iEmosies

HIPAA — Health Insurance Portability and Accountability Act (Public Law 104-191)

An Overview

SWAP
October 2003

R.H. Nixon
Salt Lake County District Attorney's Office

What we will discuss....

What is HIPAA and Who must comply

- Privacy Rule and Uses and Disclosures
- Accounting
  s
  Safeguards
- Complaints
- Documentation
- Training

6 Privacy Official

- Deadlines

Enforcemen
t

1111111111111111111111Z,:":

What is Hippa?

A significant and detailed restructuring of health insurance portability and administration.

Five Titles:

1. Health access, portability, and renewal;
2. Administrative Simplification;
3. Tax-related provisions and medical savings accounts;
4. Enforcement of group health plans; and
5. Revenue offsets.

Congress passed the Health Insurance Portability and Accountability Act in 1996.

In addition to creating consumer protection for health care benefits, the "Portability" part of HIPAA< HIPAA will (hopefully):

Standardize financial and administrative health transaction for the public and private sectors;

Increase speed and efficiency;

Cut the cost of delivering health care services; and,

Set minimum standards of protection for the storage, use, and transfer of protected health information.

. immeer=a;:.

NEU

HIPAA-Administrative Simplification

Electronic Transactions and Code Sets

Unique Identifiers

Privacy (45 CFR Parts 160 and 164)

Security

There are four main areas that comprise the administrative simplification portion of HIPAA.

The first is electronic transactions and code sets. HIPAA adopts and requires the use of unifoun national standards and requirements for conducting health care transactions.

The second area is the unique identifier. HIPAA requires establishing and assigning a standard identifier that providers, health plans, and employers will use for every electronic health care transaction.

The third is privacy. Under HIPAA, covered entities must implement standards to protect and guard against the misuse of individually identifiable health infoimation.

The final area is security. HIPAA addresses how electronic health information is stored, transmitted and accessed.

The HIPAA privacy regulations apply to only covered entities. Covered entities include health care plans, health care clearinghouses and health care providers.

A health plan is an individual or group plan that provides, or pays for the cost of medical care.

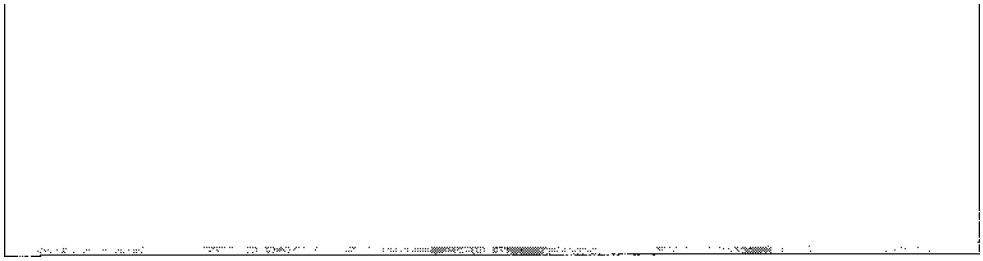
A health care clearinghouse is a public or private entity that processes or facilitates the processing of health information.

A health care provider is a provider of medical or health services who transmits any health information in electronic form in connection with a covered transaction.

See 45 CFR 160.102 and 45 CFR 160.103.

Transactions

* A Transaction is the electronic transmission of information between two parties, to carry out financial or administrative activities related to health care. (45 CFR 160.103)



The following types of information transmissions are included:

1. Health care claims or encounter information:
2. Health care payment and remittance advice;
3. Coordination of benefits;
4. Health care claims status;
5. Enrollment and disenrollment in a health plan;
6. Eligibility for a health plan;
7. Health plan premium payments;
8. Referral certification and authorization;
9. First report of injury;
10. Health claims attachments; and,
11. Other transactions the Secretary of Health and Human Services may prescribe by regulation.

Pm!

What do we mean by "Electronic"?

- Transmissions over the Internet;
- Extra net;
- Leased lines;
- Dial up lines for "direct data entry" (DDE);
- Private networks;
- Point of service; and,
- Transmissions using magnetic tape, disc, or CD media.

See 45 CFR 160.103, as changed in the 20 Feb. 2003 Federal Register.

NOT faxes using a dedicated fax machine (as opposed to faxing from a computer) and

NOT voice transmissions over the telephone.

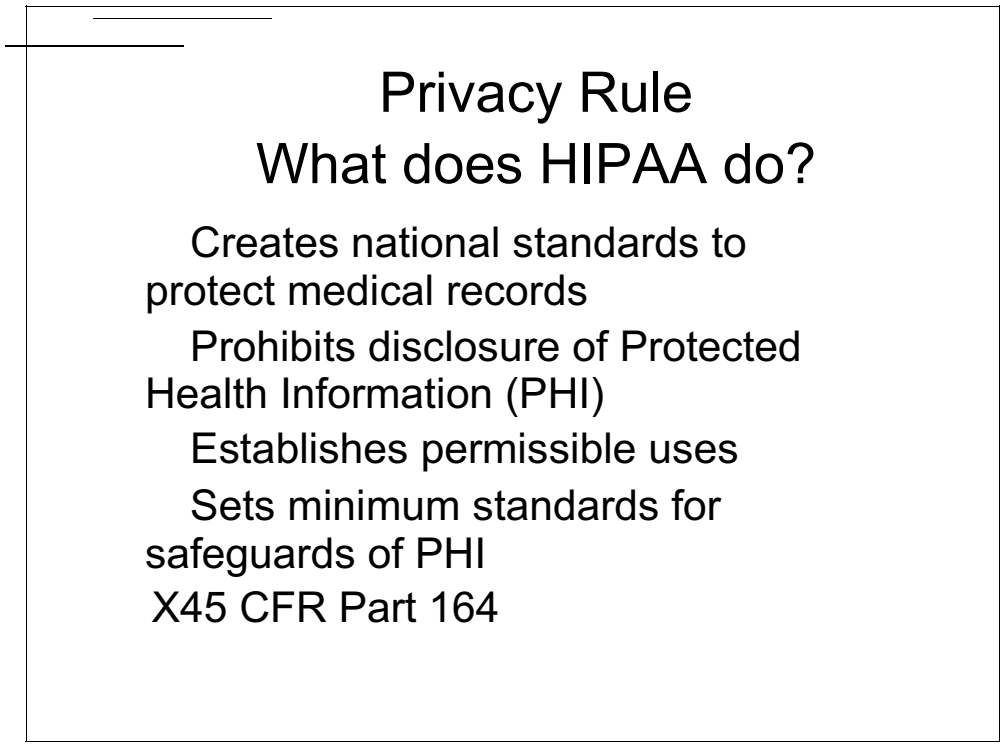
Fax and voice transmissions still have to comply with privacy and security standards if you are otherwise a "covered entity".

Privacy Rule
45 CFR Parts 160 &164

#4, General Administrative Requirements

- General Provisions-definitions-45 CFR 160.103
- Preemption of State Law-45 CFR 160.201
- Compliance and Enforcement 45 CFR 160.300
- Security and Privacy-45 CFR Part 164

Standards for Privacy of Individually Identifiable Health Information
(45 CFR Parts 160 and 164)



HIPAA privacy regulations prohibit disclosure of protected health information (also referred to as individually identifiable health information) except in accordance with the regulations.

The regulations define and limit the circumstances under which covered entities may use or disclose protected health information to others. Permissible uses and disclosures under the rules generally include four categories:

1. Use and disclosure for treatment, payment, and health care operations.
2. Use and disclosure with individual authorization.
3. Use and disclosure without authorization for specified purposes.
4. To the individual subject of the records.

45 CFR 164.502

Privacy Rule
Standards and Protections

- 1, The rule includes standards to protect the use, transfer, and disclosure of health information.

  The rule protects patient information in all forms -- electronic, paper and oral information.

Privacy Rule Preemption

A standard, requirement, or implementation specification of HIPAA that is contrary to a provision of State law preempts the provision of State law unless the State law is more stringent. 45 CFR 160.203

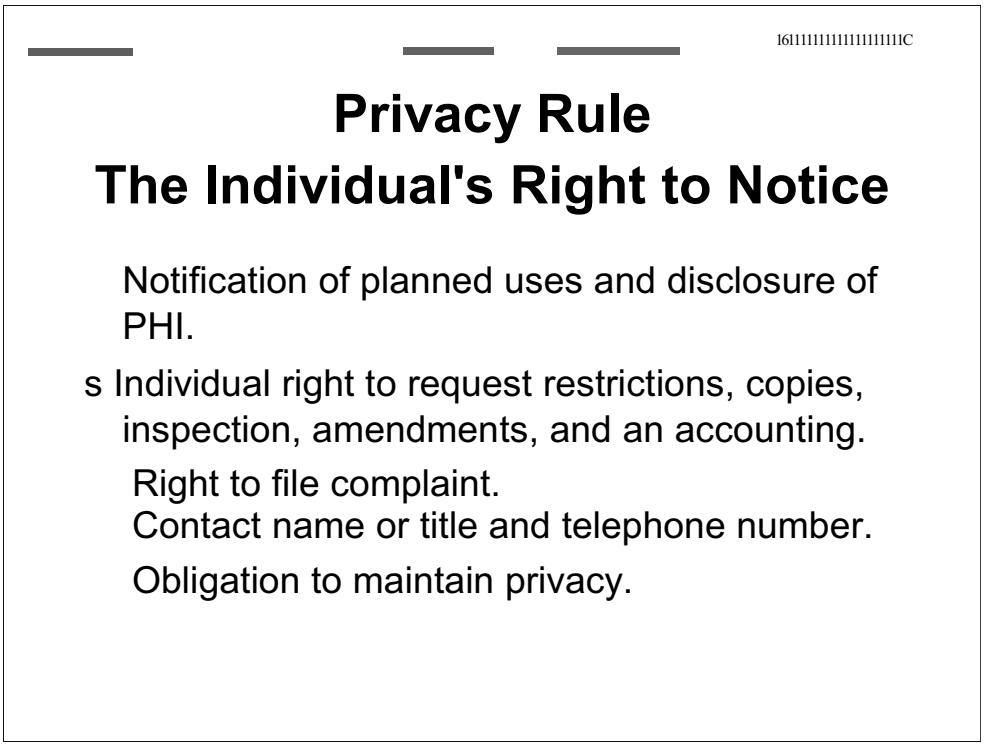
- GRAMA Amendment - 63-2-107 UCA (2003). Federal Privacy Rule Controls.

45 CFR 160.203 contains a number of other exceptions which should be carefully reviewed whenever a question of preemption arises.

Privacy Rule
Covered Entity Requirements

In order to comply, covered entities will have to:

- Provide patients with a Notice of Privacy Practice
- Provide patients with the ability to access medical information
- Secure patient information



45 CFR 164.520 sets out the requirements for the Notice of Privacy Practices for Protected Health Information. Note that "an inmate does not have a right to notice and the notice requirements do NOT apply to a correctional institution that is a covered entity." 45 CFR 164.520 (a)(3).

Notice must disclose:

Uses and disclosures: types of uses and disclosures that covered entity makes for treatment, payment, and health care operations; Must include statement that other disclosures will only be made with written authorization from subject of the record.

Individual rights: right to request restrictions on use; right to receive copies; right to inspect and copy; right to amend; right to receive an accounting of disclosures of PHI; and right to receive a paper copy of the notice at any time.

Complaints: notice must include individuals right to complain and a statement that covered entity will not retaliate against individual for making a complaint.

Contact: name, or title, and telephone number of a person or office to contact for further information.

Covered Entity's Duties: obligation to maintain privacy of PHI; obligation to be by the teHns of the notice; reservation of right to amend privacy notice and how it will provide notice to individuals.

Ls:_

Privacy Rule
Documentation by Covered Entity

A covered entity with a direct treatment relationship with an individual must:

- Provide the notice to the individual at the time of providing service, unless an emergency and then as soon as possible.
- Make a good faith effort to obtain a written acknowledgment of receipt of notice.
-

45 CFR 164.52~~0(c)(2)~~.

Waiver of Rights

A covered entity may not require individuals to waive their rights to file a complaint with the Secretary of Health and Human Services as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits. 45 CFR 164.530(h).

Definitions
(Where to find them)

General	-- 45 CFR 160.103
Compliance and Enforcement	45 CFR 160.302
Privacy	45 CFR 164.501

PHI:Protected Health Information

Individually identifiable health information is information that is a subset of health information, including demographic information

collected from an individual, and

4, (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

s (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

- (i) That identifies the individual; or
- (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

See 45 CFR 160.103- definition of "individually identifiable health infolination".

See also 45 CFR 164.501-Protected health information means individually identifiable health information.

PHI Identifiers
45 CFR 164.514

s Information may be "de-identified" if the following identifiers of the individual or of relatives, employers, or household members of the individual are removed.

- Names
- Geographic subdivisions
- **Dates**
- Telephone numbers

Names

All Geographic Subdivisions smaller than a state, including street address, city, county, precinct, zip code and equivalent geocodes, except for the initial three digits of a zip code if, according to current Census data:

(1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and

(2) the initial three digits of a zip code for all geographic units containing 20,000 or fewer people is changed to 000.

(If less than 20,000 population—no zip code may be included.)

All elements of dates (except year) for dates directly related to an individual including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

Telephone numbers

PHI Identifiers cont'
45 CFR 164.514

- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers

Fax numbers
Electronic mail addresses Social

Security numbers Medical record

numbers Health plan beneficiary

numbers Account numbers

Certificate/license numbers

PHI: Identifiers cont'
45 CFR 164.514

- Vehicle identifiers/serial numbers
- Device identifiers
- Web Universal Resource locators (URL)
- Internet protocol (IP) address number
- Biometric identifiers

Vehicle identifiers and serial numbers, including license plate numbers

Device identifiers and serial numbers

Web Universal Resource Locator (URL)

Internet Protocol (IP) address

Biometric identifiers, including finger or voice prints

Full face photographic images and any comparable images

Any other unique identifying number, characteristic or code, unless the code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual.

Use and Disclosure
45 CFR 164.502

- A covered entity may not use or disclose protected health information except as permitted by HIPAA.
- Permitted uses and disclosures:
  - To the individual;
  - For treatment, payment, or health care operations;
  - Incident to a permitted use;
  - Pursuant to an Authorization or Agreement;
  - As otherwise allowed by HIPAA.

Use and Disclosure
Minimum necessary

When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Minimum necessary does not apply to:

- **Disclosures to or requests by a health care provider for treatment;**
- **Use or disclosure to the individual subject of the PHI;**
- **Use or disclosure pursuant to an authorization;**
- **Disclosures made to the Secretary of Health and Human Services;**
- **Uses and disclosures required by law; and,**
- **Uses and disclosures required for compliance with**

HIPAA. 45 CFR 164.502(b)

See also 45 CFR 164.514(d) for additional provisions relating to the "minimum necessary" standards.

13

Use and Disclosure
45 CFR 164.502(a)(2)

tu Required disclosures:

- An individual has a right of access to inspect and obtain a copy of PHI about the individual;
- When requested by the Secretary of Health and Human Services to investigate and determine the covered entity's compliance.

Use and Disclosure
Business Associate

10 A covered entity may disclose protected health information (PHI) to a business associate and may allow a business associate to create or receive PHI on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

See: 45 CFR 164.502(e)

Note that this does not apply with respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual.

Use and Disclosure

Who is a business associate?

- A person or company that performs functions on behalf of a covered entity involving the use or disclosure of individually identifiable health information.
- A written contract between the covered entity and the business associate is necessary

A business associate is a person or company that performs functions on behalf of a covered entity and the function involves the creation or receipt of protected health infoimation. See: 45 CFR 160.103.

Examples: medical labs processing tests; counselors, doctors and hospitals providing services.

A written contract between the covered entity and the business associate is necessary in order for protected health information to be exchanged. The regulations specifies the minimum contents of the business associate agreement. See: 45 CFR 164.502(e)(2) and 45 CFR 164.504(e)(1).

Broad scope of activities supporting the provision of care and referral to other providers:

Treatment includes: direct care and management and coordination of care with other physicians and health care staff including nurses, therapists, technicians, etc.

Payment includes: activities associated with obtaining or providing reimbursement for the provision of health care services; eligibility verification, adjudication, or subrogation of health care claims; billing, claims management, and collection activities; utilization review activities; disclosure of protected health information to consumer reporting agencies

Health Care Operations include:

Quality assessment and improvement activities; Reviewing and evaluating provider or health plan perfoiniance; Underwriting, premium rating, reinsurance; Medical review, legal services, auditing functions, and compliance programs; Business planning and development; Business management activities including customer service, grievance resolution, due diligence, marketing and fundraising.

See: 45 CFR 164.506-Uses and disclosures to carry out treatment, payment, or health care operations.

See: 45 CFR 164.501-definitions.

:A111E111111

11111111=117-::::::

Use and Disclosure Individual Rights

- Right to privacy protection
- Right to access and copy PHI about them

tv Right to request an amendment to PHI about them

s Right to an accounting of disclosures

Use and Disclosure Privacy

An individual may request restriction of the use or disclosure of PHI needed to carry out treatment, payment, or health care operations.

A covered entity is not required to agree to a requested restriction but if it does it must comply with such restriction unless in an emergency situation.

45 CFR 164.522.

Use and Disclosure Individual Access

An individual has a right to inspect and obtain a copy of their PHI with some exceptions:

- psychotherapy notes,
- information compiled for use in a civil, criminal or administrative action or proceeding, or
- Prohibited by law.
- A correctional institution may deny request if disclosure would jeopardize the health, safety,security, custody or rehabilitation of the individual or others.

45 CFR 164.524 details exceptions to access, unreviewable grounds for denial, reviewable grounds for denial, and the review of denials of access.

Use and Disclosure Access Time Frames

A covered entity:

Must allow an individual to request access to their PHI.

s May require these requests to be in writing.

Must act within 30 days after receipt of the request.

s May get a one-time only 30-day extension if the information is not on site.

May get further extension if written statement of reasons for delay and sets forth date for compliance.

E-WFA1111111111111111111,W-f

Use and Disclosure Access Granted

Covered entity:

- Must inform the individual of acceptance of the request
- PHI only has to be granted once per request even if maintained at more than one location
- Provide it in the format requested by the individual, if it is readily producible in such form
- Can provide it as a summary if the individual agrees in advance to such a summary
- May charge a reasonable fee for copies

45 CFR 164.524

Note: If the individual requests a copy of the PHI, or agrees to a summary of such infoiniation, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Copying, including the cost of supplies for and labor of copying; and,

(ii) Postage, when the individual has requested that the copy be mailed.

Use and Disclosure
Access Denied

If an individual's access is denied:

- The covered entity must provide a written basis of the denial within 30 days
- The individual has the right to have the denial reviewed by another licensed health care official (designated by the covered entity) who did not participate in the original decision

LI1111111.12::

1111111111111MINNIL

Use and Disclosure

Authorization Required
45 CFR 164.508

Except as otherwise permitted or required by HIPAA, a covered entity may not use or disclose PHI without a valid authorization.

An authorization is required for any use or disclosure of psychotherapy notes unless:

- Use by organization for treatment,
- Use for internal training, or
-

Psychotherapy notes are notes recorded (in any medium) by a mental health professional documenting or analyzing the contents of conversation during a counseling session and that are separated from the rest of the individual's medical record.

Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date

See definitions at 45 CFR 164.501.

MONSIESININSI 11111EMEMENORI IMENCEZIEN9

Use and Disclosure

Opportunity to Agree or Object

45 CFR 164.510

s A covered entity may use or disclose PHI provided that the individual is informed in advance and has the opportunity to agree or object:

- Facility directory of individuals present
  - Name, location, and general condition
  - Religious affiliation only to clergy
-

Somewhat loose standard. Obtain verbal agreement, provide opportunity it object, or reasonably infer from the circumstances, based on the exercise of professional judgment, that the individual does not object.

Use and Disclosure Without Authorization 45 CFR 164.512

- Required by law.
- Air Public Health Authorities authorized to collect or receive information for disease control or prevention; child abuse or neglect; FDA.
- 40, Government authorities regarding abuse neglect or domestic violence

Look at state law. May be obligated to infottii individual of the report unless such would place the individual at risk of serious harm or information would go to a personal representative who may be responsible for the harm

Use and Disclosure Without Authorization cont'

so Health oversight activities—audits, civil, administrative, or criminal investigations

- Audit or inspection of provider of mental health or substance abuse services by the local mental health or substance abuse authority to verify services rendered
- Audit or inspection by Medicare or Medicaid

See 45 CFR 164.512(d)

Use and Disclosure

Without Authorization cont'

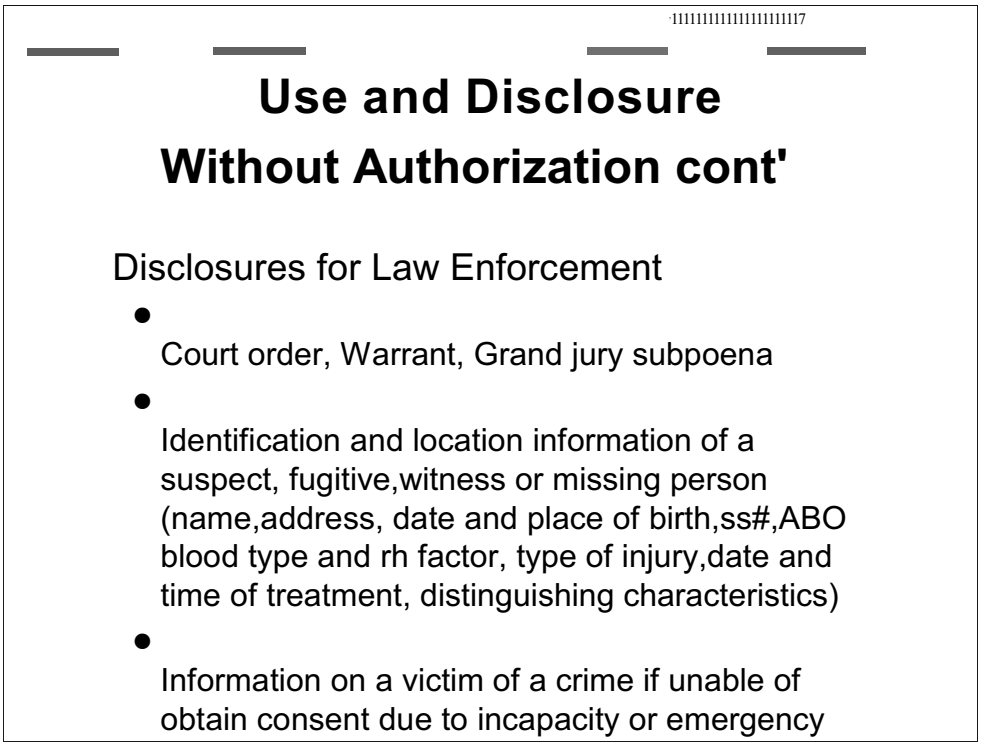
Judicial and administrative proceedings

- In response to an order of a court or administrative tribunal only to the extent of the order
- In response to a subpoena, discovery request, or other lawful process if:
  - Satisfactory assurance that individual has notice
  - Satisfactory assurance of a qualified protective order

45 CFR 164.512(e)

Satisfactory assurance: a written statement and accompanying documentation demonstrating that good faith efforts were made to provide written notice to individual, such notice contained sufficient information to permit individual to raise an objection; and the time to raise objections has passed with no objections or resolution of them by the court.

Qualified Protective Order: Order from a court or administrative tribunal limiting use of the PHI to the pending litigation or proceeding and requiring return or destruction of the PHI at the end of the litigation or proceeding



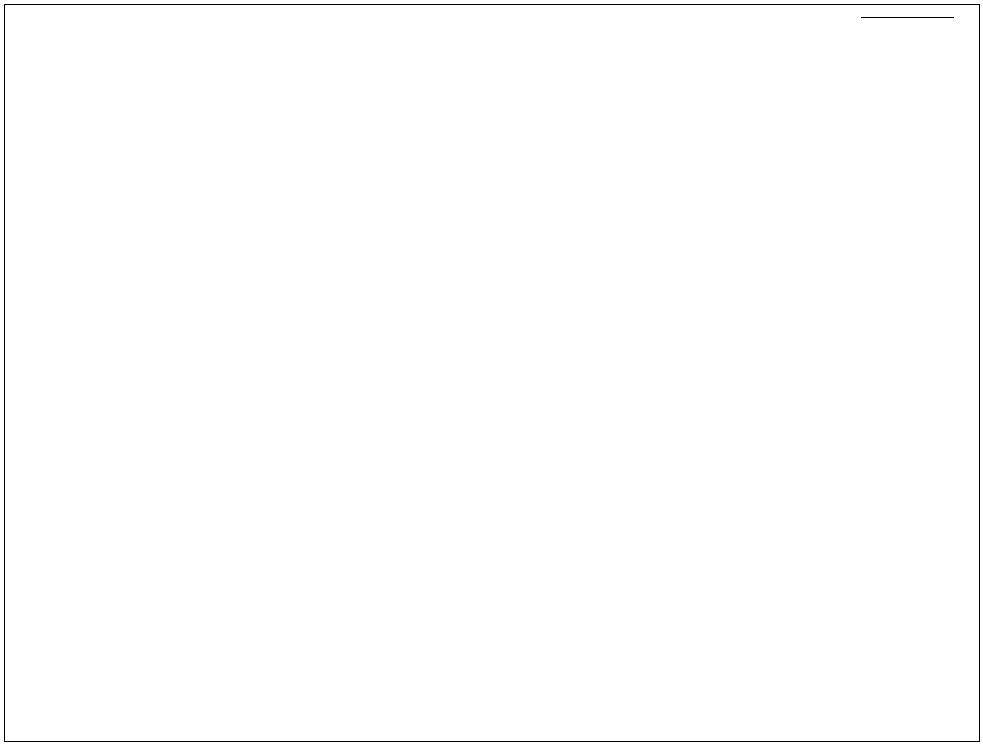
Information on victim of a crime—law enforcement official must represent that the information is needed to deteunine whether a crime has been committed, that it will not be used against the individual, and that law enforcement activities would be materially and adversely affected by waiting until the individual could consent. The covered entity, in the exercise of professional judgment, must believe the disclosure to be in the best interests of the individual. 45 CFR 164.512(f).

See also Sept. 2003 issue of "The Prosecutor". UPC also has a video presentation on disclosure to law enforcement.

Amending PHI

- An individual has a right to request to have **PHI** amended.
  - Covered entity may deny if the records were not created by that entity or the records are accurate and complete
  - Individual may insist on statement of disagreement being part of **PHI**

45 CFR 164.526 contains guidance on Amendment of Protected Health Information.



MEM

Accounting for Disclosure

'Individual has the right to receive an accounting of disclosures

'Exceptions include the following:

- To carry out TPO
- Those authorized by the individual
- To the individual - PHI about them (164.502)
- For the facility directory
- For national security or intelligence purposes
- To correctional institutions or law enforcement officials
- That occurred prior to HIPAA compliance date

Exceptions:

To carry out treatment, payment and health care operations

Disclosures authorized by the individual

To the individual - PHI about them (164.502)

For the facility directory

For national security or intelligence purposes

No obligation to go back more than 6 years.

45 CFR 164.528

Contents of Accounting

It must include:

- Disclosures of PHI that occurred during the time frame requested (not to exceed six years)
- Date of the disclosure
- Name and address of the entity or person who received the PHI
- Brief description of the information disclosed
- Statement of the purpose of the disclosure OR a copy of the written request for a disclosure

45 CFR 164.528

Additional Accounting Obligations

*The covered entity must act on the request within 60 days, and

- If delayed, provide written explanation including when the information will be sent (one-time only)

*The first accounting in any 12 month period must be without charge, and

A reasonable, cost-based fee can be charged for each additional request so long as individual is aware of fee and has opportunity to withdraw or modify request.

45 CFR 164.528

Safeguards

A covered entity must have in place administrative, technical, and physical safeguards to reasonably protect health information

- Prohibit accidental or intentional use or disclosure
- Limit incidental uses or disclosures
- 45 CFR 164.530

Complaints

Covered entity must provide a process for complaints

Covered entity must document all complaints received and their disposition

Covered entity must have and apply appropriate sanctions for failure to comply with privacy policies and procedures

Covered entity must mitigate any harmful effects resulting from wrongful use or disclosure by the entity or a business associate

Develop policies and procedures to implement HIPAA.
45 CFR 164.530

Documentation

Covered entities should utilize standard forms appropriate for their functions

lir Forms must be updated promptly to reflect changes to rules or privacy practices

Documentation Retention

Records must be maintained the minimum 6 year period required by HIPAA or such longer period as you may choose.

Must maintain documentation for at least six years from date of creation or date when the document was last in effect, whichever is later (45 CFR 164.530)

Training

A covered entity must provide training to each member of the entities workforce by no later than the compliance date for the entity; thereafter to each new employee; and to each employee whose functions are affected by any material change in HIPAA

A covered entity must document that the training has been provided.

See 45 CFR 164.530

Privacy Official

si A covered entity must designate a privacy official who is responsible for the development and implementation of the HIPAA policies and procedures of the entity. 45 CFR 164.530

Compliance Deadlines

April 14, 2003—Privacy rules.

October 16, 2003—Electronic Healthcare Transactions and Code Sets.

July 30, 2004---Employer Identifier Standard

April 21, 2005---Security Standards

Exceptions for "Small Health Plans".

Electronic Transactions and Code Sets

Original Compliance deadline of October 16, 2002, extended to October 16, 2003, IF an extension was requested by October 15, 2002.

Compliance deadline extended by adoption of the Administrative Simplification Compliance Act (ASCA)— Public Law 107-105.

HIPAA does NOT require that claims be submitted electronically but if they are, HIPAA does mandate that the HIPAA standards be used.

=or

11Mr."-

Medicare Claims

Effective October 16, 2003, Medicare claims must be submitted electronically unless:

- No method is available for doing so; or,
- The entity is a small provider (fewer than 10 FTE's)

Anticipate delayed payments if paper claims are submitted. AMA estimates that many physicians will start using paper claims to avoid being treated as "covered entities."

Enforcement of HIPAA Administrative Simplification

Centers for Medicare and Medicaid Services (CMS):

- Transactions and Code Sets Security
- Identifiers

Office of Civil Rights (OCR):

- Privacy

The Office of Civil Rights (OCR) and the Centers for Medicare and Medicaid (CMS) are part of the Dept. of Health and Human Services. For Compliance and Enforcement generally, see 45 CFR 160.300-312.

It should be noted that HIPAA is jointly enforced by the Department of Labor, the Internal Revenue Service, and the Department of Health and Human Services pursuant to a Memorandum of Understanding dated December 15, 1999. (64 Fed. Reg. 70164). It would appear that the Administrative Simplification portion of HIPAA is enforced by DHHS. At least one court has recognized a private cause of action under HIPAA although not under the administrative simplification portion. See: Stang v. Clifton Gunderson Health Care Plan, 71 F.Supp.2d 926 (W.D. Wis. 1999).

Civil Penalties
42 USC 1320d-5

c Civil monetary penalties:

- Not more than $100 per violation
- Capped at $25,000 per year for all violations of an identical requirement or prohibition.

Criminal Penalties
42 USC 1320d-6

Up to $50,000 and 1 year imprisonment for knowingly obtaining or disclosing identifiable health information.

*, Up to $100,000 and 5 years imprisonment if committed under false pretenses.

Up to $250,000 and 10 years imprisonment if intent to see, transfer, or use for commercial advantage, personal gain, or malicious harm.

Department of Justice will have jurisdiction regarding criminal actions.

Resources

- U.S. Dept. of Health & Human Services, Office of Civil Rights http://www.hhs.gov/ocr/hipaa/
- Centers for Medicare & Medicaid Services http://www.cms.gov/hipaa/
- HIPAA Privacy Joint Information Center http://www.bricker.com/hipaa/
- The Federal Register http://vvww.gpoaccess.gov/fr/index.html

List of Salt Lake County Forms

- Amendment Request
- Acknowledgement of Request to Amend
- Business Associate Agreement
- Disclosure Log
- Authorization Form
- Identity Verification
- Notification to Amend Records
- Notice of Privacy Practice
- Notification of Records Amendment Denial