Decanato de Estudios Graduados e Investigación
Universidad de Puerto Rico, Recinto de Río Piedras

PRIVACIDAD Y CONFIDENCIALIDAD EN LA INVESTIGACIÓN CON SERES HUMANOS COMO SUJETOS DE ESTUDIO

Myriam L. Vélez Galván
Oficial de Cumplimiento

21 de septiembre de 2016

CONTENIDO

- Principios éticos
- Regulaciones, normativas, definiciones
- Riesgos
- Privacidad y confidencialidad en proceso de identificación y contacto inicial; toma de consentimiento, intervención o interacción, recopilación y almacenamiento de los datos, publicación, terminación de protocolo
- Criterios de evaluación y aprobación de un protocolo
- Consentimiento informado y dispensas
- Errores u omisiones más frecuentes
- Estudios de casos

LA INTEGRIDAD Y LA CONDUCTA RESPONSABLE EN LA INVESTIGACIÓN COMPRENDE EL CONOCIMIENTO Y ATENCIÓN EN VARIAS ÁREAS:

PRINCIPIOS ÉTICOS: INFORME BELMONT

☑ Respeto por las personas

- Autonomía individual
- Protección a las personas con limitada autonomía

☑ Beneficencia

- No hacer daño.
- Maximizar los beneficios y minimizar los daños

☑ Justicia

- Distribución equitativa de los riesgos y beneficios de la investigación entre los/as voluntarios/as y la población a beneficiarse de los resultados.

PRINCIPIOS ÉTICOS: DECLARACIÓN BIOÉTICA Y DERECHOS HUMANOS DE LA UNESCO

- ☑ Dignidad humana y derechos humanos
- ☑ Beneficios y efectos nocivos
- ☑ Autonomía y responsabilidad individual
- ☑ Consentimiento
- ☑ Personas carentes de la capacidad de dar su consentimiento
- ☑ Respeto de la vulnerabilidad humana y la integridad personal
- ☑ Privacidad y confidencialidad
- ☑ Igualdad, justicia y equidad
- ☑ No discriminación y no estigmatización
- ☑ Respeto de la diversidad cultural y del pluralismo
- ☑ Solidaridad y cooperación
- ☑ Responsabilidad social y salud
- ☑ Aprovechamiento compartido de los beneficios
- ☑ Protección de las generaciones futuras
- ☑ Protección del medio ambiente, la biosfera y la biodiversidad

REGULACIONES O NORMATIVAS APLICABLES

- **Federales**
  - 45 CFR 46 (directrices para IRBs)
  - Otras
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Health Information Technology for Economic and Clinical Health) Act (HITECH)
    - Family Educational Rights and Privacy Act (FERPA)
    - Protection of Pupil Rights Amendment (PPRA)
- **Estatales**
  - Ley del Instituto de Estadísticas de Puerto Rico, Ley Núm. 209 de 28 de agosto de 2003, según enmendada
    - ✓ Informe Acceso, divulgación y confidencialidad de la información del gobierno (2009)
  - Ley de Notificación de Política de Privacidad, Ley Núm. 39 de 24 de enero de 2012
  - Ley para la Administración e Intercambio Electrónico de Información de Salud de Puerto Rico, Ley Núm. 40 de 2 de febrero de 2012
- **Institucionales**
- **Códigos de ética de las profesiones**

DEFINICIÓN SUJETO HUMANO: 46CFR46

Individuo **vivo del cual** un(a) investigador(a) (ya sea profesional o estudiante) que conduce una investigación obtiene:

- información a través de **intervención** o **interacción** con el individuo, o
- información privada identificable (directa o indirecta).

DEFINICIÓN DE INFORMACIÓN PRIVADA EN 45CFR46

- Por **información privada** se entiende la información sobre la conducta que se produce en circunstancias en que la persona puede suponer razonablemente que no se la observa directa ni indirectamente, e información facilitada con fines específicos y que la persona que la facilite puede suponer razonablemente que no se hará pública (por ejemplo, los antecedentes médicos). §46.102 (2)

CRITERIOS PARA LA APROBACIÓN DE UN PROTOCOLO

- Criterios principales para autorizar un protocolo
  - ✓ Los riesgos a los participantes se han considerado y minimizado.
  - ✓ Los riesgos son razonables en proporción a los beneficios anticipados.
  - ✓ La selección de los participantes es equitativa.
  - ✓ El proceso de la toma del consentimiento informado se realizará y es documentado adecuadamente.

☑ §46.111 (7) Cuando sea apropiado, existen estipulaciones adecuadas para proteger la privacidad de los sujetos y mantener la confidencialidad de la información.

PRIVACIDAD, CONFIDENCIALIDAD Y ANONIMATO

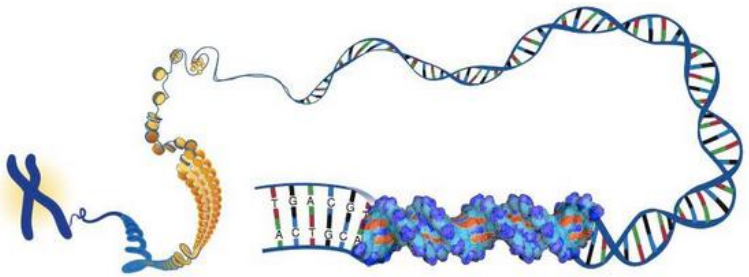
- **Privacidad:** potestad de la persona para decidir sobre el acceso a su persona o a su información.
- **Confidencialidad:** manejo de la información que provee una persona con la expectativa o acuerdo de que su identidad o información personal no será divulgada.
- **Anonimato:** la identidad de la persona no se puede establecer directa ni indirectamente.
- **Límites a la confidencialidad** (leyes, metodología, objetivos, etc.)
- Hay investigaciones cuyo interés es dar a **conocer la identidad** de los(as) participantes.
- Certificados de confidencialidad (NIH): Protege al investigador/a de revelar información sensitiva identificable de los(as) participantes.

INFORMACIÓN O DATOS

- Información de contacto (teléfono, email, dirección)
- Hojas de consentimiento informado firmada
- Formularios o instrumentos completados
- Grabaciones, audio o video, fotos, imágenes (radiografías, MRI)
- Identificadores corporales: tatuajes, cicatrices, altura, peso, etc.
- Muestras o especímenes biológicos
- Datos codificados
- Listas maestras

INFORMACION O DATOS

- Datos crudos: información primaria que no ha sido procesada.
- Datos secundarios
- Datos con o sin identificadores:
  - ✓ Identificadores directos
  - ✓ Identificadores indirectos; por ejemplo, la asignación de códigos que vincule a la persona y la combinación de variables, como las socio demográficas, pueden identificar indirectamente a una persona.
- Datos de-identificados vs datos anónimos



ADN, no tan secreto

Autor: **Lourdes Zamanillo** Fecha: **2015-03-09**

Siempre se ha creído que al participar en estudios genéticos de forma anónima hace que la identidad del donador sea confidencial. Sin embargo, las cosas ya no son así de sencillas. La información genética puede ser rastreada fácilmente con información pública para dar con el individuo en cuestión.

Suena a película de ciencia ficción, pero es algo bastante real. Yaniv Erlich, genetista miembro del Instituto Whitehead del MIT, demostró que con una sencilla búsqueda en Internet es factible descubrir la identidad de un donador de ADN.

¿Para qué se dona el ADN? Para un sinfín de proyectos de investigación. "Mil Genomas", por ejemplo, busca recopilar la información genética de alrededor de mil voluntarios con el fin de encontrar secuencias que se repitan en la mayoría de la población. El objetivo es identificar el "genoma humano", es decir la información genética que todos compartimos. La información recopilada por este proyecto está disponible en bases de datos de acceso público.

Yaniv Erlich descubrió que, con un programa llamado "lobSTR", se pueden extraer secuencias específicas del ADN de un donador masculino llamadas STRs. Estos marcadores se encuentran dentro del cromosoma (cromosoma sexual del género masculino) y son heredados directamente de padre a hijo.

Curiosamente, varios entusiastas de la genealogía utilizan los STRs para trazar las raíces y ramas de su árbol genealógico. Buscando un STR en alguna base de datos en Internet que maneje esa información suele arrojar un apellido que congenia con el marcador. No sólo un apellido. También arroja una línea genealógica y, a veces, hasta una localización geográfica de la familia.

Al ingresar un apellido y un estado en una base de datos demográfica, dar con el individuo en cuestión es cosa de unos minutos.

Lo preocupante del asunto no sólo radica en que la privacidad de los donadores está en peligro, sino en lo fácil que es accesar a información tan íntima y detallada.

Algunas compañías y laboratorios ya han removido detalles de la información del Internet con el fin de prevenir este tipo de violaciones. Sin embargo, la solución al problema apenas comienza a gestarse.

INVESTIGACIONES POR INTERNET

THE WALL STREET JOURNAL.

SUBSCRIBE NOW and 3 MONTHS for the PRI

AMÉRICA LATINA viernes, 5 de agosto, 2011, 16:56:00 EDT

Inicio | Negocios | Mercados | Tecnologia | Gestión | Actualidad | Vida y Estilo | Opinión | Pequeñas Empresas | Finanzas

SPANISH | August 5, 2011, 4:56 p.m. ET

La información disponible a partir de una foto

Artículo | Comentarios

Email | Print | Save

Por JULIA ANGWIN

Mientras los gigantes de Internet Facebook Inc. y Google Inc. compiten para ampliar su capacidad en el campo del reconocimiento facial, nuevos estudios muestran cuán impactante y perjudicial para la privacidad se ha convertido esta tecnología.

Con sólo una foto, investigadores de la Universidad de Carnegie Mellon en Pittsburgh identificaron con éxito a casi un tercio de las personas en su estudio, usando una potente tecnología de reconocimiento facial recientemente adquirida por Google.

El profesor Alessandro Acquisti, autor del estudio, también descubrió que alrededor de 27% de las veces, y usando datos extraídos de perfiles de

http://online.wsj.com/article/SB10001424053111903454504576490584142998822.html?mod=WSJS_tecnologia_MiddleTop

El profesor Alessandro Acquisti, autor del estudio, también descubrió que alrededor de 27% de las veces, y usando datos extraídos de perfiles de Facebook de participantes del estudio, podía predecir correctamente los primeros cinco dígitos de sus números de Seguro Social, la identificación nacional en Estados Unidos.
El estudio demuestra el potencial nivel de intromisión de esta tecnología al combinarse con datos personales de dominio público. El estudio fue financiado en gran parte por la Fundación Nacional de la Ciencia de EE.UU., donaciones pequeñas de Carnegie Mellon y el ejército estadounidense.
Paul Ohm, un profesor de derecho de la Universidad de Colorado, que leyó el estudio de Acquisti, **dice que la investigación demuestra lo fácil que se ha hecho "reidentificar" a personas con información supuestamente anónima.**

RIESGOS

- Riesgo

  Probabilidad de daño o perjuicio físico, psicológico, social, económico o legal que suceda como resultado de la participación en una investigación. Puede variar desde mínimo a significativo.

- Riesgo mínimo

  Probabilidad y la **magnitud** de daño o incomodidad que se encuentran normalmente en la vida diaria o en exámenes médicos o psicológicos rutinarios de personas saludables.

RIESGOS (2)

Algunos de los posibles riesgos que puede enfrentar un(a) participante son:

- incomodidad emocional, mental o física
- coerción o influencia excesiva o indebida
- daños físicos
- pérdida económica
- invasión de la privacidad
- ocurrencia de una brecha en la confidencialidad

RIESGOS (3)

- La ocurrencia de una brecha en la confidencialidad se refiere a la divulgación voluntaria o involuntaria de información privada identificable.
- Esta divulgación podría afectar al participante en:
  - ✓ su reputación personal, profesional o social (estigmatización)
  - ✓ su capacidad para obtener o mantener un empleo
  - ✓ su responsabilidad o situación legal (civil o criminal)

endi
ELNUEVODIA.COM

Tecnología

Buscar

Acceda a la Edición Electrónica

ÚLTIMA HORA | VIDEOS | FOTOS | Noticias | Opinión | Negocios | Entretenimiento | Estilos de Vida | Deportes | In English | CLASIFICADOS | SHOP.PR

CONSUMO | FINANZAS | AUTOS | BANCA | TECNOLOGÍA | EMPRESAS | ECONOMÍA

TECNOLOGÍA

Hackean al creador de Facebook

Violaron la seguridad de sus cuentas de Twitter, LinkedIn y Pinterest

lunes, 6 de junio de 2016 - 11:08 AM
Actualizado en: lunes, 6 de junio de 2016 - 2:47 PM

Por The Associated Press

75

Nota de archivo: Este contenido fue publicado hace más de 90 días

Varios usuarios en Twitter de alto perfil también han visto sus cuentas afectadas. En la foto Mark Zuckerberg. (AP)

NUEVA YORK— La cuenta en Twitter y en un par más de cuentas en redes sociales del fundador de Facebook, Mark Zuckerberg, fueron hackeadas brevemente, se informó el lunes.

Facebook Inc. emitió el lunes un comunicado para decir que ninguno de los sistemas o cuentas de la empresa fueron infiltrados y que las cuentas afectadas de Zuckerberg desde entonces ya tienen más medidas de seguridad.

La cuenta y contraseña del magnate en Facebook no se vieron comprometidas, informó la empresa. Tampoco su cuenta en Instagram.

Una persona cercana a la situación confirmó que las cuentas de LinkedIn y Pinterest también fueron afectadas. Los responsables de esas redes sociales no estaban disponibles para hacer comentarios.

Fotos de pantalla capturadas por el sitio de tecnología Engadget parecían mostrar a alguien utilizando la cuenta —que es poco usada— para decir que Zuckerberg estaba en la "base de datos de LinkedIn" e invitaba al empresario de las redes sociales a ponerse en contacto. LinkedIn no quiso comentar.

No queda claro cómo sucedió la violación de seguridad, aunque una serie de

http://www.elnuevodia.com/tecnologia/tecnologia/nota/hackeanalcreadordefacebook-2207317/

INTERNACIONALES

Servicio Secreto pierde información ultrasecreta

La agencia estadounidense dijo que perdieron información personal sobre empleados, contactos e incluso informantes

viernes, 7 de diciembre de 2012 - 8:23 PM
Actualizado en: viernes, 7 de diciembre de 2012 - 10:44 PM

Washington - El Servicio Secreto de Estados Unidos reconoció hoy que en 2008 perdió en el metro de Washington dos copias de seguridad de sus ordenadores con información, incidente que salió a la luz durante una investigación sobre sus procedimientos.

El portavoz del Servicio Secreto, Ed Donovan, señaló en un comunicado que se informó entonces a la oficina del inspector general de autoridades y descartó que la pérdida supusiera una ruptura de la seguridad, ya que las copias estaban protegidas.

Las copias incluían información personal sobre empleados, contactos e incluso informantes, según indicaron fuentes de seguridad y del Congreso a la cadena Fox.

Un empleado de una empresa privada subcontratada por el Departamento de Seguridad Nacional (DHS), del que depende el Servicio Secreto, olvidó el material en un vagón del metro en febrero de 2008 cuando lo trasladaba a unas instalaciones para su almacenamiento.

ESPAÑA | AMÉRICA | BRASIL | CATALUÑA NEWSLETTER SUSCRÍBETE

EL PAÍS

TECNOLOGÍA

MÓVILES REDES SOCIALES BANCO DE PRUEBAS RETINA MERISTATION

DROPBOX ›

Dropbox reconoce el 'hackeo' de 60 millones de cuentas: cómo saber si la tuya está afectada

El robo de las credenciales a un empleado de la firma en 2012 ha derivado en el 'pirateo' masivo del servicio

JOSÉ MENDIOLA ZURIARRAIN

31 AGO 2016 - 13:54 CEST

Dropbox es un servicio de almacenamiento masivo en la 'nube'./ CORDON PRESS

Ahora que más que nunca la seguridad en internet está puesta en entredicho por parte de los expertos, el gigante Dropbox acaba de reconocer el *hackeo* masivo de sus servicios en el año 2012, tras el robo de las credenciales a un empleado,

http://tecnologia.elpais.com/tecnologia/2016/08/31/actualidad/1472642567_500051.html

PRIVACIDAD DURANTE EL PROCESO DE IDENTIFICACIÓN Y CONTACTO INICIAL CON PARTICIPANTES

- Informantes claves
- Bola de nieve
- Expedientes o registros privados
- Directorios públicos
- Internet: redes sociales, chats, etc.

PRIVACIDAD DURANTE INTERVENCIÓN O INTERACCIÓN

- Lugar privado.
- Mantener distancia entre los(as) participantes o terceras personas.
- Si la interacción será a distancia (teléfono o Internet), asegurar o indagar si la persona tiene privacidad en su entorno.
- Construcción del instrumento.

CONSENTIMIENTO INFORMADO

- Información que será recopilada, especialmente la sensible (privacidad) y la identificable (confidencialidad).
- Tiempo que existirá la información relacionada con la identidad del participante.
- Personas que tendrán acceso a la información identificable o sensible. ¿Quiénes deben nombrarse?
- Lugar de almacenamiento y medidas de seguridad.
- Disposición del material o información luego del tiempo de conservación.
- Información que será publicada y cómo se aludirá al participante; por ejemplo grabaciones y fotos, extractos o trascripciones de entrevistas, etc.
- Si no es posible garantizar la confidencialidad.
- Límites a la confidencialidad: intencional, legal, metodológica, cantidad de participantes, características únicas de la persona, etc.
- Usos futuros o cesiones de derechos de autor.

ELEMENTOS – CONFIDENCIALIDAD Y MANEJO DE LA INFORMACIÓN

Descripción de hasta qué punto se mantendrá confidencial la información que se obtenga, los datos o expedientes. Incluir quién tendrá acceso a los datos de la investigación que puedan identificar directa o indirectamente al participante.

En **investigaciones de estudiantes**, el(la) supervisor(a) de la investigación, tesis o disertación debe incluirse como persona que podría tener acceso a los datos crudos de la investigación (datos que pueda identificar directa o indirectamente a participantes).

Además, toda hoja de consentimiento debe tener la cláusula: *Oficiales del Recinto de Río Piedras de la Universidad de Puerto Rico o de agencias federales responsables de velar por la integridad en la investigación podrían requerirle al(a la) investigador (a) los datos crudos obtenidos en este estudio, incluyendo este documento*.

¿Cómo se recopilará mi información?
¿Para qué la vas a utilizar?
¿Cómo la vas a publicar?
¿Quién la podrá ver y utilizar?
¿Cómo y dónde la vas a guardar/proteger?
¿Cómo la desecharás?
¿Hasta cuándo la tendrás?
¿La seguirás utilizando para otros propósitos?

ELEMENTOS – CONFIDENCIALIDAD Y MANEJO DE LA INFORMACIÓN

Archivo permanente de la información o datos crudos:

- Información, documentos, materiales o datos crudos recopilados que se guardarán permanentemente en un expediente, un record médico, un banco de datos, un repositorio, biblioteca, etc.
- Distinguir entre la información o datos que se conservarán por un tiempo fijo de los permanentes.
- Persona o institución custodia de la información, quién tendrá acceso o con quién se compartirá y posibles usos futuros.
- Posibilidad o no de identificar directa o indirectamente a los(as) participantes.

El CIPSHI solamente establece que las hojas de consentimiento firmadas deben ser conservadas por un mínimo de tres años una vez finalizada la investigación.

ELEMENTOS – CONFIDENCIALIDAD Y MANEJO DE LA INFORMACIÓN

- Grabaciones de audio, video o fotos: Incluir el propósito y usos de las grabaciones o fotos.
- Aseveración de que la información que se provea se mantendrá confidencial dentro de los límites de la ley o mientras no exista peligro para el participante o terceras personas.
- Si la información a obtenerse se compartirá entre participantes (por ejemplo, en grupos focales), una aseveración que indique que el(la) investigador(a) no puede garantizar que la información compartida no sea revelada por los(as) participantes.
- Límites a la confidencialidad por las características únicas de los(as) participantes.
- El propósito de la investigación es revelar la fuente de la información o la identidad de la persona.

ELEMENTOS – CONFIDENCIALIDAD Y MANEJO DE LA INFORMACIÓN

- Las investigaciones que con transferencia de información por Internet no deben considerarse como anónimas.
- En investigaciones por Internet, debe estar la advertencia: *La información que maneje en la computadora que utilice puede ser intervenida o revisada por terceras personas. Estas personas pueden ser personas con acceso legítimo o ilegítimo a la computadora y su contenido como un familiar, patrono, intrusos o piratas informáticos ("hackers"), etc. Además, en la computadora que utilice puede quedar registro de la información que acceda o envíe por Internet.*

DISPENSAS O "WAIVERS"

- **Dispensa del consentimiento informado:**
  - Exención del consentimiento.
  - Exención de la firma.
  - Restricción de la información.

- **Algunos de los criterios para conceder dispensas:**
  - Investigación de riesgo mínimo.
  - Imposibilidad de realizar la investigación sin la dispensa.
  - No atenta contra derechos y seguridad de el(la) participante.
  - Protección de la identidad del (de la) participante.
  - Se le proveerá información apropiada a el(la) participante.

¿Quién otorga la dispensa: IRB o, si aplicara, el HIPAA Privacy Board o Privacy Officer o la institución custodia de la información?

45CFR46§46.117 DOCUMENTACIÓN DEL CONSENTIMIENTO INFORMADO

(c) Un IRB podrá dispensar al investigador de obtener un formulario firmado de consentimiento de algunos o todos los sujetos si llega a la conclusión de que:

(1) El único documento que relaciona al sujeto con la investigación es el de consentimiento propiamente dicho y el principal riesgo sería el posible daño resultante de una contravención de la confidencialidad. **A todos los sujetos se les preguntará** si desean que exista documentación que lo relacione con la investigación, y **sus deseos serán respetados**;...

CONSIDERACIONES PROTOCOLOS CON DATOS SECUNDARIOS

- ¿Qué tipo de información identificable, si alguna, se recopilará?
- ¿Quién tendrá acceso a la información identificable?
- ¿Dónde se mantendrá la información identificable?
- ¿Qué tipos de códigos o *codificación criptográfica (encryption)* se utilizará para separar los datos de la investigación de los identificadores de los sujetos (participantes)?
- ¿Cómo se garantizarán los límites de acceso ?
- ¿Cómo el personal de la investigación serán adiestrando en la privacidad y la confidencialidad ?
- ¿Por cuánto tiempo será conservada la información identificable o los vínculos con identificadores personales?
- Para los datos que se transmitan físicamente o electrónicamente , ¿qué métodos de codificación serán utilizados?
- ¿Qué procedimientos se utilizarán para la eliminación o destrucción de los identificadores y los documentos de la investigación , una vez que ya no se requiera?

INFORMACIÓN DE SALUD O MÉDICA PROTEGIDA (Protected Health Information -PHI) - HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

1. Nombres
2. Todas las subdivisiones geográficas más pequeñas que un estado, incluyendo dirección, ciudad, condado, distrito, código postal, y sus códigos geográficos equivalentes, a excepción de los tres dígitos iniciales del código postal si, de acuerdo con los actuales datos de dominio público de la Oficina del Censo: La unidad geográfica formada por la combinación de todos los códigos postales con los mismos tres dígitos iniciales contiene más de 20.000 personas; y los tres primeros dígitos del código postal para todas las unidades geográficas que contienen 20.000 personas o menos se cambia a 000.
3. Todos los elementos de fechas (excepto año) para las fechas que están directamente relacionadas a un individuo, incluyendo la fecha de nacimiento, fecha de ingreso, fecha de alta, fecha de muerte, y todas las edades de más de 89, y todos los elementos de fechas (incluyendo el año) indicativos de tal edad, salvo que tales edades y elementos puedan ser agrupados en una sola categoría de 90 años o más.
4. Números de teléfono
5. Números de fax
6. Direcciones de correo electrónico
7. Números de seguro social
8. Números de historial médico
9. Numero de beneficiario de plan de salud
10. Números de cuenta
11. Certificado / números de licencia
12. Identificadores de vehículos y números de serie, incluyendo números de placas
13. Dispositivos con identificadores y números de serie
14. Direcciones de protocolo de internet (IP – por sus siglas en inglés)
15. Localizadores de recursos uniforme (URL's – por sus siglas en Inglés)
16. Identificadores biométricos, incluyendo huellas de dedos, retinas y voz
17. Fotografías de cara completa y cualquier imagen comparable
18. Cualquier otro número de identificación único, característico, o código, excepto se asigne otro código único para de identificar la data.

¿CUÁNDO ES NECESARIO EL CONSENTIMIENTO DE LA PERSONA SUJETO DEL ESTUDIO PARA USO DE DATOS SECUNDARIOS?

HIPAA: cuando la información privada de salud será revelada.

La persona debe estar informada de:

- La lista de los protocolos/investigaciones para los que será revelada su información.
- El propósito de los protocolos.
- Información que será revelada.
- Nombre e información de contacto del investigador(a).

✓ La autorización debe estar en un lenguaje sencillo y por escrito y usualmente por un término y propósito fijo.

GUÍA PARA EVALUAR PROTOCOLOS CON DATOS SECUNDARIOS

1. Indicar quién obtendrá la información de los expedientes y si esta persona está cualificada por la institución custodia y responsable de los expedientes.
2. Detallar la información que se obtendrá de los expedientes o banco de datos.
3. Señalar la relación de el(la) investigador(a) con la institución custodia de los expedientes.
4. En caso de la solicitud de la revisión regular del CIPSHI, si no va a obtener el consentimiento informado de los participantes, tiene que solicitar y justificar una dispensa en el proceso estándar de toma de consentimiento (sección IX de la solicitud).
5. Presentar evidencia o carta de endoso de la institución custodia de los expedientes que incluya lo siguiente o según aplique a los requisitos de la institución:
   - ✓ Si aplicara, que autoriza a el(la) investigador(a) a revisar los expedientes clínicos o fuente de los datos y que el(la) investigador(a) ha firmado un acuerdo de confidencialidad.
   - ✓ Información o data que se obtendrá del expediente, incluyendo si es o no información identificable o protegida por el Health Insurance Portability and Accountability Act (HIPAA).
   - ✓ Autorización para la dispensa del consentimiento informado de las personas a las que le pertenece la información del expediente.
   - ✓ Autorización del Institutional Review Board (IRB), HIPAA Privacy Board o del Privacy Official de la institución, según aplique, o declaración que no es un requisito de la institución para proveerle acceso a el(la) investigador(a) a los expedientes o a los datos. Observar que el CIPSHI no es un HIPAA Privacy Board por lo que el(la) investigador(a) es responsable de obtener los permisos institucionales pertinentes.

REVISIÓN DE PROTOCOLOS CON DATOS RECOPILADOS O SECUNDARIOS

- **Investigaciones que pueden cualificar como exentas de la revisión regular del CIPSHI:**

  Categoría #4

  Una investigación que involucre la recopilación o el estudio de datos existentes, documentos, expedientes, muestras patológicas o diagnósticas, si esas fuentes están disponibles públicamente o si el(la) investigador(a) recoge la información de tal manera que los sujetos no pueden ser identificados, ya sea directamente o a través de identificadores ligados a los sujetos.

- **Categoría de investigación que puede ser revisada mediante el procedimiento expedito:**

  Categoría #5.

  Investigación con materiales (datos, documentos, muestras, expedientes) que fueron recopilados para cualquier propósito o que serán recopilados sólo para propósitos no relacionados a la investigación (como tratamiento médico o diagnóstico).

ALMACENAMIENTO DE LOS DATOS

- Lugar seguro: físico (archivo, oficina, residencia) o digital (computadoras, *pendrives*, nubes, teléfonos. Ventajas y limitaciones de cada medio.
- Separación de los identificadores de la información recopilada. Por ejemplo, guardar por separado las hojas de consentimientos firmadas y los cuestionarios o banco de datos; guardar en archivos separados la lista con la información de contacto o ID del participante de la información sensitiva.
- Archivos con llave, archivos digitales con contraseñas o encriptadas.
- Conservación por el tiempo convenido con los(as) participantes. Información muy sensible podría requerir un tiempo más limitado. Por ejemplo, borrar las grabaciones inmediatamente después de su transcripción.

DATA SECURITY PLAN DEVELOPMENT GUIDE FOR RESEARCHERS

- http://www.appam.org/assets/1/7/APPAM_Abt_Data_Security_Plan_Development_Guide_Nov_2014.pdf

- November 2014. Prepared for: Association for Public Policy Analysis and Management Fall Research Conference Submitted by: Sean Owen, CISSP, CAP and Teresa Doksum, Ph.D., M.P.H. Abt Associates Inc. 4550 Montgomery Avenue Suite 800 North Bethesda, MD 20814

Researchers can use either a table or narrative format for this section.

Description of Data		
Data Source	Identifiers Needed	Type of Data
EXAMPLE: Primary data collection (e.g., survey, interviews, focus groups)	• E.g., Student first/last name	• Satisfaction with program (see attached survey)
EXAMPLE: Secondary/extant data (e.g., administrative data)	• E.g., Student first/last names	• School records (grades for 2013)
	•	•
	•	•

Pathway of Physical Records (each row is one step data travels)						
Source of Data	Summary of Data Types	Destination	Transport		Storage (Destination)	Return or Destruction Plan
E.g., program staff	Interview data	Researcher	☒ Paper (interview notes)	☐ USPS (Registered) ☐ UPS ☐ FedEx from site ☐ Licensed/bonded carrier ☒ Hand-delivery/carry by study member	Researcher organization locked cabinet	Shred 3 yrs after end of study
e.g., program participant	Survey data (no PII)	Researcher	☒ Paper	☐ USPS (Registered) ☐ UPS ☒ FedEx ☐ Licensed/bonded carrier ☐ Hand-delivery by study member	Researcher organization locked cabinet	Return to funder at end of study via Fed-Ex

Deliverables		
Data Sources	**Deliverable**	**Any restrictions from data agreements?**
X	• E.g., Quarterly reports highlighting key process and outcome trends associated with grantee's efforts to provide services to clients; • E.g., Annual reports detailing key trends with grantees grantee service progress and outcomes.	e.g., draft needs to be shown to school districts first
Survey Data	• E.g., data sets like restricted use dataset or public use dataset	e.g., Re-identification risk must be minimized per industry standards

CONFIDENCIALIDAD AL PUBLICAR LOS RESULTADOS

- Usar datos agrupados.
- Usar rangos o categorías amplias.
- Generalizar las características de la población, grupo o individuo.
- Evitar ofrecer información de una o muy pocas personas.
- Usar códigos o seudónimos.
- Ofrecer información parcial o distorsionada.
- Limitar la publicación de trascripciones completas o extractos extensos.
- Distorsionar rostros, voces, características únicas como cicatrices o tatuajes.

La publicación de la información deben ser consistente con lo autorizado por los participantes.

SECCIONES DE LA SOLICITUD DE REVISIÓN DEL PROTOCOLO RELACIONADO CON LA PRIVACIDAD Y CONFIDENCIALIDAD

Sección	Información
II-D	Describa detalladamente los procedimientos a los que los/as participantes se someterán.
III-A.	Número anticipado de participantes
III-C	Criterios de inclusión y exclusión de los/as participantes
III-D	Poblaciones vulnerables o especiales incluidas en la investigación
IV-A	Descripción de cómo se identificarán, contactarán y reclutarán a los/as participantes
IV-E	Relación de los/as participantes con el/a investigador/a
IV-F	Relación de el/la investigador/a con la institución donde se realiza la investigación
VI-A	Riesgos de la investigación
VI-B	Medidas a tomarse para minimizar los riesgos
VI-E	Seguimiento a los/as participantes: Indique si dará seguimiento a los/as participantes durante la investigación o una vez culmine la recopilación de los datos de la investigación. De haber un seguimiento, explique el propósito y el procedimiento así como los posibles riesgos o incomodidades para los participantes asociados con el seguimiento. (La Hoja de Consentimiento Informado debe incluir esta información).

Sección	Información
VII-A	Medidas que se tomarán para proteger la privacidad de los/as participantes durante el contacto inicial, el reclutamiento y la recopilación de los datos: Describa detalladamente las medidas que se tomarán para proteger y mantener la privacidad durante el contacto inicial, el reclutamiento y la recopilación de los datos. (La Hoja de Consentimiento Informado debe incluir esta información.) Distinga lo confidencial de lo anónimo. Si aplicara, indique si va a utilizar información pública y explique la naturaleza de la información pública.
VII-B	Medidas que se tomarán para mantener la confidencialidad de los datos durante su análisis, publicación y almacenamiento: Describa detalladamente las medidas que se tomarán para mantener la confidencialidad de los datos durante su análisis, publicación y almacenamiento. Incluya los nombres del personal de la investigación que tendrán acceso a los datos crudos de los participantes (datos con identificadores directos o indirectos). Los/as supervisores de las investigaciones de los/as estudiantes tienen que tener acceso a los datos crudos. Establezca si los datos crudos, incluyendo las hojas de consentimiento/asentimiento, se harán accesibles a otras personas que no sean el/la investigador principal y el personal clave de la investigación. En tal caso, indique quién, cómo y por qué otras personas tendrán acceso a estos datos. Describa el procedimiento para compartir los datos y cómo se le informará al participante que los datos podrían compartirse. Especifique si los datos que se compartirán contienen información que pueda identificar a los participantes. Además, indique las medidas a tomarse para garantizar la confidencialidad de los datos en la publicación de los resultados de la investigación. Por el contrario, si la investigación requiere que la identidad de los participantes sea revelada, indíquelo y explíquelo.

Sección	Información
VII-C.	Almacenamiento de los documentos, materiales y datos: Señale la persona o personas que custodiará los documentos y datos y cómo, dónde y por cuánto tiempo serán almacenados. Especifique si el periodo de almacenamiento difiere según el tipo de documento, dato o información (base de datos digital, cuestionarios, grabaciones, trascripciones, fotos, muestras biológicas, hojas de consentimiento/asentimiento, etc.). Incluya cómo se destruirán los datos según el tipo de documento, dato o información. Nótese que los documentos y datos deben conservarse por un periodo de tiempo determinado por la profesión, agencia patrocinadora, asociación profesional o departamento al cual pertenece el/la investigador/a. Es responsabilidad de el/la investigador/a cumplir con los requisitos establecidos. En términos del CIPSHI, se requiere que las hojas de consentimiento y asentimiento se conserven por un periodo mínimo de tres (3) años luego de finalizado el estudio y se recomienda que los otros documentos y datos se almacenen por un mínimo de tres años luego de que concluya la investigación. (La Hoja de Consentimiento Informado debe incluir esta información.)

Sección	Información
VII-D.	Uso de fotos y grabaciones de audio o video: Indique el uso que se le dará a las fotos o a las grabaciones de audio o video. Incluya si el tiempo y condiciones de archivo de las fotos o grabaciones son diferentes al señalado en el inciso VII-C. Observe que ciertos formatos de grabación tienen que ser borrados antes de destruirse. (El uso y la manera de disponer de las grabaciones deben explicarse en la hoja de consentimiento.)
VII-E.	Archivo permanente de la información o datos crudos: Señale si la información o datos crudos recopilados se guardarán permanentemente en un expediente, un record médico, un banco de datos, una biblioteca, etc. Justifique y especifique qué información o datos se conservarán. Identifique quién custodiará la información, quién tendrá acceso a la misma y el uso que se le dará aparte de la descrita en este protocolo. Incluya si con la información que se conservará se podrá identificar directa o indirectamente a los/as participantes. (La Hoja de Consentimiento Informado debe incluir esta información.)
VIII-E.	Persona que tomará el consentimiento informado
IX	Solicitud de dispensa en el consentimiento informado estándar
IX.B	Exención de la firma en la hoja de consentimiento o asentimiento
IX.D	Restricción de la información a proveerse a el/la participante

ERRORES MÁS COMUNES EN EL MANEJO DE LA PRIVACIDAD Y CONFIDENCIALIDAD EN LA SOLICITUD Y CONSENTIMIENTO

- Confundir privacidad y confidencialidad.
- Confundir anonimato y confidencialidad.
- Información incompleta:
  - Sobre el tiempo de conservación de los datos, documentos o materiales. Estos materiales pueden tener diferentes tiempos de almacenamiento.
  - No especifican el tiempo de conservación; indican “mínimo o máximo de X años”.
  - Indicar que el CIPSHI requiere que los datos sean conservados por un mínimo de tres años. El CIPSHI solamente establece que las hojas de consentimientos firmadas tienen que ser conservadas por un mínimo de tras años luego de finalizada la investigación.
  - No identifican a todas las personas que podrán tener acceso a los datos crudos de la investigación.
  - No especifican el propósito o usos de las grabaciones.
  - Medidas de seguridad extremas para investigaciones cuya información no es tan sensitiva.

TERMINACIÓN DEL PROTOCOLO

- Un protocolo de investigación concluye cuando se **completa**, se **transfiere** a otra jurisdicción o se **cancela**.
- Para propósitos del CIPSHI, un protocolo se considera **completado** cuando:
  - La interacción con los(as) participantes y la recopilación de datos ha concluido, se ha realizado un análisis primario de la investigación y se concluye que no es necesario volver a la fuente original que contiene la identidad de los/as participantes (persona, expedientes, datos crudos, listado de participantes, etc.) para recopilar más información.*
  - En los proyectos de investigación de estudiantes como **tesis y disertaciones**, el protocolo se considera **terminado** cuando la tesis o disertación es aprobada por su correspondiente comité o programa de estudio.
- Antes de dar por terminado un protocolo, el/la investigador/a también tiene que considerar las especificaciones de las agencias que regulan o financian la investigación que pueden requerir que el protocolo permanezca activo por un período más extenso.
- **Los datos y materiales de la investigación tienen que conservarse según las condiciones y por el tiempo establecido en el protocolo autorizado por el CIPSHI.**

LOCALES

1

Se hereda la responsabilidad de disponer de récords médicos

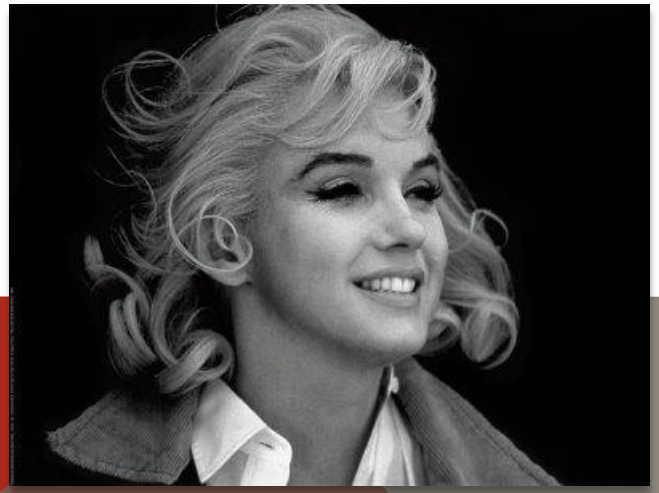
Presidente del Colegio de Médicos Cirujanos cataloga como imperdonable el hallazgo de expedientes médicos encontrados en un terreno baldío de Dorado

domingo, 5 de abril de 2015 - 11:58 PM | Por Aurora Rivera Arguinzoni | 21 | 3 | Guardar

El Departamento de Salud (DS) incautó cajas con cientos de documentos clínicos que mostraban datos de pacientes como fecha de nacimiento, dirección, teléfono y número de póliza de planes médicos. (Vanessa Serra)

La confidencialidad entre proveedores de salud y pacientes es tan sagrada como el secreto de confesión que deben guardar los sacerdores, y violarla tirando los expedientes debe ser castigado con las máximas penas posibles, afirmó ayer el presidente del Colegio de Médicos Cirujanos de Puerto Rico, doctor Víctor Ramos Otero.

"Tienen que investigar hasta las últimas consecuencias. Es imperdonable que información privada del paciente quede expuesta. Esto es como la confesión. Es inaceptable e imperdonable que expedientes no se hayan dispuesto de la manera correcta. Hay que buscar quién fue responsable e imponerle todas las sanciones posibes, ya sean administrativas, civiles e incluso penales. El Colegio no condona este tipo de acto", afirmó en entrevista con El Nuevo Día.



"Si eres cuidadoso con la gente y si respetas su privacidad, te ofrecerán una parte de ellos mismos que podrás usar."

Eve Arnold (fotógrafa)

PROCEDIMIENTOS REVISIÓN CONTINUA DE LOS PROTOCOLOS APROBADOS POR EL CIPSHI

Solicitud de revisión inicial:
Vigencia máxima de la aprobación:
1 año

Solicitud de modificación:
Autorización del CIPSHI

Solicitud de renovación:
Autorización del CIPSHI

Notificación de incidentes adversos o no anticipados:
Evaluación del CIPSHI

Notificación de Terminación del Protocolo

ENVÍO POR CORREO ELECTRÓNICO DE SOLICITUDES Y NOTIFICACIONES

- ✓ Para aceptar la solicitud por vía electrónica es necesario que acompañe los documentos requeridos con la página digitalizada de las certificaciones con las firmas correspondientes.
- ✓ Los documentos deben estar en formato Word o PDF.
- ✓ Puede enviar la solicitud por vía electrónica al correo electrónico cipshi.degi@upr.edu.

WEBPAGE CIPSHI:

- Trasfondo histórico y Bases legales
- Aplicabilidad
- Procedimientos y formularios
- Categorías expeditas
- Categorías exentas
- Consentimiento Informado
- Educación y adiestramiento
  - Adiestramiento requerido
  - Otros requisitos
  - Orientaciones
  - Enlaces Útiles
  - Definiciones
  - Errores más comunes
- Comité
  - Miembros
  - Responsabilidades
  - Calendario de reuniones
- Responsabilidades
  - Institucionales
  - CIPSHI
  - Investigadores/as
  - Supervisores/as de la investigación
  - Directores/as de departamentos, centros u oficinas del Recinto
  - Coordinadores/as de programas graduados

ADIESTRAMIENTO

Educación inicial:

- **CITI Progam** (Collaborative Institutional Training Initiative) con una vigencia de tres años o menos de haberse emitido el certificado.
- El adiestramiento de NIH, **Protección de los participantes humanos en la investigación**, solamente será aceptado si al 1º de agosto de 2014, el certificado tiene tres años o menos.

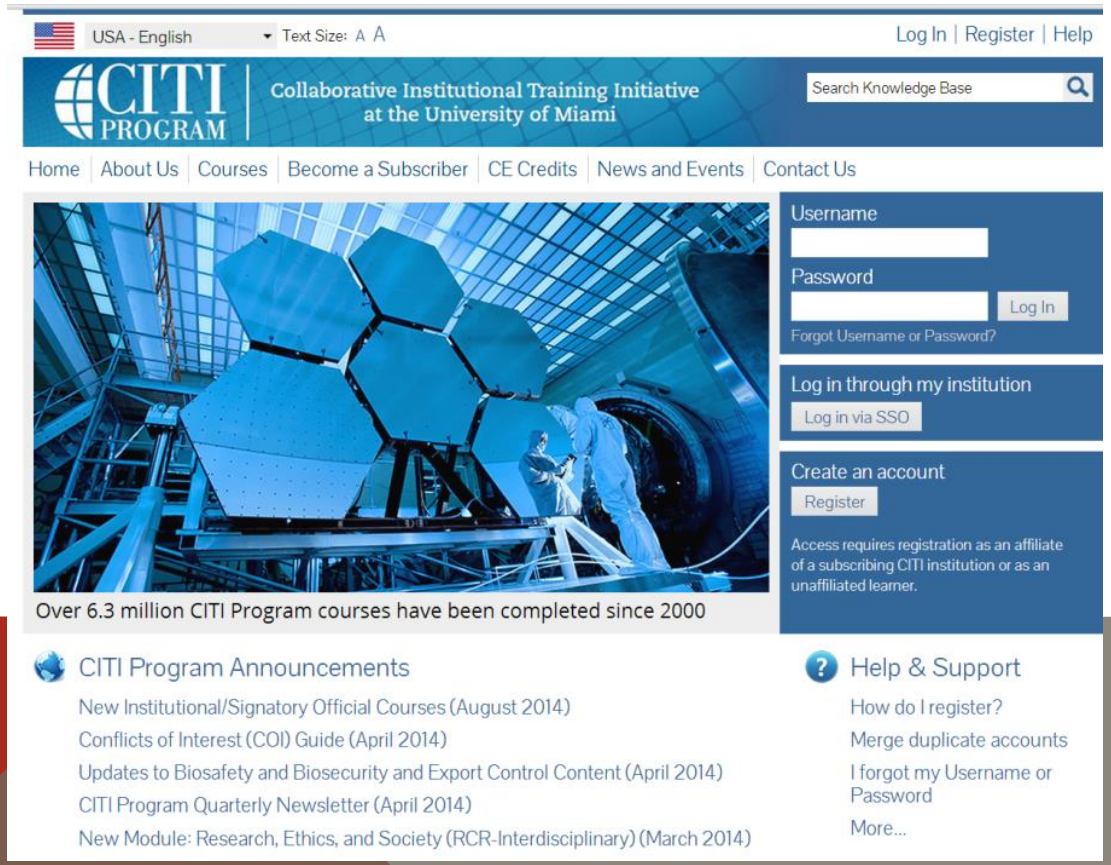
Educación continua:

Los(as) investigadores(as) y el personal clave con certificados de la educación inicial expirados podrán optar por varias alternativas como **educación continua**:

- Tomar uno de los adiestramientos iniciales o continuos sobre investigaciones con seres humanos del CITI Program.
- Tomar o retomar el adiestramiento de NIH: Protección de los participantes humanos en la investigación. Para retomar el adiestramiento, seguir las instrucciones de "retomar el curso" en la sección "Editar información del usuario".
- Participación en las orientaciones y talleres sobre el CIPSHI ofrecidos por el DEGI.
- Presentar evidencia de participación de otras actividades como conferencias, foros, talleres o adiestramiento en línea relacionados con la investigación con seres humanos como sujetos de estudio.

CITI PROGRAM

https://www.citiprogram.org



Puede accederse en computadora, tabletas y teléfonos inteligentes.

CITI PROGRAM

- **Registro:**
  - ✓ **7 pasos**
  - ✓ Para registrarse, localice nuestra institución con su nombre en español "**Universidad de Puerto Rico, Recinto de Río Piedras**".

- **Curso requerido por el CIPSHI: <u>Uno</u>** (1)de los cursos indicados en el Paso 7 ("Select Curriculum"):
  *Question **1**: Human Subject Research* **<u>o</u>**
  *Question **6**: Investigación con seres humanos*

¿CÓMO ACCEDER AL CIPSHI?

Dirección física:	Hogar Masónico 2do Piso
Dirección postal:	PO Box 21790 San Juan Puerto Rico 00931-1790
Teléfono:	787-764-0000 Ext. 86700
Fax:	787-763-6011
Correo electrónico:	cipshi.degi@upr.edu
Página electrónica:	http://graduados.uprrp.edu/cipshi

CICLO DE ADIESTRAMIENTOS CEA INVESTIGACIÓN CON SERES HUMANOS

Centro para la Excelencia Académica:

- http://cea.uprrp.edu/

Talleres:

- Investigación con seres humanos
- Consentimiento informado
- Privacidad y confidencialidad
- Conflicto de interés
- Cine Foros

WHAT ARE QUALITATIVE RESEARCH ETHICS?

- Wiles, R. (2013). *What are Qualitative Research Ethics?* (The 'What is?' Research Methods Series). London: Bloomsbury Academic. Retrieved September 20, 2016, from http://dx.doi.org/10.5040/9781849666558

- https://www.bloomsburycollections.com/book/what-are-qualitative-research-ethics/

PRIVACY AND CONFIDENTIALITY

- Módulos con temas específicos sobre la privacidad y confidencialidad.

  - ✓ *Current Issues in Research Ethics* (CIRE). Columbia University's Center for Bioethics.

  - ✓ http://ccnmtl.columbia.edu/projects/cire/pac/foundation/index.html

ENLACES ÚTILES

- Office for Human Research Protections (OHRP):

  http://www.hhs.gov/ohrp

  Canal de videos educativos
  - https://www.youtube.com/playlist?list=PL5965CB14C2506914

- **Búsqueda recomendada en YouTube: Human Research Ethics**