Privacidad y confidencialidad en la investigación con seres humanos como sujetos de estudio

Myriam L. Vélez Galván

21 de febrero de 2020

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

PRESUNCIÓN DE INCLUSIÓN DE GÉNEROS: Todos los títulos, los puestos y las funciones incluidas en esta presentación son aplicables a ambos géneros por igual, ya que pueden referirse o ser ocupados o ejecutados por hombres o mujeres, indistintamente.

Contenido

- ✓ Principios éticos
- ✓ Regulaciones, normativas, definiciones
- ✓ Riesgos
- ✓ Privacidad y confidencialidad:
  - Identificación y contacto inicial
  - Toma de consentimiento informado
  - 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

La integridad y la conducta responsable en la investigación comprende el conocimiento y atención en varias áreas:

Principios Éticos:
Informe Belmont (1979)

☑ 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 voluntarios y la población a beneficiarse de los resultados.

Principios éticos: Declaración Bioética y Derechos Humanos de la UNESCO (2005)

- ☑ 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

Códigos de ética de profesiones

Organización	Enlace
American Anthropological Association	https://s3.amazonaws.com/rdcms-aaa/files/production/public/FileDownloads/pdfs/issues/policy-advocacy/upload/ethicscode.pdf
American Educational Research Association	http://www.aera.net/About-AERA/AERA-Rules-Policies/Professional-Ethics
American Medical Association	https://www.ama-assn.org/delivering-care/code-medical-ethics-research-innovation
American Psychological Association	http://www.apa.org/ethics/homepage.html
American Sociological Association	https://www.asanet.org/code-ethics
American Statistical Association	https://www.amstat.org/ASA/Your-Career/Ethical-Guidelines-for-Statistical-Practice.aspx
Asociación de Psicología de Puerto Rico	https://www.asppr.net/reglamento
Colegio de Trabajadores Sociales de Puerto Rico	http://cptspr.org/wp-content/uploads/2016/11/Co%CC%81digo-de-E%CC%81tica-2017-REV050317web.pdf
National Association of Social Workers	https://www.socialworkers.org/About/Ethics/Code-of-Ethics/Code-of-Ethics-English
Oral History Association: Principles and Best Practices	http://www.oralhistory.org/about/principles-and-practices/
Data Science Association	https://www.datascienceassn.org/code-of-conduct.html

Regulaciones o normativas aplicables

- **Internacionales**
- **Federales**
  - 45 CFR 46 (directrices para IRBs)
  - Otras (FDA, HIPAA, FERPA, PPRA, etc.)
- **Estatales**
- **Institucionales**
  - ✓ UPRRP: Comité Institucional para la protección de los Seres Humanos en la Investigación (**CIPSHI**)
  - ✓ Otros: Departamento de Educación, Departamento de la Familia, otros IRBs, etc.

Sujeto Humano: Definición

Individuo vivo sobre el que un investigador (ya sea profesional o estudiante) realiza una investigación y obtiene:

- obtiene **información** o **muestras biológicas** a través de la **intervención** o **interacción** con el individuo, y usa, estudia o analiza la información o muestras biológicas; u
- **obtiene, utiliza, estudia, analiza o genera** información privada identificable* o muestras biológicas identificables.

*Identificable directa o indirectamente.

Definición de información privada en 45 CFR 46

- La **información privada** incluye información sobre el comportamiento que ocurre en un contexto en el que un individuo puede esperar razonablemente que no se realice ninguna observación o registro, y la información que ha sido provista para fines específicos por un individuo y que el individuo puede esperar razonablemente que no se haga pública (por ejemplo, un expediente médico).

Definiciones de información privada identificable en 45 CFR 46 (2)

- La **información privada identificable** es información privada para la cual la identidad del sujeto es o puede ser fácilmente determinada por el investigador o asociada con la información.

- Una **muestra biológica identificable** es una muestra biológica para la cual el investigador puede o puede determinar fácilmente la identidad del sujeto o asociarla con la muestra biológica.

Criterios principales para la aprobación de 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 disposiciones adecuadas para proteger la privacidad de los sujetos y mantener la confidencialidad de la información o datos.**

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 identificable no será divulgada.
- **Anonimato:** la identidad de la persona no se puede establecer directa ni indirectamente.
- Certificados de confidencialidad (NIH): Protege al investigador de revelar información sensitiva identificable de los participantes.

Límites a la confidencialidad

- Confidencialidad limitada por la ley.
- Objetivo de la investigación es divulgar la identidad o fuente de la información al público en general.
- Metodología para la recopilación de los datos. Investigador no tiene control sobre la información compartida (ej. grupos focales).
- Medio de recopilación de los datos (ej. cuestionarios o data vía electrónica).
- Características particulares o cantidad de participantes.
- Uso y manejo de la información: interés en compartir datos con otros investigadores.
- Requisitos institucionales del lugar donde se reclutan a los participantes.

Información o datos

- Información de contacto (teléfono, dirección postal, residencial o electrónica, nombre de usuario, etc.)
- Hojas de consentimiento informado firmadas
- 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

Tipos de información o datos

- Datos crudos: información primaria que no ha sido procesada.
- Datos secundarios
- Datos con 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 sin identificadores:
  - De-identificados
  - Anónimos

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 | Tecnología | 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.

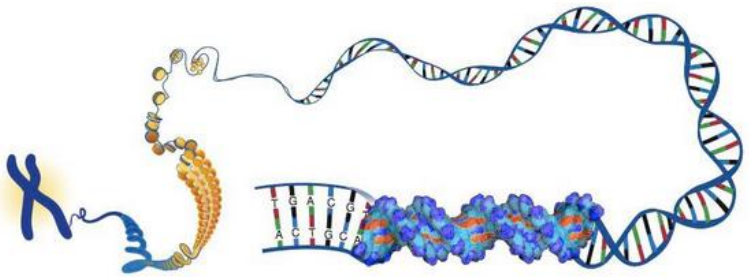
El profesor Alessandro Acquisti, autor del estudio, también descubrió que alrededor de 27% de las veces, y usando datos extraídos de perfiles de

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.**



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.

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** del daño o la incomodidad anticipada en la investigación no son mayores en sí mismas que las que se encuentran habitualmente en la vida diaria o durante la realización de exámenes o pruebas físicas o psicológicas de rutina.

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
- pérdida de servicios o beneficios
- límites en el progreso educativo
- **invasión de la privacidad**
- **ocurrencia de una brecha en o violación de la confidencialidad**

Riesgos (3)

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

endi
ELNUEVODIA.COM

Tecnología

Buscar

Acceda a la Edición Electrónica

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

CONSUMO | FINANZAS | AUTOS | BANCA | TECNOLOGIA | EMPRESAS | ECONOMIA

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/

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

BUSINESS 01/24/2019 03:51 am ET

24 Million Mortgage And Bank Loan Documents Leaked Online

The unsecured server contained loan and mortgage agreements, repayment schedules and other highly sensitive financial and tax documents.

TechCrunch

CNYTHZL VIA GETTY IMAGES

A trove of more than 24 million financial and banking documents, representing tens of thousands of loans and mortgages from some of the biggest banks in the U.S., has been found online after a server security lapse.

The server, running an Elasticsearch database, had more than a decade's worth of data, containing loan and mortgage agreements, repayment schedules and other highly sensitive financial and tax documents that reveal an intimate insight into a person's financial life.

d with a password, allowing anyone to access and read the massive

TRENDING


Alexandria Ocasio-Cortez Has 3 Burning Questions For Sean Hannity And Fox News


'Folded Like A Cheap Suit': Twitter Users Taunt Trump For Being 'Outplayed' By Pelosi


Anderson Cooper Mocks Kellyanne Conway's Bonkers New Rant On Trump's Wall


Sen. Joni Ernst Says She Was Raped In College


Cambridge
Analytica


facebook
Accused of mishandling
data of 50M+ users

EL PAÍS TECNOLOGÍA SUSCRÍBETE

REDES SOCIALES

Facebook deja al descubierto más de 540 millones de datos de usuarios

Una aplicación de terceros almacenaba información sin cifrar en un servidor de Amazon

JOSÉ MENDIOLA ZURIARRAIN

4 ABR 2019 - 19:44 CEST

El máximo responsable de Facebook, Mark Zuckerberg, el pasado martes en Dublín tras un encuentro sobre regulación de la red social. NIALL CARSON (PA WIRE/PA IMAGES)

Aunque cueste creerlo y pese a las declaraciones de Mark Zuckerberg, **Facebook** sigue sufriendo brechas en la salvaguarda de datos privados de sus usuarios. Hace tan solo unas horas se ha conocido que los datos de más de 540 millones de datos de abonados a la red social han estado al descubierto durante no se sabe cuánto tiempo en unos servidores accesibles a cualquier usuario. La última y gravísima vulneración de la privacidad fue descubierta por la compañía de seguridad UpGuard, que detectó a comienzos de año la existencia de dos masivas bases de datos alojadas en servidores de Amazon AWS sin ningún tipo de protección y conteniendo datos de usuarios de la red social. UpGuard notificó en hasta tres ocasiones esta situación, pero no ha sido hasta hace dos días que se ha protegido este contenido.

https://elpais.com/tecnologia/2019/04/04/actualidad/1554372746_414151.html

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.

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 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 sensitiva (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 (por ejemplo grabaciones y fotos, extractos o trascripciones de entrevistas, etc.) y cómo se aludirá al participante
- Si no es posible garantizar la confidencialidad.
- Límites a la confidencialidad: intención, legal, metodológica, cantidad de participantes, características únicas de la persona, etc.
- Usos futuros o cesiones de derechos de autor.

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 supervisor 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 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 investigador no puede garantizar que la información compartida no sea revelada por los participantes.
- Límites a la confidencialidad por las características únicas de los 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.
- Informar si recopilará direcciones electrónicas, o de IP u otra información identificable o rastreable, especialmente cuando esta información no está en el formulario.
- 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, piratas informáticos , hackers, etc. Además, en la computadora que utilice puede quedar registro de la información que acceda o envíe por Internet.*

Lenguaje recomendado en el modelo de HCI para resumir uso, conservación y manejo de la investigación

- Los documentos, materiales o datos de la investigación serán almacenados (explique condiciones de almacenamiento). Los (documentos, materiales o datos que conservará por un periodo fijo) recopilados serán conservados por (cantidad de tiempo) años una vez finalizada la investigación. (Los datos digitales serán borrados y los impresos triturados antes de desecharse.) Los (documentos, materiales o datos que conservará indefinidamente) serán conservados permanentemente para ser utilizados en otras investigaciones. Además, serán compartidos con otros investigadores. (Explique las condiciones para compartir los datos en términos de si serán con o sin identificadores o compartidos bajo un acuerdo de confidencialidad).

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 del participante.
  - **Protección de la identidad del participante.**
  - Se le proveerá información apropiada al participante.

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

45 CFR 46§46.117 Documentación del consentimiento informado

- (c) Un IRB podrá dispensar al investigador de obtener una hoja de consentimiento firmada de algunos o todos los sujetos si encuentra alguno de los siguientes:

  (1) El único registro que vincula al sujeto con la investigación es la hoja de consentimiento informado y el riesgo principal sería el daño potencial relacionado con una violación de la confidencialidad. **A cada sujeto (o representante legalmente autorizado) se le preguntará si desea que exista documentación que relacione al sujeto con la investigación, y su deseo deberá ser respetado…**

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.

Información de salud o médica protegida (Protected Health Information-PHI) - Health Insurance Portability and Accountability Act (HIPAA) (2)

4. Números de fax
5. Números de teléfono
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

Información de salud o médica protegida (Protected Health Information-PHI) - Health Insurance Portability and Accountability Act (HIPAA) (3)

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.

✓ 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 investigador con la institución custodia de los datos o expedientes.
4. 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. Si aplica, evidencia del permiso de uso de la información (por ejemplo, hoja de consentimiento informado).

Guía para evaluar protocolos con datos secundarios (2)

5. Presentar evidencia o carta de endoso de la institución custodia de los datos o expedientes que incluya lo siguiente o según aplique a los requisitos de la institución:
   - ✓ Si aplicara, que autoriza a el investigador a revisar los expedientes clínicos o fuente de los datos y que el investigador 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 al investigadora los expedientes o a los datos. Observar que el CIPSHI no es un HIPAA Privacy Board por lo que el investigador es responsable de obtener los permisos institucionales pertinentes.

(21/May/2016) Datos personales de 70.000 usuarios de OkCupid fueron dados de baja después de orden de la DMCA

La semana pasada, sin el permiso de los usuarios, investigadores daneses liberaron públicamente los datos de 70.000 perfiles de OkCupid, incluyendo nombres de usuario, edad, género, ubicación, el tipo de relación (o el sexo) que les interesa, rasgos de personalidad, y respuestas a miles de preguntas perfiladas utilizadas por el sitio.

El viernes, el Open Science Framework (OSF) eliminó los datos tras una denuncia de la Digital Millennium Copyright Act (DMCA) por parte de OkCupid.

http://www.globalcybersec.com/reader.php?p=1704

Kirkegaard dijo que los investigadores se sorprendieron de la protesta:
"Que no anticipamos ninguna reacción fuerte, no. Quisimos contribuir con un buen conjunto de datos abiertos a la ciencia, no queríamos ser famosos por ello".

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 participantes. Información muy sensitiva 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)
	•	•
	•	•

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 divulgación de trascripciones completas o extractos extensos.
- Distorsionar rostros, voces, características únicas como cicatrices o tatuajes.

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

Ejemplos de información identificable:

- Divulgación del extracto de la entrevista: "El incidente de violencia fue en la nochebuena del 2017. Esa misma noche fui al cuartel de Maricao y denuncié a mi pareja." (caso ficticio.)

- Descripción de los participantes: "Los participantes son los directivos de las escuelas de arquitectura de Puerto Rico." En los resultados se comparan las instituciones privadas con las públicas.

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 participantes se someterán.
III-A.	Número anticipado de participantes
III-C	Criterios de inclusión y exclusión de los participantes
III-D	Poblaciones vulnerables o especiales incluidas en la investigación
IV-A	Descripción de cómo se identificarán, contactarán y reclutarán a los participantes
IV-E	Relación de los/as participantes con el investigador
IV-F	Relación de el investigador 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 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 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 participante

VII-D. Uso, almacenamiento de los documentos, materiales y datos:

- **Documentos, materiales o datos que conservará por <u>tiempo limitado</u>:**

Persona responsable o custodia:			
⇨ Documento, material o datos ⇨ Con/sin identificadores	Tipo: impreso (papel), digital, biológico, etc.	Personas que tendrán acceso.	⇨ Tiempo de conservación ⇨ Lugar de almacenamiento ⇨ Disposición/desecho
Si es necesario, indique algún otro detalle relacionado:			

- **Documentos, materiales o datos que conservará <u>permanentemente</u>:**

Persona responsable o custodia:			
⇨ Documento, material o datos ⇨ Con/sin identificadores	Tipo: impreso (papel), digital, biológico, etc.	Serán o no compartidos con otros investigadores	Serán compartidos con o sin identificadores
Si es necesario, indique algún otro detalle relacionado:			

ERRORES MÁS COMUNES en el manejo de la privacidad y confidencialidad en la solicitud y consentimiento

- Confundir anonimato con confidencialidad.
- Confundir el proceso de recopilación de datos con el uso y divulgación de la información.
- 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.

ERRORES MÁS COMUNES en el manejo de la privacidad y confidencialidad en la solicitud y consentimiento (2)

- Información incompleta:
  - No incluir a todas las personas que podrán tener acceso a los datos crudos o identificables de la investigación.
  - No especificar el propósito o usos de las grabaciones.
  - No especificar posibles usos futuros de la información o datos.
  - 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 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 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.

Terminación del protocolo (2)

- Antes de dar por terminado un protocolo, el investigador 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.**

Almacenamiento y transmisión de los datos

- Nivel de seguridad o protección debe corresponder con la sensibilidad de la información o de los datos.
- Obtención y conservación solo de la información necesaria para los objetivos de la investigación.
- De-identificación de los datos para su almacenamiento.
- Almacenamiento de datos en nubes, dispositivos o computadoras con o sin acceso a Internet, etc.
- Acceso protegido mediante contraseñas o archivos bajo llave.
- Precauciones al compartir documentos o folders. Verificar que el destinatario sea la persona correcta.
- Protocolos de seguridad: SSL (Security Socket Layer), TLS (Transport Layer Security) u otros. Ej.: https:// vs http//.

LOCALES

1

Se hereda la responsabilidad de disponer de récords médicos

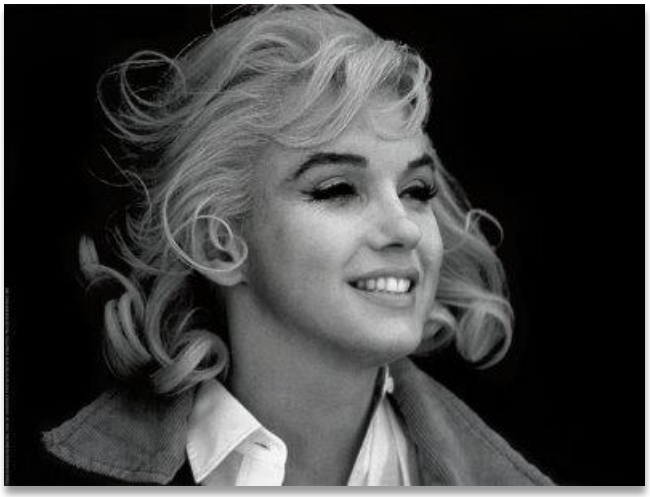
Presidente del Colegio de Médicos Cirujanos cataloga como imperdonable el hallazgo de expedientes médicos encontrados en un terreno baldío de Dorado

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)

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

Envío por correo electrónico de solicitudes y notificaciones

- ✓ Acompañar los documentos requeridos con la página digitalizada de las certificaciones con las firmas correspondientes.
- ✓ Los documentos deben estar en formato Word o PDF y como anejos ordenados en el mensaje electrónico.
- ✓ Puede enviar la solicitud por vía electrónica al correo electrónico cipshi.degi@.upr.edu.

Proceso de revisión inicial

Preevaluación:

Solicitud de información o documentos y determinación del tipo de revisión.
(Aproximadamente 5 días laborables.)

ADMINISTRATIVA
(Aprox. 7 días laborables)

↓

Enmiendas o aclaraciones

↓

AUTORIZACIÓN:
Declarada exenta de la revisión adicional del CIPSHI

CIPSHI

LIMITADA o EXPEDITA
(Riesgo mínimo.
Aprox. 15 días laborables)

COMITÉ EN PLENO
(Reunión mensual*).

Revisión diferida o autorización condicionada

↓

CONDICIONES COMPLETADAS Y VERIFICADAS

↓

AUTORIZACIÓN

*Notificación del resultado al investigador en aprox. 7 días laborales luego de la reunión.

Procedimientos revisión continua de los protocolos aprobados por el CIPSHI

GUÍA RÁPIDA: PÁGINA ELECTRÓNICA DEL CIPSHI

Procedimientos y formularios

- Revisión inicial
- Renovación
- Modificación
- Terminación de protocolo
- Determinaciones

Consentimiento

- Elementos
- Modelo
- Formato
- Dispensas

Errores más comunes

Enlaces de interés

Definiciones

Adiestramiento

Calendario de reuniones

Aplicabilidad

Responsabilidades

Trasfondo y bases

Miembros

Requisitos de otras instituciones

Información de contacto

Adiestramiento

Educación inicial:

- Curso de investigación con seres humanos del **CITI Progam** (Collaborative Institutional Training Initiative) con una vigencia de 5 años o menos de haberse emitido el certificado.

Educación continua:

- Cada 5 años.

Requerido al personal clave de la investigación:

- **Personal clave** incluye al investigador principal, coinvestigadores, supervisores de investigaciones de estudiantes, estudiantes, asistentes y empleados adscritos a una investigación que tendrán contacto directo con los participantes o mediante información privada que pueda identificarles directa o indirectamente.

CITI PROGRAM

https://www.citiprogram.org

- **Puede accederse en computadoras, tabletas y teléfonos inteligentes.**
- Registro bajo "Universidad de Puerto Rico – Recinto de Río Piedras"

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
  - Investigación con estudiantes o contexto académico
  - Cine Foros

Calendario de talleres

¿Cómo acceder al CIPSHI?

Dirección física:	Decanato de Estudios Graduados e Investigación (DEGI Hogar Masónico 2do Piso
Dirección postal:	18 Ave. Universidad STE 1801 San Juan PR 00925-2512
Teléfono:	787-764-0000 Exts. 86773 o 86700
Fax:	787-763-6011
Correo electrónico:	cipshi.degi@upr.edu
Página electrónica:	graduados.uprrp.edu/cipshi