medidas razonables para proteger la privacidad de todos los intercambios verbales o las conversaciones de **información personal** o **confidencial**, independientemente del lugar donde se lleve a cabo la conversación.
- Encuentre oficinas adjuntas para analizar **información personal** o **confidencial**.
- No hable sobre **información personal** o **confidencial** con familiares o amigos.
- No hable sobre **información personal** o **confidencial** con personas que no necesitan conocerla para un propósito comercial válido, incluso si trabajan con usted.
- Verifique la identidad y autoridad de las personas con las que intercambia información verbalmente.
- No hable sobre la **información personal** o **confidencial** de una persona con sus familiares o amigos.

Seguridad de los Dispositivos Móviles

- Los dispositivos móviles incluyen computadoras portátiles, tabletas, computadoras portátiles, dispositivos de almacenamiento USB, memoria flash y teléfonos celulares.
- Si utiliza su propio dispositivo móvil para fines de Programa de Pruebas asegúrese de que esté protegido con contraseña o cifrado de alguna manera.
- Al sacar los dispositivos móviles de las instalaciones del lugar de trabajo (lo que incluye su hogar si cuenta con autorización para trabajar de forma remota), no deben estar separados de los empleados de aeropuertos, automóviles, habitaciones de hotel, etc.
- Cuando los dispositivos móviles se sacan de las instalaciones del lugar de trabajo:
  - No deje dispositivos móviles sin supervisión.
  - Cuando no se utilice, asegure todos los dispositivos móviles.
  - El cable bloquea una computadora portátil en una superficie inmóvil.

Medidas de Seguridad Técnicas

- **Las medidas de seguridad técnicas** son medidas de seguridad que especifican cómo usar la tecnología para proteger la información recopilada, almacenada y transmitida, en particular al controlar el acceso a ella.

Seguridad del Correo Electrónico

- Siempre revise las direcciones de correo electrónico para garantizar la entrega a destinatario(s) previstos.
- No reenvíe PHI o PII a una cuenta de correo electrónico personal.
- No envíe mensajes de correo electrónico que contengan **información personal** o **confidencial**, incluso si es a otra dirección de correo electrónico de otra entidad gubernamental

Seguridad del Correo Electrónico (continuación)

- Inserte una declaración de confidencialidad al final de su correo electrónico.

- Ejemplo de una declaración de confidencialidad:
  - *AVISO DE CONFIDENCIALIDAD: Esta comunicación con su contenido puede contener información confidencial y/o legalmente privilegiada. Solo se utiliza para el/los destinatario(s) previstos. Se prohíbe la intercepción, revisión, uso o divulgación no autorizados y pueden violar las leyes aplicables, incluida la Ley de Privacidad de las Comunicaciones Electrónicas. Si usted no es el destinatario previsto, comuníquese con el remitente y destruya todas las copias de la comunicación. Su recepción de este mensaje no pretende anular ningún privilegio aplicable.*

Contraseñas

- Usted es responsable de la confidencialidad y seguridad de sus contraseñas. Usted debe:
  - Cambie la contraseña al menos cada 60 días, o antes si sospecha que ha sido comprometida.
  - No comparta ni anote su contraseña.
  - No incluya su contraseña en un archivo de datos, script de inicio de sesión o macro.
- Cree una contraseña “segura” evitando referencias comunes como el nombre de su pareja, el nombre de su mascota, el cumpleaños, el color favorito, los números/dedos secuenciales (abc, 123, 5555), fácil de adivinar, etc.
  - No utilice una palabra en el diccionario.
  - Tener una contraseña única para cada inicio de sesión y no usar la misma contraseña para varios sistemas.
  - Use una contraseña con un número impar de caracteres, de al menos nueve dígitos de longitud, con al menos:
    - Una letra mayúscula y una letra minúscula
    - Un número
    - Un carácter único como !@#$%^&*()

Informe de inmediato a su supervisor y CDPH cualquier sospecha de uso no autorizado de una contraseña.

Equipos Informáticos

- Use Ctrl-Alt-Eliminar, Windows-L o una tecla de bloqueo para bloquear la pantalla de su computadora antes de dejarla sin supervisión.

- Almacenar los archivos en un servidor o en una unidad compartida porque se hace una copia de seguridad. No almacene información o archivos en escritorios.

- No use equipos informáticos para ningún propósito no autorizado.

Dispositivos Informáticos Móviles

- No descargue ni almacene **información personal** o **confidencial** en dispositivos móviles a menos que haya obtenido permiso por escrito para hacerlo. Si está permitido, solo descargue o almacene la cantidad mínima de información **personal** o **confidencial** necesaria en dispositivos móviles.
- No acceda a Primary.Health ni a otras plataformas del Programa de Pruebas desde su dispositivo móvil, a menos que se encuentre en su lugar de pruebas o en una zona de trabajo designada.
- Asegúrese de cerrar siempre la sesión de todas las plataformas del Programa de Pruebas cuando no las use activamente.
- **NUNCA** descargue ni almacene números de seguro social en dispositivos móviles.

¡No Sea el Eslabón más Débil!

- Históricamente, los departamentos estatales y sus contratistas han sufrido incumplimientos que involucraron pérdidas o robos. **Esté atento con computadoras o dispositivos móviles emitidos por el estado o cualquier computadora o dispositivo móvil en el que se realice el trabajo estatal.**
  - No descargue archivos personales en computadoras o dispositivos móviles emitidos por el estado.
  - No verifique las cuentas de correo electrónico personales en computadoras o dispositivos móviles emitidos por el estado.
  - No utilice redes inalámbricas no seguras.
  - Si tiene un blog, un sitio web de redes sociales, etc., no publique **información personal** o **confidencial sobre el** Programa de Pruebas , incluso cuando esté en su casa.

Acceso Remoto

Acceso Remoto

- El acceso remoto implica el uso de una computadora externa (p. ej., doméstica, hotel) para acceder al correo electrónico, los documentos y las aplicaciones del Programa de Pruebas.
- El acceso remoto se utiliza con mayor frecuencia después del horario de atención, cuando se viaja o cuando se realiza teletrabajo/trabajo desde el hogar.
- No debe acceder a la información del Programa de Pruebas de forma remota, a menos que el Programa de Pruebas lo haya autorizado a hacerlo.

Riesgos e Inquietudes del Acceso Remoto

- Las áreas de preocupación incluyen:
  - Medios, dispositivos o documentos impresos perdidos o robados.
  - Eliminación incorrecta de medios y documentos impresos.
  - Software malicioso en una computadora personal que roba información.
- Exposición inadecuada o divulgación de **información personal** o **confidencial** a terceros, como visitantes de su hogar, que puede desencadenar leyes estatales o federales de notificación de violaciones.
- Las violaciones de las políticas del Programa de Pruebas también pueden derivar en medidas disciplinarias y el despido del programa de pruebas de antígenos.

Descargar Peligros

- Minimice la descarga o la realización de pruebas **personales** o **información confidencial** del centro de pruebas.
- No descargue **información personal** o **confidencial del Programa de Pruebas** en computadoras personales o dispositivos móviles. Esto incluye transferir información a través de unidades flash, CD, etc.
- No envíe por correo electrónico ni publique **información personal** o **confidencial del Programa de Pruebas** a cuentas de correo electrónico personales, redes sociales u otras aplicaciones, medios o sistemas de programas que no sean parte del Programa Prueba.
- No envíe por correo electrónico capturas de pantalla con PII/PHI a nadie, incluidos los empleados de CDPH.
- Si no está seguro de qué está permitido, consulte a su supervisor inmediato y al CDPH.

Seguridad Informática

Por lo general, las computadoras personales no cuentan con todas las protecciones contra el software malicioso que tiene su computadora estatal. Si está disponible, se recomienda el uso de una computadora portátil administrada y emitida por el departamento si accede a información personal o confidencial a través del acceso remoto.

- Si usa una computadora doméstica para el acceso remoto, asegúrese de que:
  - El software antivirus está actualizado y configurado para actualizarse al menos una vez al día.
  - Los parches de seguridad se instalan mensualmente.
  - El software o hardware de firewall esté instalado
- Para computadoras de propiedad personal, configure la instalación automática o la notificación de parches de seguridad, y asegúrese de actualizar el software como Adobe Acrobat y su navegador de Internet mensualmente.
- No utilice redes inalámbricas no seguras.
- Si sospecha que alguien ha visto su contraseña o lo ha observado ingresarla, cambie de inmediato su contraseña.

¡No olvide bloquear su pantalla cuando esté lejos de la computadora, incluso cuando trabaje desde su casa!

Seguridad Informática (continuación)

- No confíe en ninguna persona que reclame autoridad para acceder a su información o contraseña. Las contraseñas nunca deben compartirse.
- No haga clic en enlaces o archivos adjuntos en correos electrónicos a menos que esté esperando el correo electrónico o pueda validar que es auténtico. No haga clic en enlaces a menos que estén relacionados con el trabajo y sean necesarios para hacerlo... el sitio web puede ser falso.
- Las políticas y los controles de seguridad de acceso remoto protegen la información del Programa de Pruebas y evitan las violaciones de la ley estatal y federal. Ignorar, deshabilitar o trabajar cerca de controles o políticas de seguridad y privacidad pueden ser causales de medidas disciplinarias y despido del programa.
- No permita que una organización privada de soporte técnico tenga acceso a control remoto de su PC o computadora portátil iniciada en los portales de información del Programa de Pruebas.
- Si se sospecha una violación de la seguridad, informe de inmediato a CommunityRapidTesting@@cdph.ca.gov y a la Oficina de Seguridad de la Información de CDPH (CDPH.InfoSecurityOffice@cdph.ca.gov).
- Si sospecha que una persona no autorizada vio la información personal o confidencial del Programa de Pruebas, notifique a CommunityRapidTesting@cdph.ca.gov y notifique a la Oficina de Privacidad del CDPH (Privacy@cdph.ca.gov).

Incidentes de Seguridad de la Información y Violaciones de Privacidad

Incidentes de Seguridad de la Información

- Un incidente de **seguridad de la información** es un suceso real o presunto de daño, destrucción, acceso no autorizado o divulgación de equipos o información. Esto incluye robo, intento de robo o pérdida de equipos o dispositivos con PII o PHI en ellos (computadoras portátiles, teléfonos celulares, etc.); o información, así como fraude, uso indebido o uso inapropiado de propiedad estatal. Además, la detección de un virus informático o la piratería en una computadora estatal también se considera un incidente.
- **En pocas palabras**: el robo o la pérdida de cualquier información, equipo o dispositivo del Programa de Pruebas es un incidente de seguridad y debe informarse de inmediato a la Oficina de Seguridad de la Información (ISO) del CDPH.
- La ISO determinará si la computadora contenía **información personal** o **confidencial**. Si hubiera información de este tipo, el incidente también podría clasificarse como una violación de la privacidad.
- Cuando se sospeche de una violación de privacidad, la ISO se elevará a la Oficina de privacidad del CDPH. Si bien los incidentes de seguridad de la información y las violaciones de privacidad son similares, existen diferencias en el proceso de escalamiento y los requisitos de informe.

Informe de Incidentes de Seguridad

El CDPH tiene una notificación específica y procesos de presentación de informes cuando se producen incidentes de seguridad de la información. Tan pronto como sepa que se ha producido o puede haber ocurrido un incidente, informe a su gerente/supervisor, quien notificará a las personas necesarias.

Informe la siguiente información a su gerente/supervisor:

- Su nombre y cargo
- Centro de pruebas al que está ayudando
- Su número de teléfono de contacto
- Su dirección física

Además, según corresponda al incidente, debe informar lo siguiente:

- El equipo o dispositivo de TI perdido o robado
- Descripción de la información divulgada o consultada por una persona no autorizada
- Fecha en que se descubrió el incidente por primera vez y fecha en que se tomó la medida
- Cómo se llevó a cabo el incidente, si se conoce
- Qué evidencia está disponible para ayudar en la investigación y quién puede tener conocimientos adicionales
- Un número de informe policial, si se robó algún equipo estatal

Informe de Incidentes de Seguridad (continuación)

Su gerente/supervisor (o la persona designada) debe informar el incidente de inmediato y toda la información relevante al CDPH.

Después de que se informe, bajo la orientación de ISO, su gerente/supervisor trabajará con el CDPH para completar un formulario de informe de incidentes y un plan de medidas correctivas para la presentación en un plazo de 5 días. La acción correctiva detalla los pasos que tomó el Programa de Pruebas para mitigar o remediar el incidente. Las demoras en la presentación de informes, el manejo o la corrección de planes de acción dan lugar a la elevación de daños y al riesgo de pérdidas adicionales de la información que se confía en el Programa de Pruebas

Dirija cualquier pregunta relacionada con el informe de incidentes de seguridad de la información a:

- Dirección de correo electrónico ISO: CDPH.InfoSecurityOffice@cdph.ca.gov
- Teléfono ISO a través del Servicio de Asistencia de TI: 916-440-7000 o 800-579-0874.

Violaciones de Privacidad

Una violación de privacidad es una divulgación no autorizada de información personal o PHI en virtud de la Ley de Prácticas de Información de 1977, la Norma de privacidad de la HIPAA o la Política estatal.

Las violaciones de privacidad pueden ser orales, impresas o electrónicas y producirse cuando la información se transmite a un destinatario no autorizado o no intencionado.

Algunos ejemplos de incumplimientos incluyen:
Violaciones verbales: divulgar **información personal/PHI** de forma verbal a personas no autorizadas durante las llamadas telefónicas, de una manera no permitida por las leyes estatales o federales, que representa un riesgo significativo de daño financiero, de reputación u otro daño a la persona/el paciente afectado.

Violaciones de papel: los correos o faxes impresos mal dirigidos con **información personal/PHI**, la pérdida o el robo de documentos impresos que contienen **información personal/PHI**, los envíos de **información personal/PHI** a la persona incorrecta, o la impresión de **información personal/PHI** en el exterior de un sobre o visible a través de la ventana de un sobre.

Violaciones electrónicas: robo/pérdida de datos no cifrados, computadoras portátiles, discos duros, PC con **PHI/información personal**; robo/pérdida de datos digitales no cifrados con **PHI/información personal**; fax o correos electrónicos mal dirigidos con **PHI/información personal** que se enviaron a personas no autorizadas; intercambio no autorizado de **PHI/información personal** en las redes sociales; correos electrónicos no cifrados; intercambio de contraseñas; y piratería en bases de datos electrónicas.

Sanciones

Responsabilidad

- La Ley de Prácticas de Información (IPA) establece que una violación intencional de la IPA por parte de un empleado es causa de medidas disciplinarias, que pueden incluir hasta el despido. Solicitar u obtener un registro de **información personal** con engaños constituye una mala conducta, y usted puede recibir una multa de hasta **$5,000** y el encarcelamiento de hasta un año por hacerlo. Incluso si viola involuntariamente la IPA, una vez que se descubre la violación y la oficina de privacidad le ha indicado que cese cualquier medida que esté violando, debe tomar medidas inmediatas y cumplir con la solicitud.

- **Los directores, funcionarios y empleados** pueden ser responsables de sanciones penales. Es suficiente que conozcan los hechos que constituyen el delito, ya sea que sepan o no que la conducta fue contraria al estatuto o a las reglamentaciones.

Quejas por Violaciones de PHI/ información personal

- **Las personas tienen derecho a quejarse sobre una violación de las políticas de privacidad o de seguridad de la información, ya sea un paciente, un miembro de la fuerza laboral u otro asociado comercial.**

- CDPH prohíbe las represalias contra cualquier persona que presente una queja.

- Cualquier persona cuya **PHI/información personal** sea mantenida por un departamento puede presentar quejas sobre presuntas violaciones de la norma de privacidad de la IPA o de la HIPAA. Otras personas que pueden presentar quejas incluyen, entre otras, empleados, empleados asociados comerciales, destinatarios de servicios, defensores, abogados y denunciantes.

Resumen de los Conceptos Clave

- Los problemas de privacidad existen en cualquier lugar y en cualquier momento en que se recoja, almacene o difunda **información personal** o **confidencial**. La privacidad es una preocupación, ya sea electrónica, verbal o física.
- La Ley de Prácticas de Información (IPA) establece requisitos para todas las agencias estatales para la recopilación, el mantenimiento y la difusión de **información personal**.
- **El acceso mínimo necesario** a la **PII** debe limitarse a la cantidad más pequeña necesaria para hacer su trabajo
- Solo comparta **PII** con otras personas en el Programa de Pruebas si la requieren para sus operaciones.
- No divulgue ninguna **PHI** ni **PII** a ninguna entidad externa a menos que lo apruebe el CDPH

Medidas a Tomar en su Lugar de Trabajo

- **No** incluya ninguna información personal en las tarjetas de prueba, los mensajes de texto ni los correos electrónicos, incluidos el nombre, la fecha de nacimiento o la captura de pantalla que contenga PII o PHI.
- Tome medidas para proteger la privacidad de todos los intercambios verbales o discusiones de **información personal o confidencial**, independientemente del lugar donde se lleve a cabo la conversación.
- Si utiliza su propio dispositivo móvil para fines de Programa de Pruebas, asegúrese de que esté protegido con contraseña o cifrado de alguna manera.
- Cada vez que envíe mensajes de correo electrónico que contengan **información personal** o **confidencial**, incluso si se envían a otra dirección de correo electrónico de otra entidad gubernamental, el correo electrónico debe cifrarse.
- **En pocas palabras**: el robo o la pérdida de cualquier información, equipo o dispositivo del Programa de Pruebas es un incidente de seguridad y debe informarse a CommunityRapidTesting@cdph.ca.gov y a CDPH ISO CDPH.InfoSecurityOffice@cdph.ca.gov de inmediato.
- **La información personal y confidencial** DEBE protegerse siempre, incluso fuera del horario de trabajo.
- **Los documentos en papel corren un mayor riesgo que los archivos electrónicos** de ser violados. ¡Asegúrelos!