El impacto de la privacidad y reglas de seguridad?
HIPAA

Power In-Service

Training Center | Your Sucess is our Priority

HIPAA - investigación general

- ¿Qué es HIPAA?
- ¿Por qué se creó?
- ¿Cuál es el impacto en la investigación clínica?
- WMC HIPAA formas y propósitos
- Regla de Seguridad HIPAA
- Recursos / Información de contacto

Que es HIPAA?

El Health Insurance Portability and Accountability Act: entró en vigor el 14 de abril 2003.

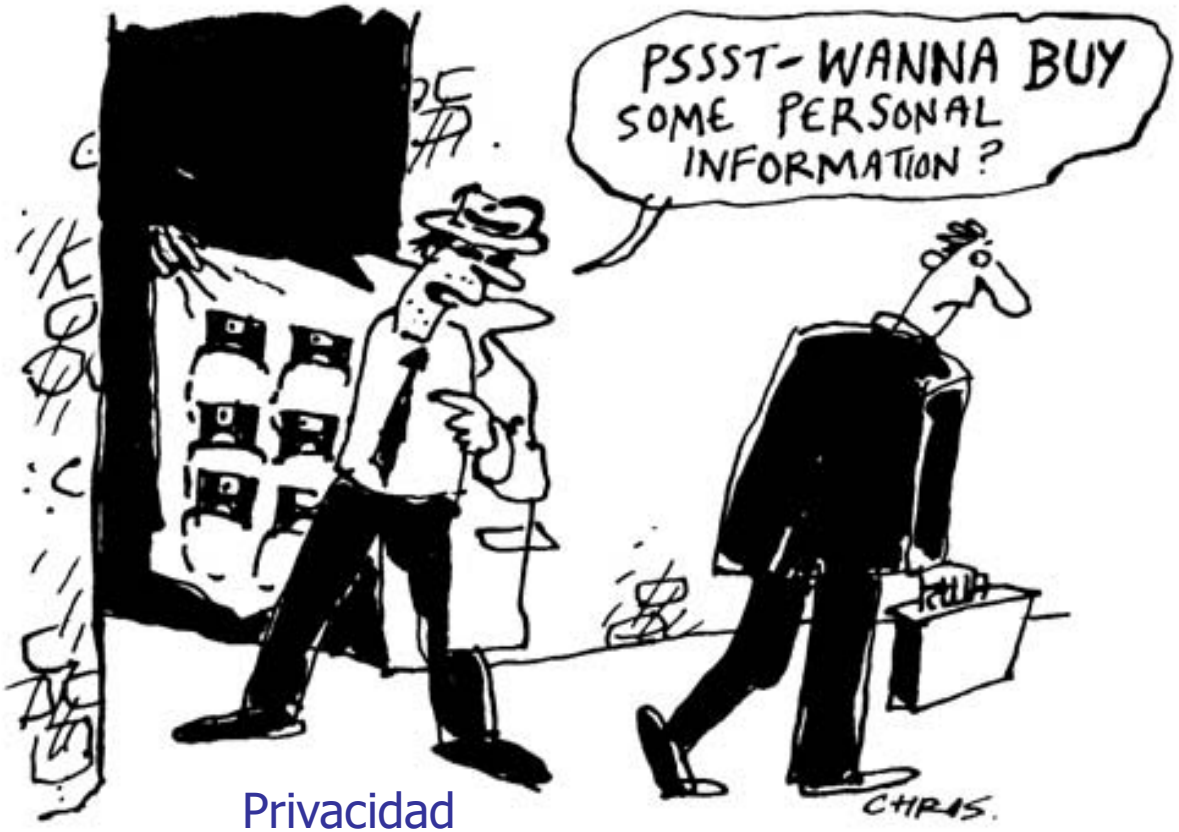
2 partes a HIPAA: La Regla de Privacidad HIPAA y la Regla de Seguridad HIPAA

HIPAA se aplica a todo tipo de papel (Norma de Privacidad) y electrónicos (Security regla) información de salud personal (PHI). PHI es cualquier documento o información electrónica que puede ser utilizada para identificar a un sujeto incluyendo su / su nombre, número de teléfono dirección, número de seguro social, o las fechas. Es cualquier información de salud personal almacenada en papel, en un ordenador, CD, disco o transmitida a través de Internet.

La regla se aplica a las "entidades cubiertas" (es decir, un centro de atención médica, plan de salud o un profesional de la salud que transmite cualquier información médica en forma electrónica en relación con las transacciones de la salud)

Un investigador se considera una "entidad cubierta" cuando él / ella provee servicios de salud que se cobra a un plan de seguro, además de la realización de la investigación.

Porque fue HIPAA creada?



Privacidad
Por Chris Slane

Porque fue HIPAA creada?

1. Administración Clinton: Para asegurar que la información de salud individual está protegida y que los individuos comprendan y controlen cómo su información de salud es usada

   La Administración de Bush: Elaboración de un plan de acción para digitalizar todos los registros médicos dentro de 10 años (una base de datos central).

   Que motivó a la creacion de esta?
   Los casos de los registros médicos electrónicos “hackeados” o manipulados o pirateados.
   The Associated Press encontró informed psicológicos de pacientes tirados junto con la basura.

Porque fue HIPAA creada?

Pivacidad! By Chris Slane

HIPAA:
Impacto en investigaciones clinicas

- Ahora pueden aplicar sanciones en caso de incumplimiento, tales como la acción institucional disciplinaria y / o sanciones monetarias
- Ocasiono camibios en el reclutamiento, la identificación de los sujetos participantes en el estudio y en como contactar a participantes potencialmente elegibles.
- La adición de la forma de Autorización HIPAA para ser firmado por los sujetos de investigación y otros documentos que ahora deben presentarse en la oficina de contabilidad IRB para HIPAA.
- Restricciones en donde médicos investigadores y su personal pueden buscar participantes potenciales.
- Una revision de como los records en papel o electrónicos pueden ser revelados.

HIPAA en otras instituciones calificadas

- Los componentes son los mismos (por regulaciones federales), pero la forma y la estructura de ejecución son diferentes de una institución a otra.

- HIPAA no es necesaria para el tratamiento, pago u operaciones. (Un punto comunmente mal entendido)

Las 8 WMC HIPAA disponibles

FORM 1: **HIPAA Authorization** to Use or Disclose PHI

- Cuando un estudio de investigación utiliza un formulario de consentimiento IRB, una forma HIPAA - Autorización firmada también puede ser necesaria además de cada sujeto (Formulario No. 1). Si un sujeto no firma el formulario de Autorización de él / ella no puede estar inscrito en el estudio y sus / sus datos no se puede utilizar.

  El formulario de autorización debe estar archivada en la oficina del IRB. El IRB debe tener toda la HIPAA.

  El no cumplir con HIPAA puede resultar en una acción disciplinaria institucional y gubernamentales sanciones pecuniarias.

HIPAA Authorization form *(continued)*

- Repository: The Principal Investigator (PI) plans on holding on to data/specimens collected during this study and using it for future research (a repository)

- Psychotherapy Notes: Doctor's notes about your psychotherapy sessions.

FORMS 2 & 3: **Request for Waiver** or Alteration of Authorization to Use or Disclose PHI

- RULES OF THUMB:
  - There are 3 kinds of Waivers:
    - 1) Complete: Not obtaining consent from subjects, no subject contact. Asking permission to 'Waive' obtaining consent from subjects to use PHI for a study. (ex) Retrospective chart review, study using waste material)
    - 2) Partial: Plan on obtaining consent once a subject is enrolled & consented. You are asking permission to *initially* 'Waive' obtaining consent from subjects in order to determine eligibility. ex) Chart review to determine eligibility
    - 3) Waiver for Coded Samples (FORM 3): Only role in the study is to process coded samples. Never plan on breaking the code.

FORM 4: Investigator Representation for Research on **De-Identified** PHI

PROTOCOLS NOT USING ANY OF THE 18 IDENTIFIERS BELOW:

- Names
- All geographic subdivisions smaller than a State (including street address, county, precinct, zip codes)
- All elements of dates (except year) for dates directly related to an individual; all ages over 89; and all elements of dates (including year) for ages over 89, except that all such ages and elements may be aggregated into a single category for age 90 or older
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers (i.e. DNA), including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

Investigator Representation for Research on De-Identified PHI *(continued)*

- Ask yourself: 'Is there any way anyone can ever figure out who a particular record/sample belongs to?' If the answer is 'yes' it does not qualify for this form. (most studies do not qualify for this form)

FORM 5: Investigator Representation for Research on Limited Data Sets (LDS) of PHI

- Data collected for a protocol must not contain any of the 16 identifiers listed on the form. (the only difference between Limited Data Set and De-Identified form is LDS Allows : 1) Elements of dates (i.e. city, state, zip code) 2) any unique identifying codes or characteristics not listed as direct identifiers and the De-Identified form does not.

- However: LDS must be used in conjunction with a Data Use Agreement

FORM 6: Data Use Agreement for A Limited Use Agreement

- A covered entity must use a Data Use Agreement with the researcher in order to provide a Limited Data Set to the an outside researcher/entity.
- The data use agreement defines the purposes for which the data will be used and obtains assurances from the researcher that it will not be re-disclosed, except under the same restrictions and conditions.
- Requires that the researcher will not attempt to identify or contact the individuals whose PHI is contained in the Limited Data Set.

FORM 7: Investigator Representation for Research on PHI of **Decedents**

- Use or disclosure solely for research on decedents' information.

- PHI is necessary for research, and the individual is a decedent, and provide documentation upon covered entity's request.

FORM 8: Investigator Representation for Review of PHI **Preparatory to Research**

- The use or disclosure of PHI is sought solely to prepare a protocol or for a similar preparatory purpose.
- PHI will not be removed from the covered entity. AND
- PHI is necessary for research purposes.

END OF HIPAA FORMS (Whew!)

Hodgepodge HIPAA

- The 'Grandfathered In' provision: No subjects enrolled and/or no new data collected after April 14, 2003? Consider it 'grandfathered in.'

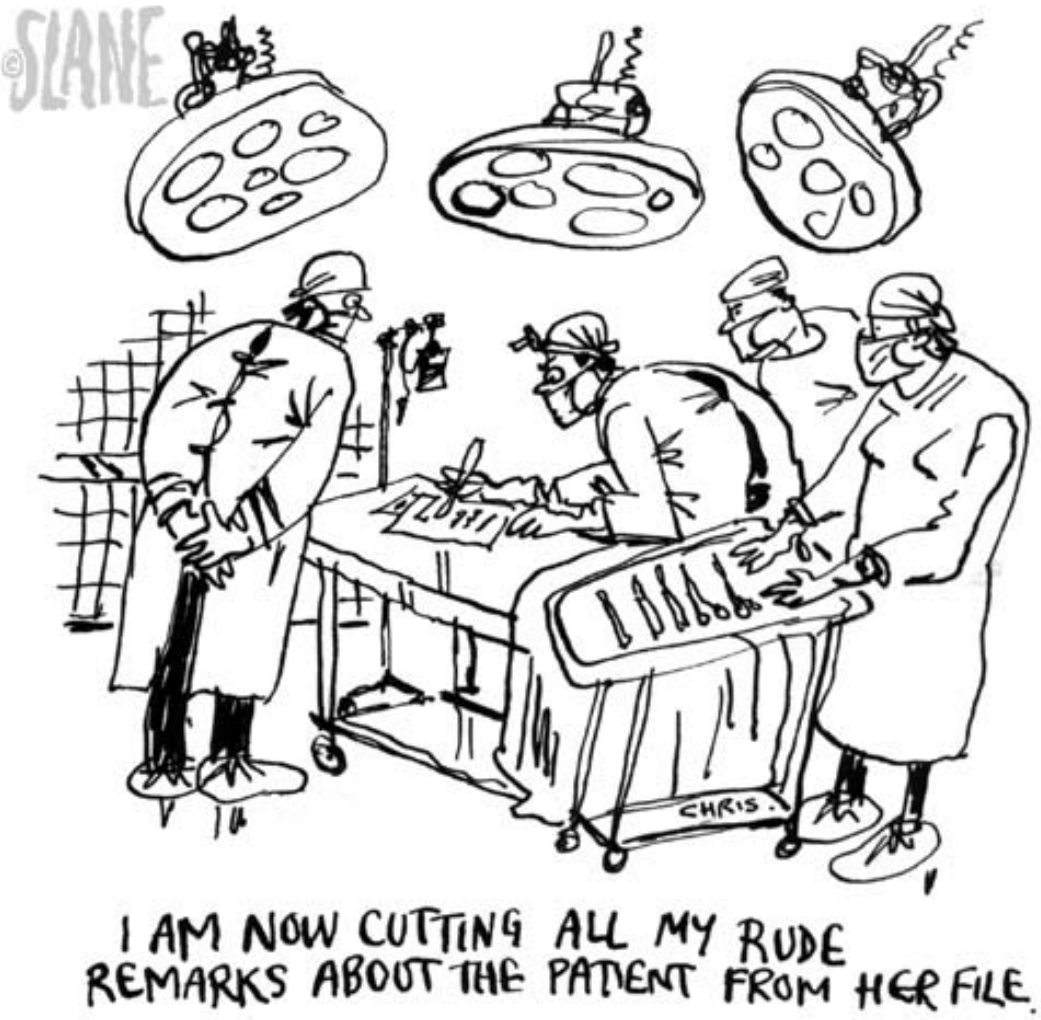
- Revoking an Authorization: Can be done, but does not apply to data already collected.

Points to Remember

- Only completely anonymous data that does not contain PHI whatsoever (not even a code) does not require HIPAA paperwork
- HIPAA requires researchers 'be as specific as possible' on all forms (i.e. specify tests to be done & don't just refer back to the consent form)
- Only use 'the minimal necessary' to complete the study
- HIPAA does not hold up conducting *OR* recruiting for an IRB approved research study

The HIPAA Security Rule

- Security Standards: General Rules
  - Ensure the confidentiality, integrity and availability of all electronic protected health information
  - Protect against any reasonably anticipated threats or hazards to security or integrity of such information
- Administrative Safeguards
  - Risk analysis, risk management, vulnerability (study specific)
- Physical Safeguards
  - Limit access to electronic information systems and the facility in which they are housed while ensuring that properly authorized access is allowed.
- Technical Safeguards
  - Automatic log-off, encryption, decryption
- Organizational Requirements
  - Contracts, business associate



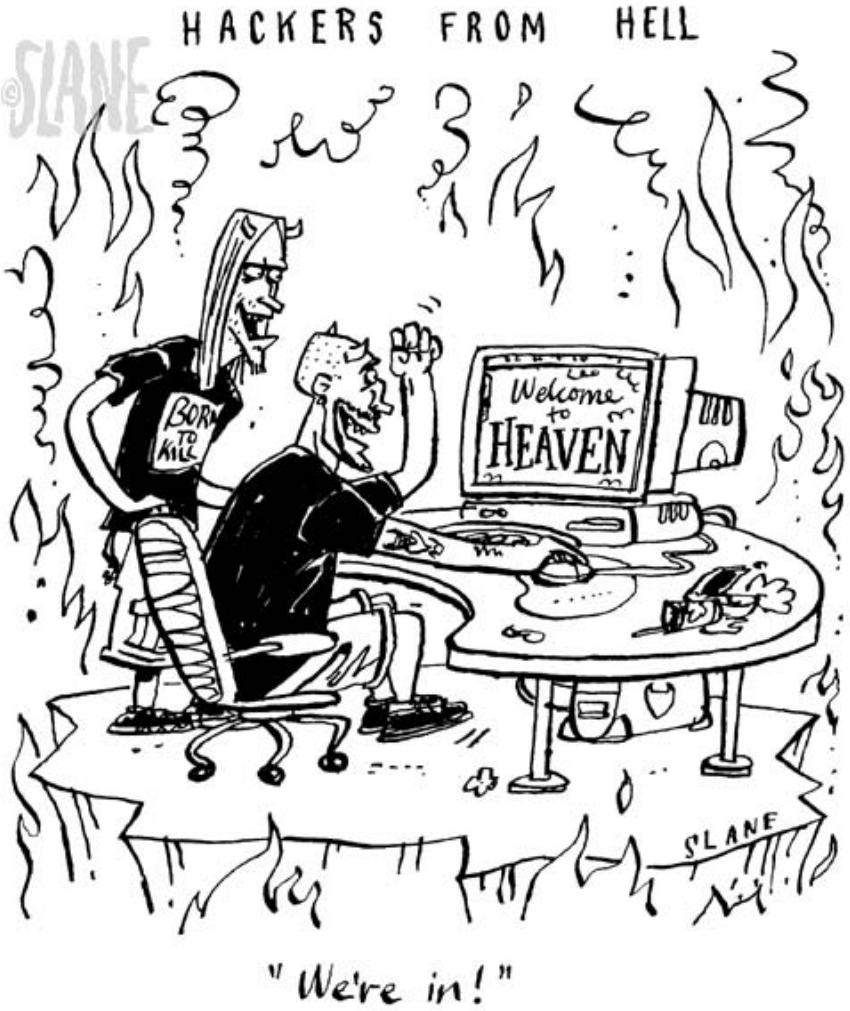
Privacy! By Chris Slane

More Points to Remember

- **ACCESS**: Ensure that only authorized people have access to electronic or paper PHI. It should never be altered or destroyed in an unauthorized manner.

- **Good Security Standards follow the "90/10" Rule:** 10% of security safeguards are technical. 90% of security safeguards rely on the computer user (YOU!) to adhere to good computing practices. Example: The lock on the door is the 10%. Remembering to lock, check to see if it is closed, ensuring others do not prop the door open, keeping controls of keys is the 90%.

- **PASSWORDS:**
  - Choose passwords that are not easy to guess
  - Are eight characters long (use letters & numbers)
  - Change the password every 3-6 months
  - Check every e-mail for viruses and filter for spam



Privacy! By Chris Slane

The Security Rule *(continued)*

- E-MAIL
  - Never use e-mail with a patient in an urgent situation
  - Patient/subject must complete a separate form authorizing e-mail transmission (which can also be revoked)
  - Never hit 'forward' or 'reply all' and double check the attachments being sent
  - Never use any PHI in the subject line (only use the word 'Confidential')
  - Try to avoid using names, dates, social security numbers and other unique identifiers in case the e-mail is misdirected

Resources:

- WMC IRB HIPAA in research webpage/forms:
  http://med.cornell.edu/research/rea_com/hip_rea.html
- General WMC HIPAA guidelines:
  http://intranet.med.cornell.edu/hipaa/
- Department of Health and Human Services National Institutes of Health (HIPAA Privacy Rule):
  http://privacyruleandresearch.nih.gov/
- United States Department of Health and Human Services; Office for Civil Rights HIPAA (HIPAA Security Rule)
  http://www.os.dhhs.gov/ocr/hipaa/

- Knock, knock.
  Who's there?
  HIPAA.
  HIPAA who?
  Sorry, I'm not allowed to disclose that information!

Contact Information

HIPAA Research Privacy Coordinator

Fax: (212)821-0660

E-mail: HIPAAresearch@med.cornell.edu

Interoffice: BOX 5

External Address: 425 East 61st Street

Suite DV301, NY, NY 10021

Power In-Service

Training Center | Your Sucess is our Priority