MedPro Group
a Berkshire Hathaway company

PEACE OF MIND | EXPERTISE | CHOICE | THE MEDPRO GROUP DIFFERENCE

Elementos Esenciales de Privacidad y Seguridad de HIPAA

Programa de hoy

Joyce Bruce, RN, MSN, JD, CPHRM
AVP, Patient Safety & Risk Solutions, MedPro Group
(Joyce.Bruce@medpro.com)

Joyce provee servicios comprensivos a los sistemas de cuidado de salud, hospitales y clínicas. Tiene más de 20 años de experiencia en la industria de cuidado de salud, trabajando en la práctica clínica, administración de hospital y consultoría.

El extenso liderazgo clínico de Joyce incluye experiencia como directora de enfermeras en facilidades terciarias y pediátricas. En estos roles, dirigió el desarrollo de programas de calidad, modelos de distribución de cuidado y trayectorias de cuidado clínico, incluyendo la creación de sistemas de colección de data. En adición a su trasfondo y expertise en el cuidado de salud, la experiencia legal de Joyce incluye defensa de seguros, defensa criminal y leyes de cuidado de salud.

En posiciones anteriores, Joyce también proveía consultoría de manejo de riesgo, incluyendo desarrollo de programa, servicios educativos, reducción de riesgo, encuestas de acreditación, cumplimiento regulatorio (EMTALA e HIPAA). Además, participó en el desarrollo de mejores políticas para grupos de médicos y hospitales.

Joyce es graduada de la Universidad de Indiana con un bachillerato en Ciencias de Enfermería y una maestría en Ciencias de Administración de Enfermería. Joyce adquirió su Juris Doctor de la Universidad de Indiana-Indianápolis. Es miembro del Bar de Indiana, del Bar de Ohio, del American Society for Healthcare Risk Management, el American Association of Nurse Attorneys y el Ohio Society for Healthcare Risk Management. Además, es una profesional certificada en manejo de riesgo en cuidado de salud (CPHRM).

Objetivos

Al finalizar este programa, los participantes deben ser capaz de:

- Revisar provisiones esenciales del Reglamento de Privacidad y Seguridad de la Ley de Transferencia y Responsabilidad de Seguro Médico (HIPAA)
- Discutir vulnerabilidades comunes en las prácticas y organizaciones de cuidado de salud que resultan en incumplimiento con HIPAA
- Identificar las mejores prácticas que pueden mitigar el riesgo de incumplimiento
- Entender cómo responder a incidentes e incumplimiento
- Discutir las consideraciones de HIPAA sobre comunicaciones electrónicas
- Discutir multas y penalidades por incumplimiento con HIPAA
- Revisar las mejores prácticas para reducir la incidencia e impacto de ataques cibernéticos y ransomware.

Definiciones y acrónimos

Incumplimiento	Uso o divulgación no permitido de PHI que comprometa su seguridad y privacidad
Asociado de negocio (BA)	Persona o entidad que lleva a cabo ciertas funciones o actividades que envuelven el uso o divulgación de PHI de parte o para un CE
Acuerdo de asociado de negocio (BAA)	Contrato legal que describe cómo se adhiere el BA a HIPAA con las responsabilidades y riesgos que asume
Entidad cubierta (CE)	Proveedor de cuidado de salud, plan de salud u oficina de información de cuidado de salud que electrónicamente transmite data de salud
Información protegida de salud (PHI) E-PHI: PHI electrónico	Información creada o recibida por CE que identifica pacientes (e.g. dirección, # teléfono, etc.). PHI es data de salud física y mental pasadas, presente y futura

Provisiones esenciales

HIPAA le provee al paciente el derecho a su PHI, incluyendo:

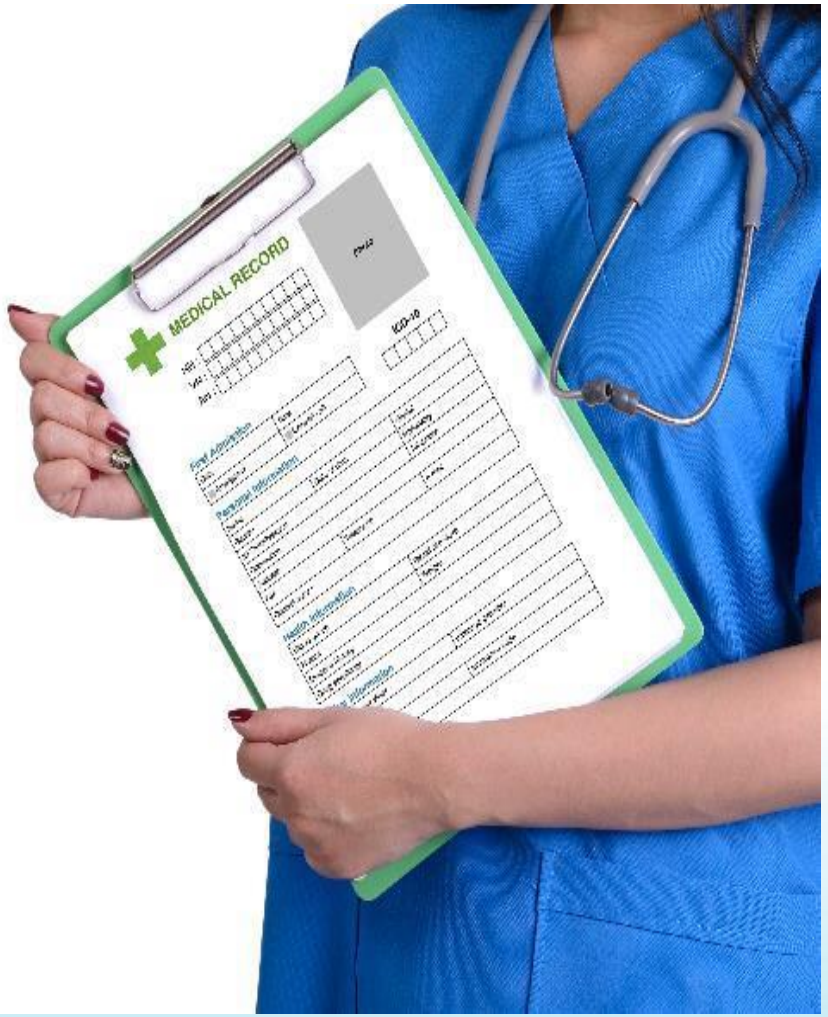
- Una notificación sobre cómo la práctica u organización utiliza PHI
- El derecho del individuo a una copia de su expediente médico
- El derecho a solicitar restricciones en la liberación de su PHI
- El derecho a solicitar enmiendas a su récord de salud
- El derecho a solicitar la contabilidad de las divulgaciones de su PHI
- Restricciones en la divulgación o uso de PHI sin su autorización
- El derecho a recibir comunicaciones confidenciales
- El derecho a reclamación por violaciones a los derechos de privacidad

Requisitos de Privacidad de HIPAA para entidades cubiertas

- Identificar un Oficial de Privacidad de HIPAA
- Asegurar que todo el equipo, voluntarios, estudiantes, etc. estén entrenados y actualizados anualmente.
- Identificar todos los BAs y mantener todos los BAAs con ellos
- Desarrollar e implementar políticas de privacidad de HIPAA (como mínimo):
  - Qué está definido como conjunto de registros designados
  - Publicación de Notificación de Prácticas de Privacidad
  - Estándar mínimo necesario
  - Liberación de récords/divulgación de PHI
  - Solicitudes para restricciones
  - Solicitudes para enmiendas
  - Solicitudes para la contabilidad de divulgación
  - El uso y divulgación del PHI de un individuo

Reglas básicas en cuanto a la liberación de información protegida de salud

- La información de los pacientes puede ser liberada sin autorización si el propósito es por tratamiento, pagos u operaciones de cuidado de salud.
- La divulgación del PHI de los pacientes para cualquier otra razón que no sea tratamiento, pago u operaciones de cuidado de salud requiere completar el proceso de autorización.
- Algunas excepciones existen para las actividades de monitoreo de salud pública (e.g., reporte de enfermedades), vigilancia del gobierno y algunas investigaciones implementadas legalmente. Los empleados deben consultar con el Oficial de Privacidad de HIPAA para asegurar la liberación adecuada.



Respondiendo a la solicitud de expedientes médicos por un paciente

- Debe proveer expedientes médicos no más tarde de 30 días desde la solicitud, salvo que una ley estatal requiera menos tiempo.
- Sólo tres recargos pueden ser cobrados al paciente:
  - Costo razonable de labor por crear y entregar los récords médicos de la forma y formato solicitado.
  - Costos de equipo para crear la copia de papel (como papel o “toner”) o copia electrónica (como un “USB drive”)
  - Costos de sellos si el paciente ha solicitado el envío del expediente por correo.
  - Los costos asociados para revisión de la solicitud, búsqueda y recuperación del expediente médico o preparación del récord no pueden ser cobrados
- Los expedientes médicos de un paciente nunca deben ser retenidos por razón de balances pendientes.

Cuál es el estándar mínimo necesario?

- Cuando el PHI de un paciente es utilizado o divulgado, ya sea a otro CE o BA, sólo debe ser divulgada la información necesaria para cumplir el propósito.

Ejemplo: La práctica utiliza una agencia de colección que ha solicitado información de facturación de varios pacientes. La práctica envía la información de facturación, pero también incluye información de diagnóstico de los pacientes. La agencia de colección no necesita la información de diagnóstico para llevar a cabo sus tareas, por ende, la práctica violentó el estándar mínimo necesario.

Vulnerabilidades comunes de las reglas de privacidad que resultan en incumplimiento o infracciones

Fracaso en…

Resulta en incumplimiento

- Orientar y entrenar a los empleados; proveer actualizaciones y educación continua
- Identificar un Oficial de Privacidad de HIPAA
- Tener políticas y procedimientos
- Adherirse al estándar mínimo necesario para acceder y liberar PHI
- Identificar todos los BAs
- Obtener BAAs
- Tener un proceso de respuesta para incidente e incumplimiento

Mejores prácticas de privacidad para mitigar el riesgo de incumplimiento

- Asegurar orientación y educación continua a los proveedores y empleados.
- Implementar políticas y procedimientos organizacionales (como mínimo):
  - Notificación de Prácticas de Privacidad
  - Liberación de récords
  - Solicitudes para restricciones
  - Solicitudes para enmiendas
  - Contabilidad de divulgaciones
  - Acción correctivas
  - Respuestas a incumplimiento
  - Respuestas a quejas

- Identificar un Oficial de Privacidad y Seguridad
- Cumplir con el estándar mínimo necesario en el acceso a PHI y liberación de información

Preguntas más frecuentes

P: Puedo proveer copias de expedientes a otros proveedores sin la autorización del paciente?

R: Sí, si la solicitud es con el propósito de tratamiento.

P: Si un paciente solicita expedientes, necesito proveer copias de expedientes de otros proveedores?

R: Sí, cualquier expediente que un proveedor utilice para decisiones de tratamiento, ya sea si fue generado por él/ella o no, es parte del conjunto de récords designado. Si un proveedor hacereferencia a notas tomadas fuera del expediente o laboratorios de otro proveedor, entonces, se convierten en parte de conjunto de récords designados.

P: Si el paciente pregunta por su expediente original, se los puedo proveer?

R: Nunca debes expedir los expedientes originales porque son propiedad de la organización de cuidado de salud. HIPAA estipula que los pacientes pueden recibir una copia. No obstante, puedes ofrecerle al paciente la opción de revisar el expediente original en la misma localización con un empleado del equipo presente.

P: El paciente ha solicitado que no proveamos información a su compañía de seguro. Debemos respetar esta solicitud?

R: Sí, estás requerido cumplir con la solicitud siempre y cuando el paciente pague de su bolsillo el servicio.

MedPro Group
a Berkshire Hathaway company

PEACE OF MIND | EXPERTISE | CHOICE | THE MEDPRO GROUP DIFFERENCE

Reglamentos de Privacidad y Seguridad de HIPAA

Provisiones esenciales del Reglamento de Seguridad de HIPAA

El Reglamento de Seguridad de HIPAA protege la información cubierta por el Reglamento de Privacidad, la cual es información de salud identificable individualmente que un CE crea, recibe, mantiene o transmite en forma electrónica (e-PHI). El reglamento de seguridad no aplica a PHI transmitido oralmente o por escrito.

La Regla de Seguridad de HIPAA requiere que los CEs mantengan y protejan e-PHI a través de salvaguardas razonables y apropiadas:

- Salvaguardas administrativas
- Salvaguardas técnicas
- Salvaguardas físicas

Requisitos de seguridad de HIPAA para entidades cubiertas

Asegurar la confidencialidad, integridad y disponibilidad de todos los e-PHI que los CEs crean, reciben, mantienen o transmiten

Identificar y proteger en contra de amenazas razonablemente anticipadas contra la seguridad o integridad de la información

Proteger contra usos y divulgaciones impermisibles que son razonablemente anticipadas.

Asegurar cumplimiento por todo su personal

Llevar a cabo un análisis de riesgo como parte del proceso de manejo de seguridad y actualizarlo regularmente

Componentes de análisis de riesgo

El proceso de análisis de riesgo debe incluir como mínimo:

- Evaluación y probabilidad del impacto de riesgos potenciales a e-PHI
- Riesgos identificados en el análisis de riesgo
- Medidas de seguridad apropiadas tomadas dirigidas a la identificación de riesgo
- Documentación de las medidas de seguridad tomadas y la razón fundamental para adoptar esas medidas de seguridad

Mantener protección de seguridad continua, razonable y apropiada

Salvaguardas administrativas

- Proceso de manejo de seguridad
  - Incluye completar un análisis de riesgo, identificando vulnerabilidades e implementando medidas de seguridad que hay que atender
- Designación de un Oficial de Seguridad de HIPAA
- Manejo del acceso a información
  - Políticas y procedimientos para autorizar el acceso a e-PHI basado en el rol del recipiente o usuario (acceso basado en rol)
- Entrenamiento y manejo en la fuerza laboral
  - Todos los empleados de la fuerza laboral deben ser entrenados sobre las políticas y procedimientos de seguridad
  - Debe poseer y aplicar sanciones apropiadas contra los miembros de la fuerza laboral que violenten las políticas y procedimientos
- Evaluación
  - Evaluación periódica de cuán bien sus políticas y procedimientos de seguridad cumplen los requisitos del Reglamento de Seguridad

Salvaguardas técnicas

- Acceso y control de la facilidad
  - Debe poseer límites físicos en el acceso a las facilidades mientras se asegura que se permite acceso autorizado
- Seguridad en el área de trabajo y equipo
  - Debe poseer políticas y procedimientos para especificar el uso y acceso apropiado a las estaciones de trabajo y medios electrónicos (laptops, correos electrónicos, sitios web, memorias USB)

Salvaguardas físicas

- Control de acceso
  - Políticas y procedimientos que permiten sólo a personas autorizadas para acceso a e-PHI
- Control de auditoría
  - Debe implementar hardware, software u otros mecanismos procesales para grabar y examinar el acceso y otras actividades en el sistema de información que contiene o utiliza e-PHI
- Control de integridad
  - Políticas y procedimientos y medidas electrónicas que aseguren la destrucción segura de e-PHI
- Seguridad de transmisión
  - Implementar medidas de seguridad técnicas que protejan contra acceso no autorizado a e-PHI siendo transmitidos sobre una red electrónica

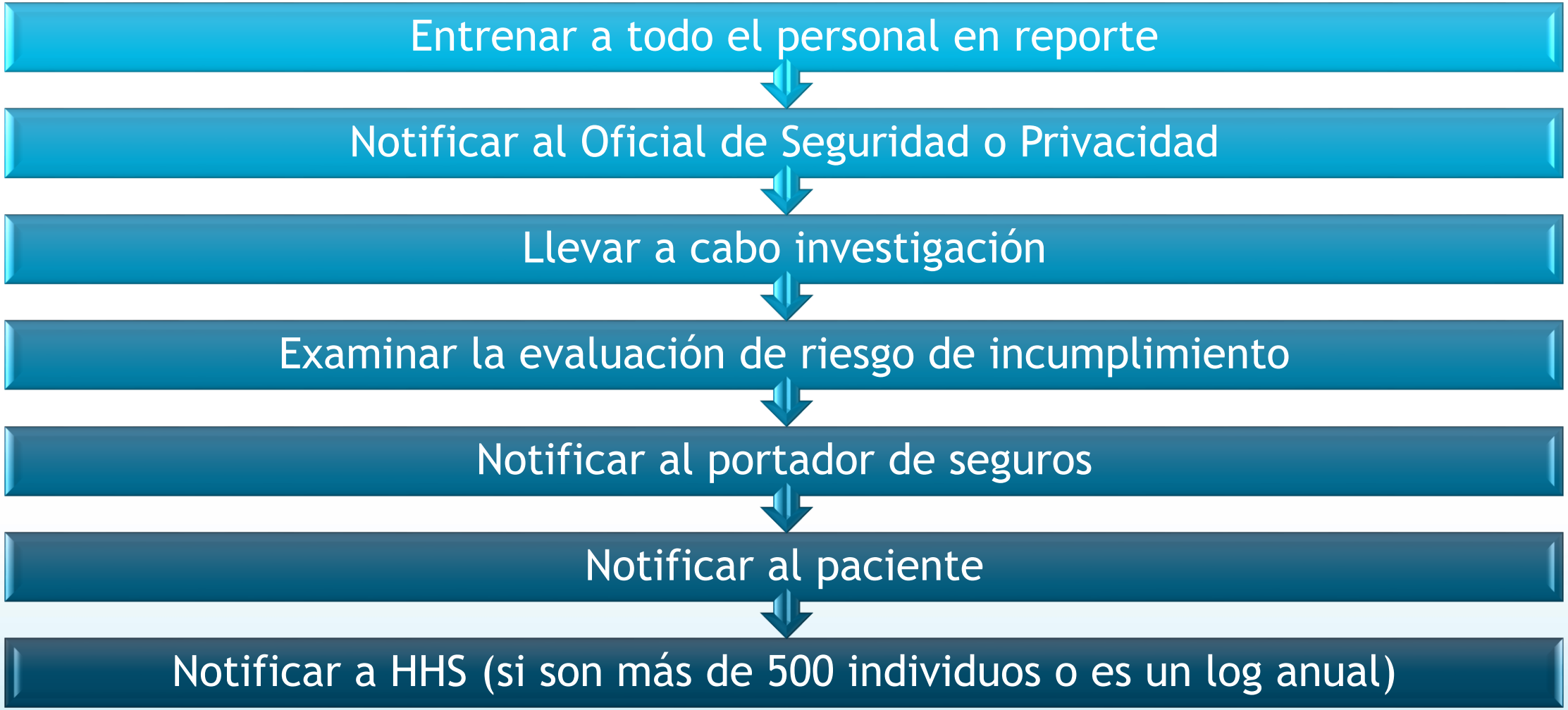
Vulnerabilidades comunes de seguridad que resultan en incumplimiento

Fracaso en… resulta en incumplimiento
• Conducir un análisis de seguridad y atender vulnerabilidades • Utilizar cifrado o codificación (encryption) y asegurar los correos electrónicos • Cumplir con el estándar mínimo necesario y las limitaciones en autorizaciones • Identificar BAs y obtener BAAs • Conducir entrenamiento del personal • Actualizar programas y parches

Las mejores prácticas para mitigar el incumplimiento de seguridad

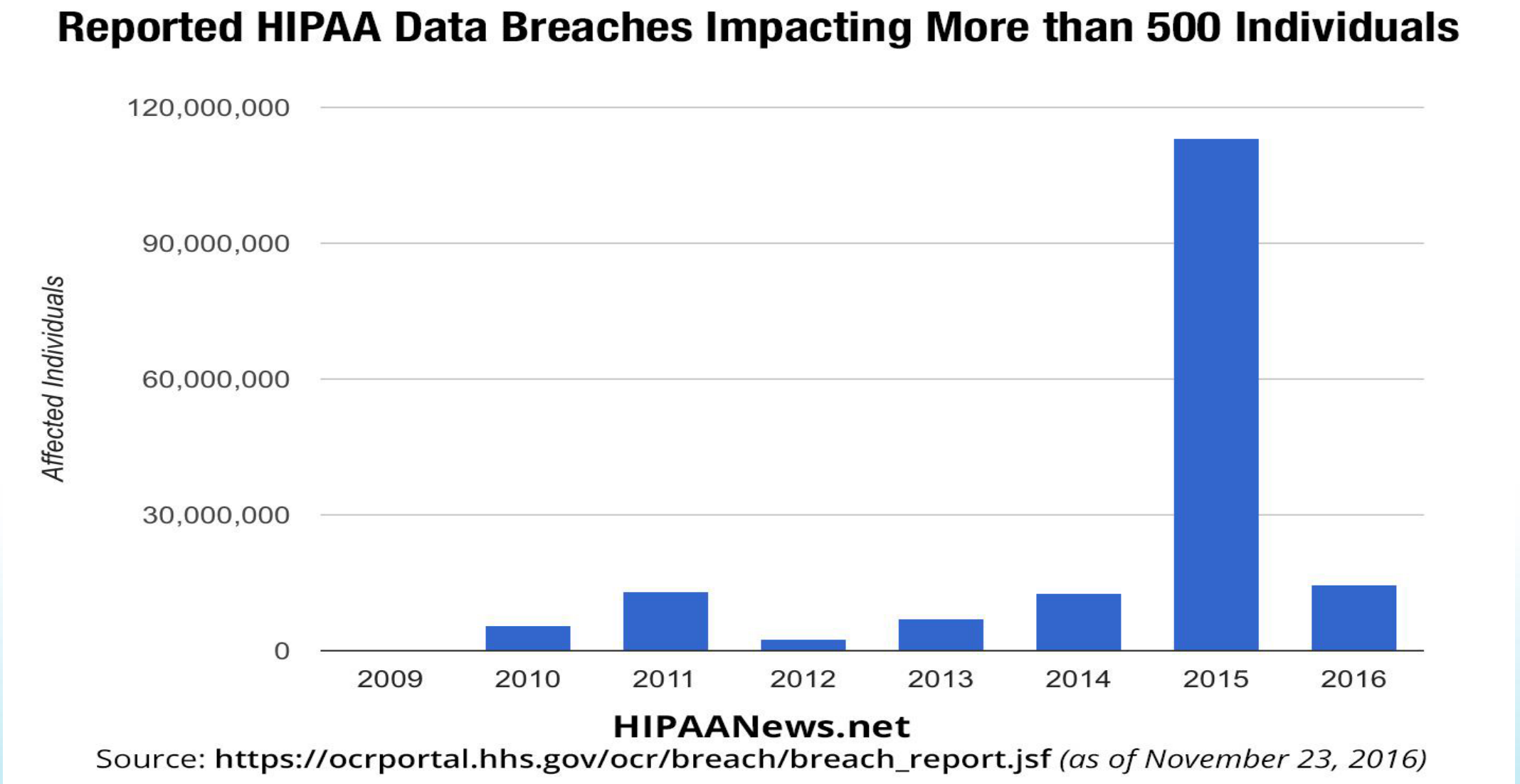
- Llevar a cabo entrenamiento del personal en la identificación y reporte de incidentes potenciales e incumplimiento, uso y riesgo
- Colocar codificación o cifrado en todos los equipos electrónicos, incluyendo equipo portable y thumb drives
- Implementar calendarización y asignación de contabilidad para actualización de programas y parches
- Utilizar equipo médico y el “Internet of things” (IoT), así como marcapasos cardiacos, equipo para administración de medicamentos, equipo de monitoreo, bomba de infusión, desfibriladores, glucómetros y equipo de medida de presión sanguínea
- Colocar salvaguardas físicas apropiadas en su lugar

Respondiendo a incidentes e incumplimientos de seguridad



HHS: U.S. Department of Health and Human Services

Incumplimiento de data



Source: U.S. Department of Health and Human Services Office for Civil Rights. (2018). Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Tipos y fuentes de incumplimiento

Number of Individuals Affected by a Protected Health Information Breach: 2010-2015
Count of affected individuals by the type and source of information breach

	2010	2011	2012	2013	2014	2015
Type of Information Breach						
Hacking/IT incident	568,358	297,269	900,684	236,897	1,786,630	111,812,172
Improper disposal	34,587	63,948	21,329	526,538	93,612	82,421
Loss	924,909	6,019,578	95,815	142,411	243,376	47,214
Theft	3,691,460	4,720,129	927,909	5,397,989	7,058,678	740,598
Unauthorized access/disclosure	130,106	118,444	338,767	383,759	3,019,284	572,919
Other breach	158,593	13,981	503,900	254,305	413,878	--
Source of Information Breach						
Desktop computer	246,643	2,042,186	81,385	4,348,129	2,378,304	316,226
Electronic medical record	803,600	1,720,064	136,751	40,196	121,845	3,948,985
E-mail	8,050	3,111	294,308	58,847	519,625	583,977
Laptop	1,507,914	405,873	575,529	1,023,181	1,273,612	391,830
Network server	665,123	613,963	921,335	320,127	7,253,441	107,252,466
Paper/Film	204,966	103,711	198,409	575,076	590,352	229,743
Portable Electronic Device	29,714	1,516	124,978	154,877	141,110	209,558
Other source	2,058,166	8,259,368	455,709	422,381	343,537	322,539

Note: Each count above is the total number of individuals affected by a breach of the specific information source and the breach type. Individual reports of a breach may involve one or more information sources, i.e. laptop, e-mail, etc, and one or more breach types, i.e. theft, loss, etc. In those cases, there may be double-counting of the number of affected individuals or reported breaches in a specific year.

Source: U.S. Department of Health and Human Services (HHS) Office for Civil Rights. Breaches Affecting 500 or More Individuals. Febrauary 1, 2016.

Source:U.S. Department of Health and Human Services Office for Civil Rights. (2016, February 1). Breaches affecting 500 or more individuals. Washington, DC: HHS.

Ejemplos de notificación de incumplimiento

Mirar los expedientes médicos de un vecino por curiosidad

Enviar por correo información de facturación a un paciente equivocado

Perder un thumb drive no codificado

Hablar a un familiar sobre un paciente

Perder un teléfono con imágenes de un paciente en él

Computadora perdida o robada que contenga PHI

Un supervisor u Oficial de Privacidad debe ser notificado inmediatamente si se sospecha de un incidente o incumplimiento o que el mismo pueda ocurrir.

Respondiendo a incidentes e incumplimientos

Incumplimiento significa la adquisición, acceso, uso o divulgación de PHI en una manera no permitida que compromete su seguridad y privacidad

A menos que esté cubierto por una de las excepciones de incumplimiento, un incumplimiento se presume a menos que el CE o BA demuestre una baja probabilidad de que el PHI ha sido comprometido basado en una evaluación de riesgo

Evaluación de riesgo de incumplimiento

Debe incluir como mínimo los siguientes factores

- Naturaleza y extensión del PHI envuelto
- La(s) persona(s) no autorizada que utilizó o a quien se le divulgó el PHI
- Si el PHI fue adquirido o visto
- La extensión de mitigación de del riesgo

Notificación

La notificación de menos de 500 debe ser anotada y reportada 60 días luego del año calendario al que fue descubierto

Incumplimiento de más de 500 deben ser reportados inmediatamente a HHS y a los medios de comunicación local

Ningún cambio en la información es requerida en las cartas de notificación de incumplimiento

Ningún cambio en el periodo de tiempo por reportar 60 días desde la fecha del descubrimiento o desde que se debió haber descubierto al emplear diligencia razonable

HHS: U.S. Department of Health and Human Services

Consideraciones especiales para comunicaciones electrónicas

Texteando

- Las órdenes están prohibidas
- Los mensajes deben estar en plataformas codificadas

Correo electrónico

- Sistemas codificados seguros

Telemedicina

- Cuenta para consideraciones de privacidad y seguridad

MedPro Group
a Berkshire Hathaway company

PEACE OF MIND | EXPERTISE | CHOICE | THE MEDPRO GROUP DIFFERENCE

Sanciones y penalidades

Sanciones civiles monetarias

TABLE 1—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect—Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect—Not Corrected	50,000	1,500,000

- Fracaso en cumplir con políticas y procedimientos puede resultar en acciones correctivas
- CEs (incluyendo empleados individuales) y BAs están sujetos a penalidades monetarias civiles (sanciones) y penalidades criminales

Penalidades criminales

- Conducta prohibida
  - Obtener o divulgar con conocimiento PHI sin autorización
  - Si es realizado bajo falsos pretextos
  - Si es realizado con la intención de vender, transferir o utilizar la información para ventajas de anuncios, ganancias personales o daño malicioso
- Penalidad
  - Hasta $50,000 en sanciones y 1 año en prisión
  - Hasta $100,000 en sanciones y 5 años en prisión

Cargos de los fiscales generales de los estados

La Ley de Health Information Technology for Clinical and Economic Health (HITECH) provee al Fiscal General del Estado la autoridad de instar acciones civiles a nombre de los residentes del estado por violaciones al reglamento de Privacidad y Seguridad de HIPAA

La Ley HITECH permite al Fiscal General del Estado obtener daños y perjuicios en nombre de los residentes del estado o imponer violaciones adicionales al Reglamento de Privacidad y Seguridad de HIPAA

Leyes estatales de HIPAA

La ley del estado entra en efecto sólo si

No existe una disposición específica sobre una materia en la ley federal	Si la ley estatal es más rigurosa (es decir, que permita mayor acceso a los individuos o provea más protecciones). Por ejemplo: HIPAA requiere proveer a los pacientes copias de sus récords no más tarde de 30 días luego de la solicitud	O si existe otra excepción según HIPAA

Ataques cibernéticos y ransomware

NEWS

Ransomware attack on Cass Regional shuts down EHR

by **Jessica Davis** | July 11, 2018

Emergency and stroke patients are still being diverted to ensure patients receive the best possible care, but the Missouri health system

Allscripts hit by ransomware, knocking some services offline

by **Jessica Davis** | January 19, 2018

Users took to Twitter to complain about the cloud EHR being down, with some unable to access patient information all day.

Primary Health Care announces email breach one year after discovery

by **Jessica Davis** | March 19, 2018

Hackers broke into four employee email accounts of the Iowa provider, allowing access to a wide range of sensitive data.

NEWS

Phishing attacks breach Alive Hospice for 1 to 4 months

by **Jessica Davis** | July 18, 2018

Two employee email accounts were breached by phishing attacks, which potentially gave hackers access to a trove of highly sensitive

NEWS

Phishing hack on Ohio provider breaches data of 42,000 patients

by **Jessica Davis** | May 29, 2018

A hacker hit some email accounts of Aultman Health Foundation with a phishing attack in February, but officials didn't discover the

Vulnerabilidades presenciadas frecuentemente en cuidado de salud

- Proveedores de software múltiple y de nichos
- Interoperabilidad fragmentada; variación en prácticas, políticas y tecnologías
- Fracaso en proveer recursos para actualizaciones, mejoras y educación
- Habilidad limitada y presión por falta de tiempo para crear cambios en récords electrónicos
- Equipo médico y sistemas de proveedores
- Falta de educación y entrenamiento

Impacto y resultados potenciales de ataques cibernéticos

Seguridad del paciente

- Historial e información inaccesible de pacientes, limitando la habilidad de tratamiento

Impacto financiero

- Pérdida de récords de facturación y récords clínicos que apoyen la facturación

Investigación de incidente

- Uso y recursos forenses

Determinación y notificación de incumplimiento

- Notificación de riesgo de incumplimiento de evaluación

Investigación y sanciones estatales y federales

Credibilidad y reputación

Estrategias/mejores prácticas para evitar y mitigar riesgo cibernético

Contraseña

- Debe ser fuerte- mínimo de 8 caracteres con al menos un número/letra/cap/caracter especial
- Necesario de cambiar en una base calendarizada
- Utilizar autenticación multifactorial (huellas digitales, contraseña fob, etc.)

Estrategias/mejores prácticas para evitar y mitigar riesgo cibernético

Utiliza software antivirus y "firewalls"

- Programa robusto de antivirus con actualizaciones continuas
- Firewalls
- Prohibir o monitorear medios externos y aplicaciones

Estrategias/mejores prácticas para evitar y mitigar riesgo cibernético

Acceso

- Asegurar los servidores y el hardware
- Limitar el transporte del hardware o equipo que contengan PHI
- Colocar políticas/limitaciones/acceso prohibido a sitios de alto riesgo
- Auditar el horario de acceso a la red
- Prohibir aplicaciones de software por el personal
- Considerar y planificar para riesgos ambientales

Estrategias/mejores prácticas para evitar y mitigar riesgo cibernético

Estrategias/mejores prácticas para evitar y mitigar riesgo cibernético

Crear y promover una cultura de seguridad cibernética

- Construir mejores prácticas
- Reducir variaciones e incrementar consistencia
- Asegurar y monitorear cumplimiento
- Asignar contabilidad
- Proveer entrenamiento continuo y educación del personal
- Ser competente en cuanto a los riesgos de correos electrónicos y suplantación de identidad
- Asegurar cumplimiento y debida diligencia por los proveedores

Resumen

Familiarizarse con las políticas de privacidad y seguridad en su organización

Entender los derechos de los pacientes en relación a revisar, solicitar y liberar PHI

Entender los reglamentos con relación a BAs, así como el concepto de estándar mínimo necesario

Familiarizarse con cómo cualquier sospecha de incidente o incumplimiento está siendo reportado

Sé diligente en utilizar las mejores prácticas para evitar ataques cibernéticos

Recursos

- Cybersecurity Resource List (MedPro Group)
- Guidelines: Medical Records release (MedPro Group)
- Risk Q & A on Telehealth/Telemedicine (MedPro Group)
- Summary of the HIPAA Privacy Rule (MedPro Group)
- Summary of the HIPAA Security Rule (MedPro Group)
- Virtual Risk: An Overview of Telehealth from a Risk Management Perspective (MedPro Group)

Aviso Legal

La información contenida en esta presentación y expuesta por el conferenciante está basada en recursos creídos como ciertos en el momento que fueron utilizados como referencia. El conferenciante ha realizado un esfuerzo razonable para asegurar la exactitud de la información presentada; no obstante, ninguna garantía o representación es hecha para con tal exactitud. El conferenciante no está comprometido a proveer servicios legales o profesionales. Si se requiere asesoramiento legal o cualquier otra asistencia legal experta, los servicios de un abogado u otro profesional competente del derecho deben ser solicitados.