

Protecting Clients & Their Information

Massachusetts Dietetic Association

**Fall Meeting: November 10, 2003
Westborough MA**

HIPAA: Good Nutrition for the Health Industry

A Presentation by:

Matthew C. Rosenblum

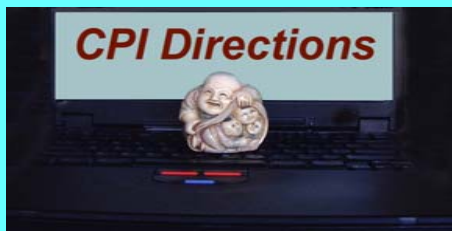
Chief Operations Officer

Privacy, Quality Management & Regulatory Affairs

CPI Directions, Inc.

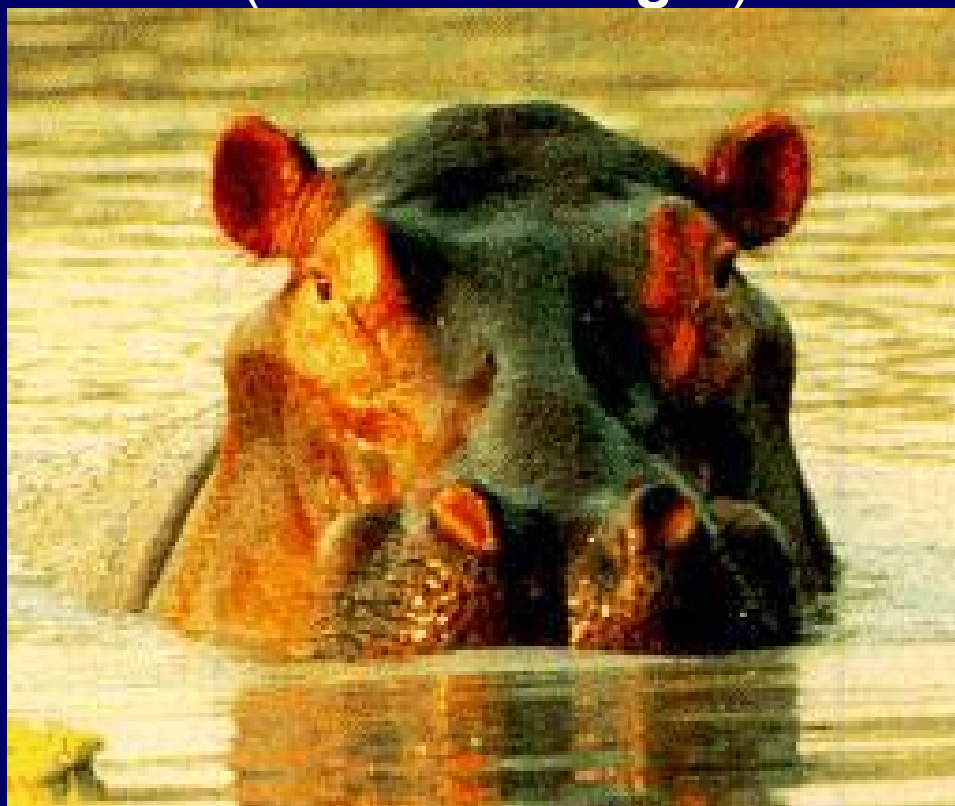
MRosenblum@att.net

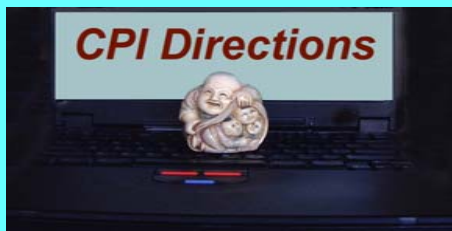
<http://www.CPIdirections.com>



Protecting Clients & Their Information

Health Insurance Portability & Accountability Act of 1996 **(HIPAA is Huge!)**

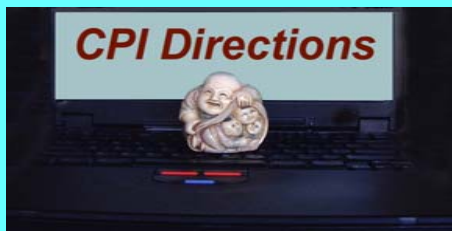




Protecting Clients & Their Information

Some recent **HORROR** stories

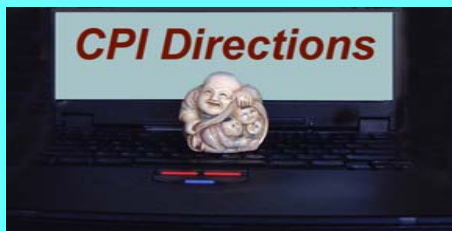
- Large Pharmaceutical Company: Revealed >600 patient e-mail addresses when it sent a message to every individual registered to receive reminders about taking Prozac.
- Major Medical Research University: 1) Mistakenly posted the MH records of 20 children on a public Web site. 2) Mailed a survey to 1200 transplant recipients participating in a long-term research study and mistakenly revealed the names of those who had donated their kidney to the recipients.
- National Retail Drug Chain: Customers pick up prescriptions and sign a log to indicate that they do not want counseling of the pharmacist. Drug chain staff takes the signature (written on a gum-backed sticker) and puts it on a form authorizing the drug store to use the customer's prescription record for promotions.



Protecting Clients & Their Information

Overview of 5 HIPAA Rule-Sets

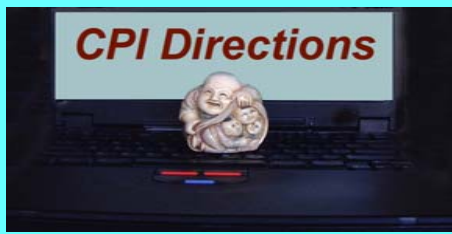
- **Transaction Standards**: standardizes and reduces the current # of electronic formats (claims, eligibility, etc.)
- **Privacy Standards**: provides that our *PHI* will be protected from *bad* uses and disclosures, and provides the patient/client with certain *controls* and *rights*
- **Security Standards**: aim is to provide administrative, technical, and physical-space safeguards
- **Employer/Provider Unique IDs**: unique identifiers for providers & employers to facilitate transfer of information to/from health plans, clearinghouses, payers, etc.
- **Enforcement Standards**: HHS & OCR oversight & enforcement methodologies, penalties for non-compliance



Protecting Clients & Their Information

Some General HIPAA Terms

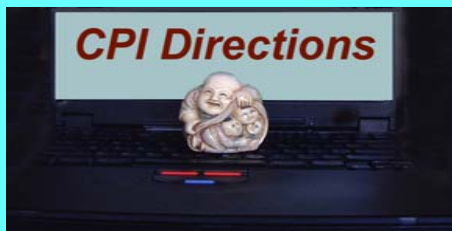
- **Covered Entity (CE)**: Health Plans, Clearinghouses, Healthcare Providers that transact PHI electronically
- **Business Associate (BA)**: Indirectly covered - Attorneys, IT vendors, consultants, transcription services, etc.
- **Protected Health Information (PHI)**: individually identifiable health info that relates to past, present, or future health; written, oral, stored in any media
- **TPO**: routine uses and disclosures for Treatment, Payment, Healthcare Operations
- ***Authorization*** to use & disclose PHI for non-TPO
- ***Minimum Necessary***: Role-, use-based *need to know*



Protecting Clients & Their Information

Business Associate Contracts (BAC): CE to ensure BA's appropriately handle shared PHI

- Signatures, contract start/expiration or review dates
- Terms & conditions, including conditions for disclosure of PHI, data rights of each party, minimum security
- Procedures for reporting breaches and time frame
- Method of recording breaches: incident logs
- Penalties: intentional vs. unintentional breaches
- P&P for the retention and/or destruction of data
- Language requiring subcontractors to be compliant
- TCS certification to be attached (when appropriate)



Protecting Clients & Their Information

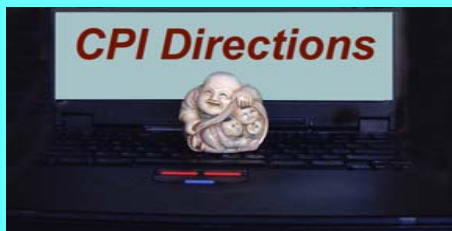
Uses & Disclosures of PHI

Minimum necessary principle

Reasonable efforts to ensure that only *minimum necessary* PHI is used/ disclosed, except:

- **To provider for treatment**
- **To the patient**
- **To HHS pursuant to a privacy investigation**
- **As required by Federal or other law**

Categorize workforce by *need to know* and establish P&P's to limit inappropriate use & disclosure. CE must limit its own requests for PHI (from other CE's) to the *minimum* needed.



Protecting Clients & Their Information

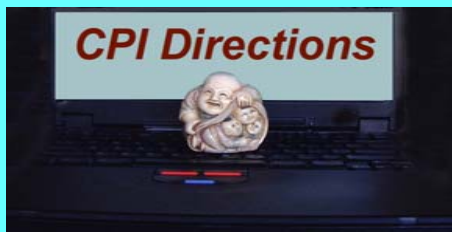
TPO: What is meant by Treatment?

Provision, coordination, or management of health care, & related services by health care provider, including:

- **Coordination or management of healthcare by a provider with a 3rd party consultation(s) among providers relating to a patient**
- **Referral of a patient for health care from one health care provider to another**

Direct treatment relationship: E.g., hands-on exam, verbal assessments (in-person or even on the telephone), filling an Rx at the pharmacy.

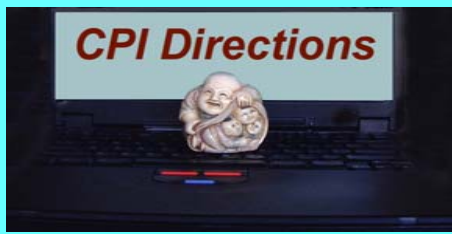
Indirect treatment relationship: E.g., remote consults, diagnoses, laboratory work-ups, and radiological readings.



Protecting Clients & Their Information

TPO: What is meant by Payment?

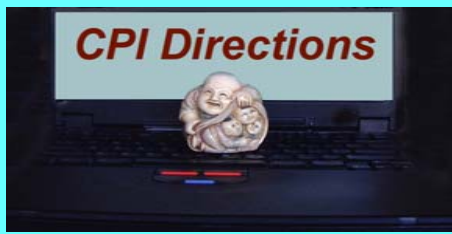
- Review of care for medical necessity, health plan coverage, appropriateness of care, justification of charges
- UR activities, pre-certification and preauthorization of services, concurrent and retrospective review of services
- Determinations of eligibility or coverage, coordination of benefits and adjudication of claims
- Billing, claims management, collection activities
- Disclosures to reporting agencies re collection of payments: Name, address, SSN, DOB, payment hx, acc' #, name and address of provider and/or health plan
- Risk adjustments of amounts due based on enrollee health status and demographic characteristics



Protecting Clients & Their Information

TPO: What are Health Care Operations?

- **Case management/coordination, contacting providers & patients re treatment alternatives, related functions**
- **Workforce evaluation, training, activities re accreditation, certification, licensing, credentialing**
- **Peer review, legal services, auditing functions re fraud, abuse detection, compliance**
- **Outcomes analysis, activities re performance improvement**
- **Formulary development and administration**
- **Grievance resolution**
- **Due diligence in connection with the sale or transfer of assets**
- **HIPAA implementation & compliance**

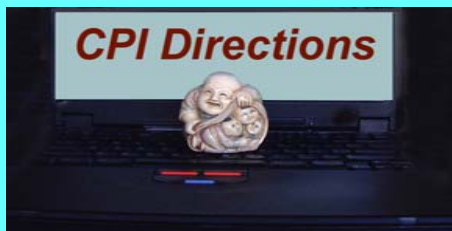


Protecting Clients & Their Information

Designated Record Set

A group of records maintained by or for a CE that is:

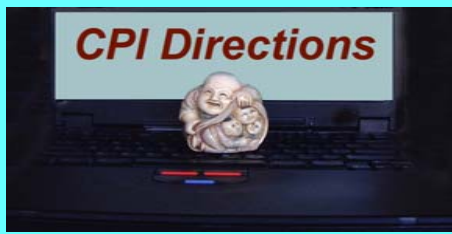
- The medical records and billing records about individuals maintained by or for a covered health care provider, or
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan, or
- Used, in whole or in part, by or for the CE to make decisions about individuals.



Protecting Clients & Their Information

HIPAA Requirements

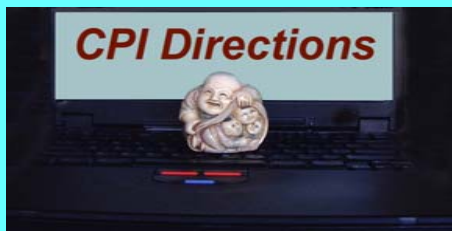
- **Policies and procedures**: Create & implement a privacy P&P **set**. Having a “policy” is **not adequate**; P&P ***set*** must take into account the CE’s size and type of operations
- **Privacy Official**: Requires (documented) appointment of an individual to be accountable for the development implementation of privacy policies & procedures
- **Training**: All workforce members. Initial, and on-going as privacy P&P’s change. Workforce includes Board, employees, volunteers, trainees, etc.



Protecting Clients & Their Information

Patient Rights! & Needed P&P's

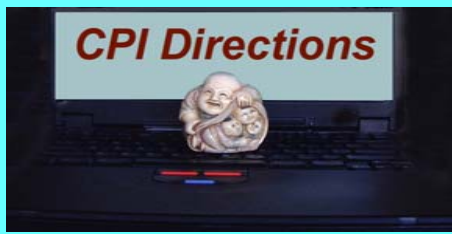
- **Notice of privacy practices (NPP)**: Right to be notified of the CE's uses & disclosures of PHI, individual's rights, and CE's legal duties with respect to PHI.
- **Signed-Acknowledgements** (for receipt of ***NPP***): Direct treatment providers to make "***good faith effort***" to obtain signed-acknowledgement by initial visit.



Protecting Clients & Their Information

Contents of the Notice of Privacy Practice (NPP)

- 1. Use & Disclosure of PHI**
- 2. Contacting the patient**
- 3. Patients Rights**



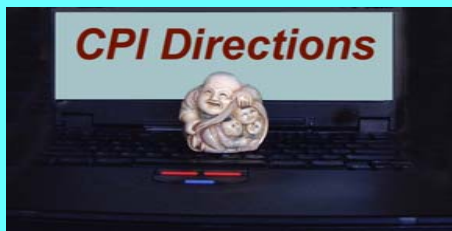
Protecting Clients & Their Information

More Patient Rights! & Needed P&P's

Access to PHI: Access, inspect, and obtain a copy of the individual's PHI in the ***designated record set***. There are exceptions to this requirement, time frames for compliance, and specific required processes that must be implemented.

Right to amend: Amend the PHI. Requirements for addressing requests include timely action, accepting or denying the amendment, informing the individual, etc.

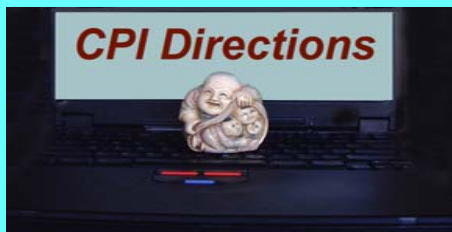
Right to accounting of disclosures of PHI: Right to an accounting of PHI disclosures within the last 6 years, or since compliance was first required for the CE. Exceptions for disclosures for **TPO**, disclosures pursuant to an authorization



Protecting Clients & Their Information

Accountings of PHI Disclosures

- Research pursuant to IRB waivers
- Suspected abuse reporting
- Underage pregnancy reporting
- Communicable disease reporting
- Disclosures to law enforcement
- State neonatal reporting
- Birth defects registry
- Batch P.H. disclosures to State
- Cancer registry
- Trauma registry
- Death registry
- Poison control
- County medical examiner
- Disclosures to funeral homes
- Reporting to FDA
- Privacy Breaches



Protecting Clients & Their Information

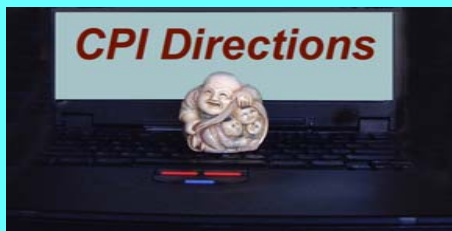
And yet even more Rights and P&P's

Right of an individual to request confidential communications & restrict PHI uses and disclosures:

Need P&P to accept and/or deny requests, respond to requests, and track requests accepted by the CE

Authorizations for uses and disclosures:

Authorization prior to PHI use or disclosure for most non-TPO purposes. Patient has right to revoke authorization. E.g., psychotherapy notes, research without an IRB waiver, press & media events, most marketing activities

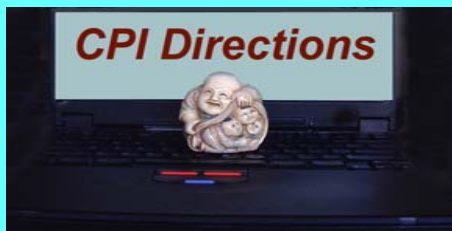


Protecting Clients & Their Information

Privacy: Authorizations

Components of an Authorization Form:

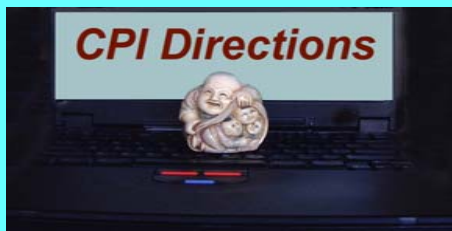
- A description of the information to be used or disclosed
- ID's the persons authorized to make use or disclosure
- ID's the persons who use, or to whom the CE may make the disclosure
- Description of each purpose of the use or disclosure. May be as simple as, "at the request of the individual".
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. For research purposes, may be "end of research study", or "none".
- Signature of the individual and date



Protecting Clients & Their Information

Research, as Defined by HIPAA

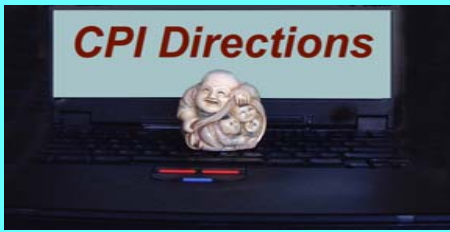
“.....a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.”



Protecting Clients & Their Information

Research WithOUT an Authorization

- Written IRB or Privacy Board approval
- Preparatory to Research
- Research on PHI of Decedents
- De-identified Data Sets
- *Limited Data Set & Data Use Agreement*



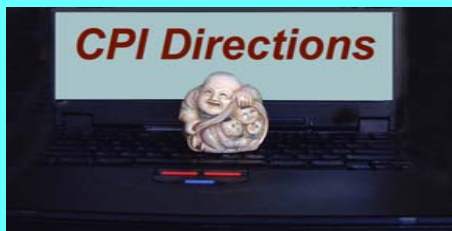
Protecting Clients & Their Information

Identifier

De-ID'd

LDS

• Name	X	X
• Address components	X	Town, State Zip code OK
• All elements of dates	X	Dates OK
• Telephone or fax number	X	X
• E-mail, URL, IP addresses	X	X
• Social Security number	X	X
• Driver's license number	X	X
• Medical record number(s)	X	X
• Health plan numbers	X	X
• Account numbers	X	X
• Certificate, license #'s	X	X
• Vehicle identifiers	X	X
• Medical device identifiers	X	X
• Biometric identifier	X	X
• Photographic images	X	X
• Other unique identifiers	X	Minimum Necessary Rule

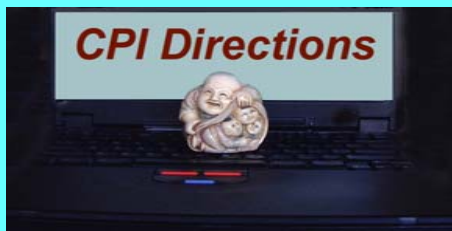


Protecting Clients & Their Information

Uses & Disclosures of PHI for Marketing

“To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service...” Exceptions for:

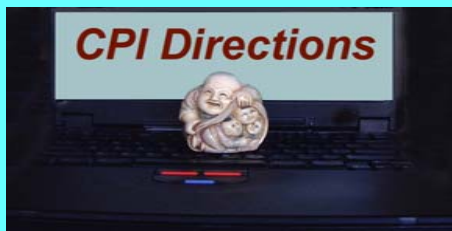
- Descriptions of products or services
- Replacements or enhancements of products or services
- Treatment communications
- Most face-to-face communications
- Providing items of nominal value (e.g., calendars, pens with provider's name)



Protecting Clients & Their Information

Tracking the HIPAA HIPPO

- NPPs & Acknowledgements
- Authorizations
- Patient requests, denials, and complaints
- Workforce Awareness Training
- Disclosure accountings
- Confidential communications
- Agreed-upon restrictions
- Opt-outs from fundraising
- Opt-outs from facility directory
- BACs, DUAs, LDSs
- Amendments of PHI in various sections of the medical record, electronic databases, and already disclosed to other providers & BAs
- Identifiers of PHI in various places in the Designated Record Set (DRS)
- *Breaches* in HIPAA rules
- Etc., etc., etc., etc.



Protecting Clients & Their Information

Penalties for Privacy Breaches

➤ Civil monetary fines:

Up to \$100 per person, per violation

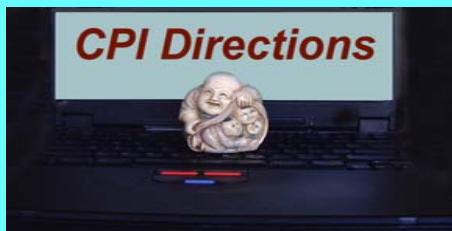
Up to \$25K per person, per standard, per year

➤ Criminal penalties:

Up to \$50K + 1 yr prison: (knowing actions)

Up to \$100K + 5 yrs prison: (false pretense)

Up to \$250K + 10 yrs prison: (sale, malicious harm)



Protecting Clients & Their Information

For additional information, please contact:

Matt Rosenblum

Chief Operations Officer

Privacy, Quality Management & Regulatory Affairs

CPI Directions, Inc.

10 West 15th Street, Suite 1922

New York, NY 10011

(212) 675-6367

MRosenblum@att.net

<http://www.cpidirections.com>