

Protecting Clients & Their Information

WINS - Institute for Cancer Prevention
New York NY - May 21 & 27, 2003

Understanding & Implementing HIPAA In a Research Environment

A Presentation by:

Matthew C. Rosenblum

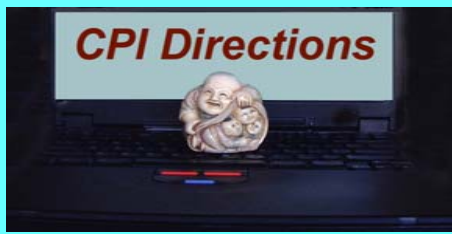
Chief Operations Officer

Privacy, Quality Management & Regulatory Affairs

CPI Directions, Inc.

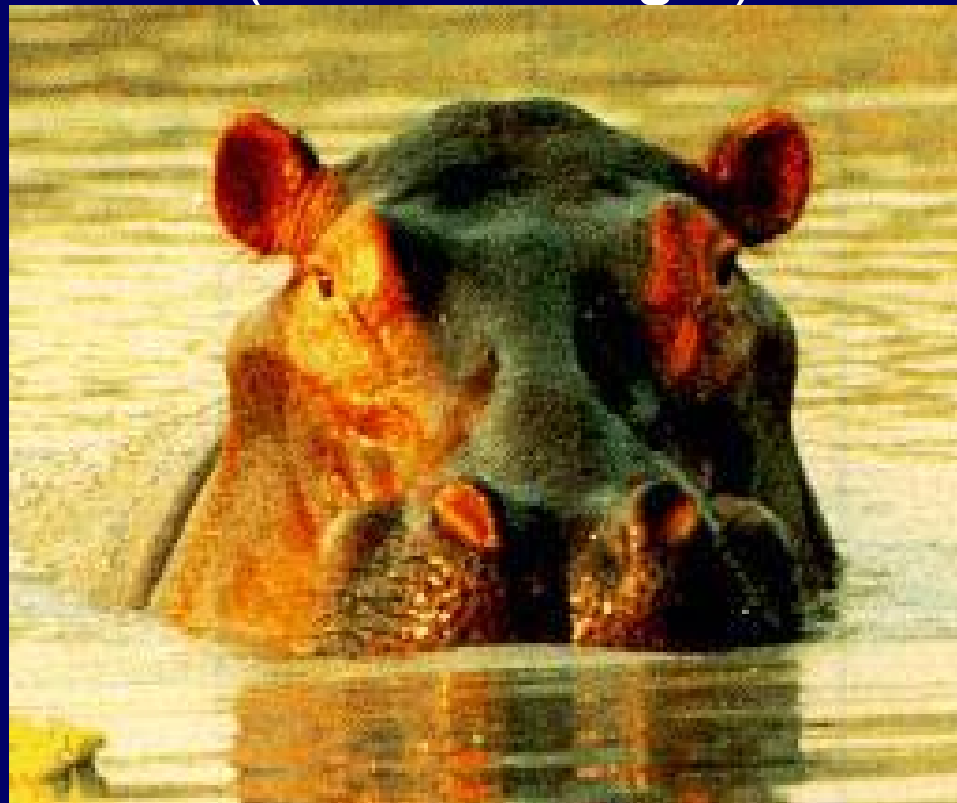
MRosenblum@att.net

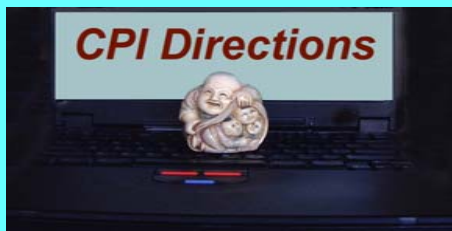
<http://www.CPIdirections.com>



Protecting Clients & Their Information

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



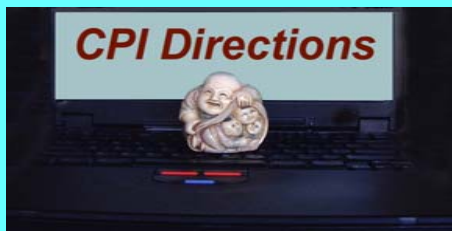


Protecting Clients & Their Information

HIPAA is Huge

Impacts all aspects of treatment, payment and operations:

- ***Cultural Change***: whose info is it? Patient's? Providers? Insurer's?
- ***Y2K*** = single event with no punitive legal actions
- ***HIPAA*** = possibility of on-going erosion of profit margins + civil, criminal penalties (including prison)
- ***Push toward standard electronic transactions***: major restructuring of administration of paper processes & staffing
- ***Corporate restructuring & firewalls***: requires legal, administrative, technical, & physical-space transformations
- Implementation cost: ***\$22B over 5 years*** for hospitals alone (AHA)
- ***Minimum Necessary rule***: prohibits common practices, ranging from *talking in elevators* to providing insurance companies with *whole chart*
- ***Pre-empts State laws*** that provide less privacy

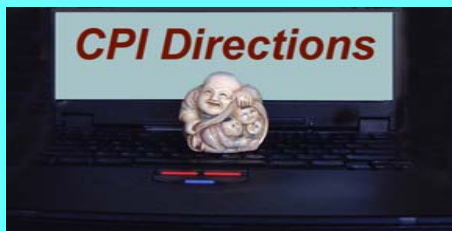


Protecting Clients & Their Information

HIPAA Timeline & Deadlines

- **August 1996:** Congress passes HIPAA
- **August 1998:** Congress fails deadline to publish HIPAA implementation rules; HHS takes over the process
- **1998-9:** Proposed HIPAA rules formulated & published
- **August 2000:** Final *Transaction Rules* published
- **December 2000:** Final *Privacy Rules* published
- **December 2001:** ASCA - Final *TCS Rule* extension to 10-2003, if implementation plan filed by 10-15-02 & testing begun by 4-15-03
- **March 2002:** HHS proposes changes to Final *Privacy Rule*
- **May 2002:** Final Rule *Employer ID Rule*, comply by 7-30-2004
- **May 2002:** HHS proposes changes to Final *Transactions Rule*
- **August 2002:** Final Privacy Rules revisions, comply by 4-14-2003
- **October 15, 2002:** 1-Yr TCS extension requests to be filed by Midnight
- **February 20, 2003:** Final Security Rules published, comply by 5-20-2005

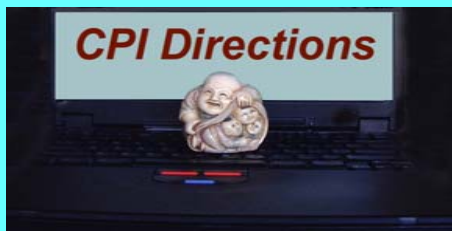
Privacy Compliance by APRIL 14, 2003!



Protecting Clients & Their Information

Some recent **HORROR** stories

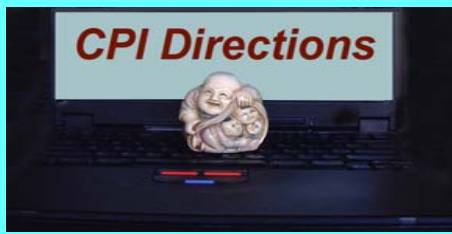
- Large Pharmaceutical Company: Revealed >600 patient e-mail addresses when it sent a message to every individual registered to receive reminders about taking Prozac.
- Major Medical Research University: 1) Mistakenly posted the MH records of 20 children on a public Web site. 2) Mailed a survey to 1200 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

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 non-TPO activities
- ***Minimum Necessary***: Role-, use-based *need to know*



Protecting Clients & Their Information

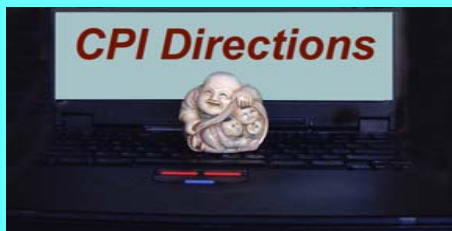
Privacy: Uses & Disclosures of PHI

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**

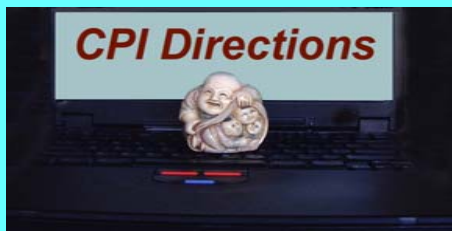
Categorize workforce by need to know and establish P&P's to limit inappropriate use & disclosure. CE must limit its own requests for PHI (from other CE's) to the *minimum* needed.



Protecting Clients & Their Information

Overview of 5 HIPAA Rule-Sets

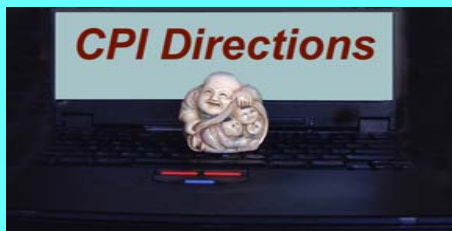
- **Transaction Standards**: standardizes and reduces the current # of electronic formats (claims, eligibility, etc.)
- **Privacy Standards**: provides that our *PHI* will be protected from *bad* uses and disclosures, and provides the patient/client with certain *controls* and *rights*
- **Security Standards**: aim is to protect the integrity, confidentiality, and availability of *PHI*
- **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

Components of Transaction Rules

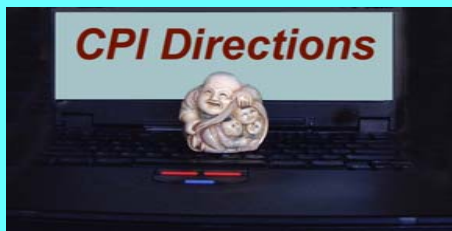
- **Healthcare claims (or equivalent) encounter**
- **Enrollment/Disenrollment in a health plan**
- **Eligibility for a health plan**
- **Healthcare payment & remittance advice**
- **Health plan premium payments**
- **Health claim status**
- **Referral certification & authorization**
- **Coordination of benefits**



Protecting Clients & Their Information

Components of Privacy Rules

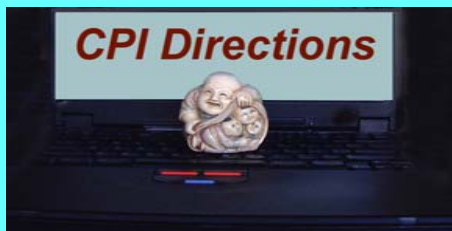
- **Covered entities**
- **Consumer controls & Notice of Privacy Practices**
- **Authorizations & Restrictions**
- **Administrative requirements**
- **Uses and disclosures of PHI**



Protecting Clients & Their Information

Components of Security Rules

- **Security administration**: training, contingency planning assigned responsibility, etc.
- **Physical safeguards**: facility access, work station use & security, etc.
- **Technical security**: access & audit controls, authentication, etc.



Protecting Clients & Their Information

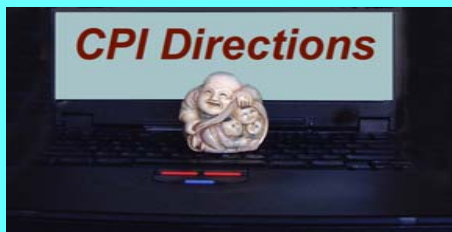
TPO: What is meant by Treatment?

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.

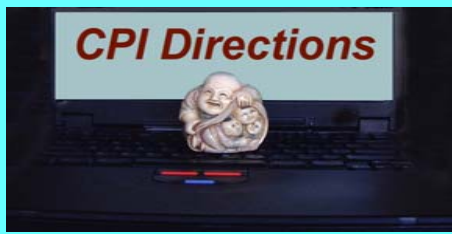
Indirect treatment relationship: E.g., remote consults, diagnoses, laboratory work-ups, and radiological readings.



Protecting Clients & Their Information

TPO: What is meant by Payment?

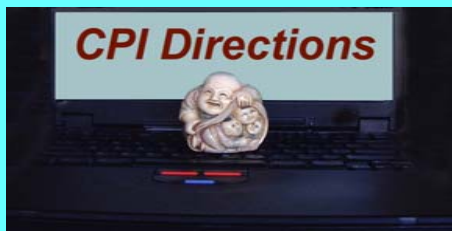
- Review of care for medical necessity, health plan coverage, appropriateness of care, justification of charges
- UR activities, pre-certification and preauthorization of services, concurrent and retrospective review of services
- Determinations of eligibility or coverage, coordination of benefits and 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**



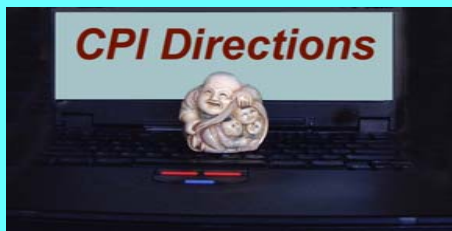
Protecting Clients & Their Information

Two required uses & disclosures of PHI:

- To the individual who is the subject of the records
- To HHS & OCR to investigate compliance with HIPAA

Permitted uses and disclosures of PHI:

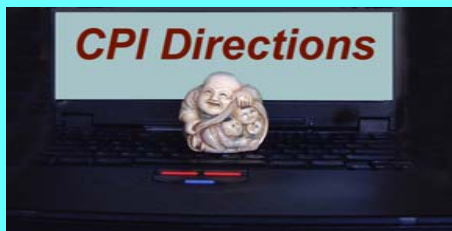
- With patient notice for Treatment, Payment, and health care Operations (**TPO**)
- Without notice in *emergencies* for *TPO*
- For any purpose, with a signed-authorization
- With an opportunity to *opt-out* prior to use or disclosure: limited to *patient directory* listing & fundraising
- When PHI is de-identified
- When the *public good* permits the disclosure
- Legal requests (regulators, courts)



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 by April 2003. Initial, and on-going as privacy P&P’s change. Workforce includes Board, employees, volunteers, trainees, etc.



Protecting Clients & Their Information

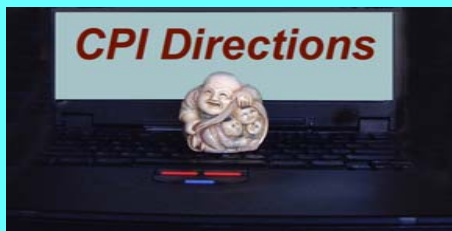
Privacy: Consumer Rights

Notice of privacy practices (NPP):

Individuals have the right to be notified of the types of uses and disclosures of PHI that may be made by a CE. They also have the right to be notified of their individual rights and the 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.

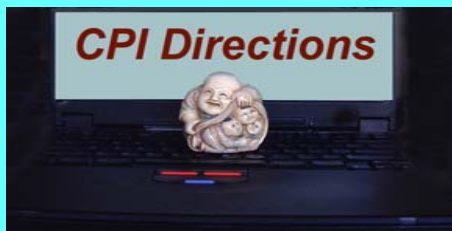


Protecting Clients & Their Information

Privacy: Consumer Rights

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

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



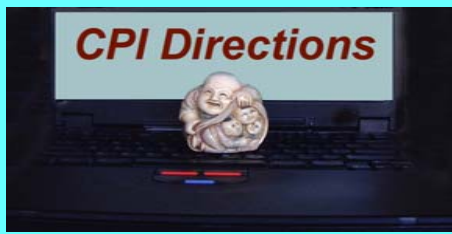
Protecting Clients & Their Information

Privacy: Consumer Controls

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.

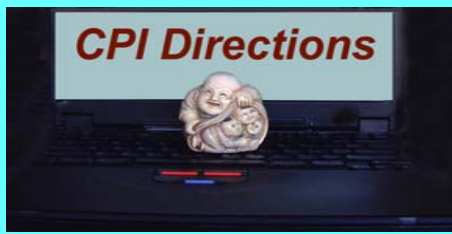
Right to accounting of disclosures of PHI: Right to an accounting of PHI disclosures within the last 6 years, or since compliance was first required for the CE. Exceptions for disclosures for **TPO**, disclosures pursuant to an authorization



Protecting Clients & Their Information

HIPAA Administrative Costs (\$M)

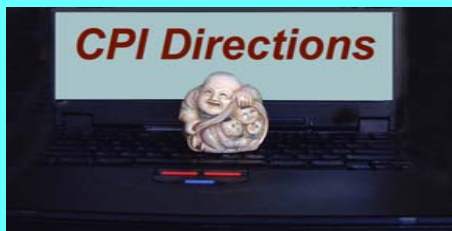
HIPAA Provision	Cost Yr 1 (2003)	Ave. Cost (Yrs 2-12)	Ave. Cost (2003-12)
Develop P & P	597.7	0	597.7
Minimum Necessary	926.2	536.7	5,756.7
Privacy Official	723.2	575.8	5,905.8
Accountings	261.5	95.9	1,125.1
BAs & BACs	299.7	55.6	800.3



Protecting Clients & Their Information

HIPAA Administrative Costs (\$M)

HIPAA Provision	Cost Yr 1 (2003)	Ave. Cost (Yrs 2-12)	Ave. Cost (2003-12)
NPP Provisions	50.8	37.8	391.0
*Consent	166.1	6.8	227.5
Access/Copying	1.3	1.7	16.8
PHI Amendment	5.0	8.2	78.8
Research	40.2	60.5	584.8
Training	287.1	50.0	737.2

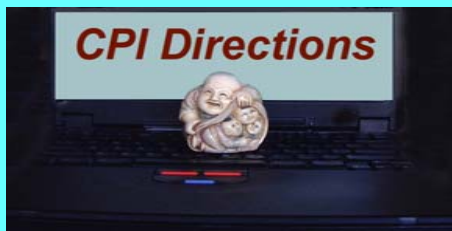


Protecting Clients & Their Information

HIPAA Administrative Costs (\$M)

HIPAA Provision	Cost Yr 1 (2003)	Ave. Cost (Yrs 2-12)	Ave. Cost (2003-12)
De-ID PHI	124.2	117.0	1,177.4
Health Plans	52.4	0	52.4
Complaints	6.6	10.7	103.2
Total*	\$3,242.0	\$1,556.9	\$17,554.7

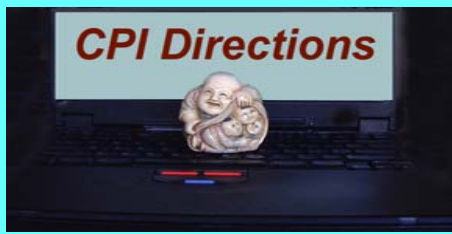
*Note: Numbers may not add due to rounding



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.”

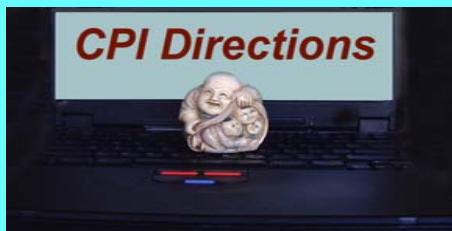


Protecting Clients & Their Information

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.

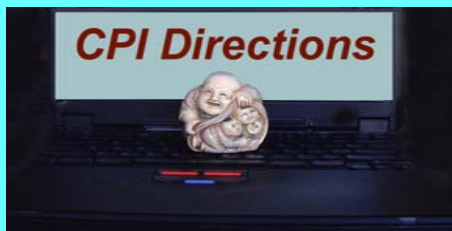


Protecting Clients & Their Information

Research WithOUT an Authorization

1. Written IRB or Privacy Board approval

- ID's IRB and the date "waiver" was approved
- Research not practical without PHI access, use, and "waiver"
- Description of "necessary" PHI
- "Waiver" approved under normal/expedited review
- Signature of IRB or Privacy Board (chair)
- Waiver satisfies the three criteria in the Rule

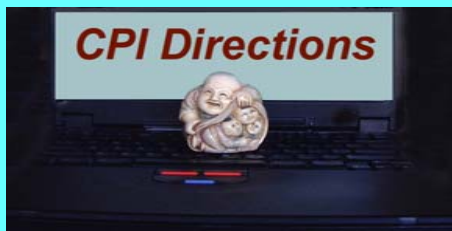


Protecting Clients & Their Information

3 HIPAA Criteria for an IRB

Minimum Risk to the Individual

- Plan to protect the identifiers from improper use or disclosure
- Plan to destroy identifiers at the earliest opportunity
- Written assurances that PHI will not be reused or disclosed except as allowed by law or for oversight

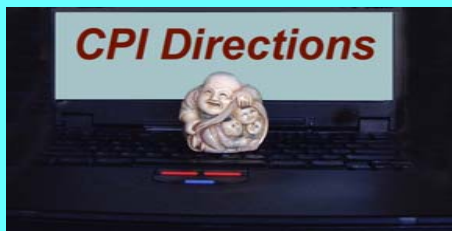


Protecting Clients & Their Information

Research WithOUT an Authorization

2. Preparatory to Research

- PHI is solely to prepare research protocol
- No removal of any PHI from the covered entity
- PHI is “necessary” for the research purpose

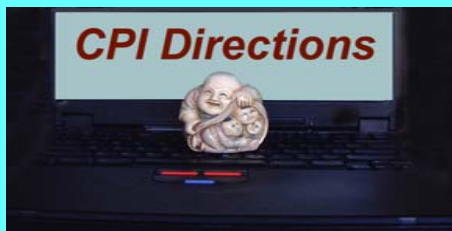


Protecting Clients & Their Information

Research WithOUT an Authorization

3. Research on PHI of Decedents

- PHI is solely for research about decedents
- PHI being sought is necessary for the research,
and,
- Documentation of the death of the individual(s)

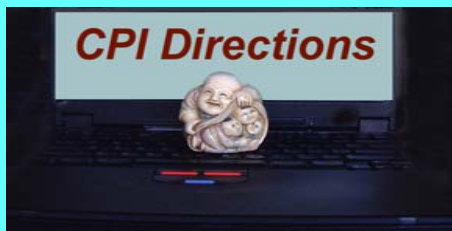


Protecting Clients & Their Information

Research WithOUT an Authorization

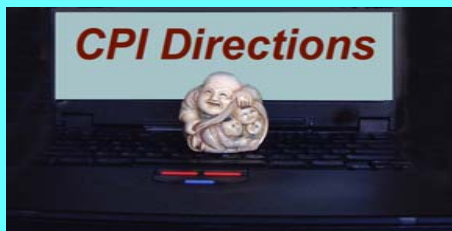
4. Limited Data Set & Data Use Agreement

- **LDS** excludes specific identifiers of the individual or of relatives, employers, or household members of the individual.
- **DUA** between CE and researcher documents who can use or receive the **LDS**



Protecting Clients & Their Information

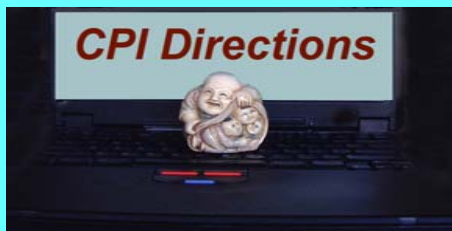
<u>Identifier</u>	<u>De-ID'd</u>	<u>LDS</u>
• Name	X	X
• Address components	X	Town, State Zip code OK
• All elements of dates	X	Dates OK
• Telephone or fax number	X	X
• E-mail, URL, IP addresses	X	X
• Social Security number	X	X
• Driver's license number	X	X
• Medical record number(s)	X	X
• Health plan 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

Contents of a Data Use Agreement (DUA):

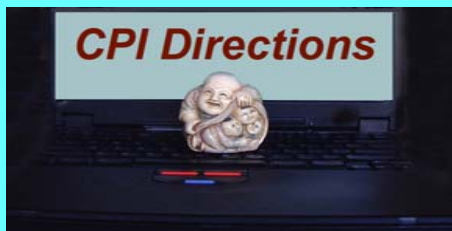
- Establish who is permitted to use or receive the LDS
- Establish permitted use / disclosure by the researcher
- May not authorize the researcher to (re)disclose the LDS in manner that would violate HIPAA
- State appropriate safeguards to prevent use or disclosure of the information other than as provided for by the DUA (including safeguards implemented by agents & subcontractors)
- Require reporting to the CE of any use / disclosure not provided for by the DUA
- May not (re)identify the LDS or contact subjects



Protecting Clients & Their Information

Research WITH an Authorization

- Requires *HIPAA compliant “authorization”*, but with some differences.....
- Possibility of “open ended” expiration date
- May be combined with a consent to participate in the research

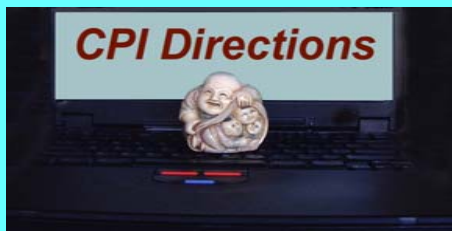


Protecting Clients & Their Information

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

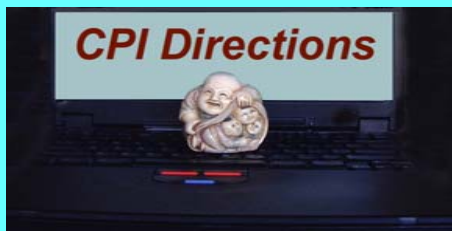
Transition from Pre- to Post-HIPAA

For PHI received prior to 4-15-2003:

- Authorization, express legal permission
- Informed consent to participate in research
- IRB waiver

Any consents sought, or PHI received after 4-15-2003:

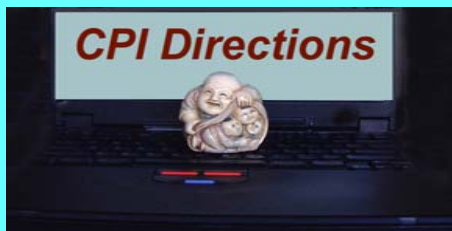
- HIPAA-compliant authorization may be required



Protecting Clients & Their Information

E-mail P&P to Protect PHI

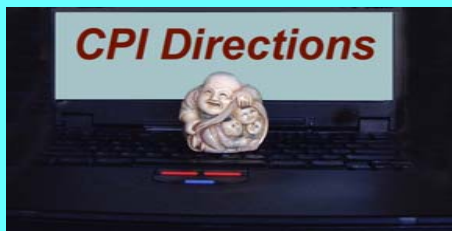
- Workforce has no privacy-rights when using CE's e-mail system
- CE has the right to monitor workforce e-mails
- Encrypt all e-mails containing PHI
- Include aspects of e-mail P&P in *Privacy Notice*
- Enforce workforce adherence to *User ID & Password P&P* (*no sharing of ID's & Passwords!*)



Protecting Clients & Their Information

Fax P&P to Protect PHI

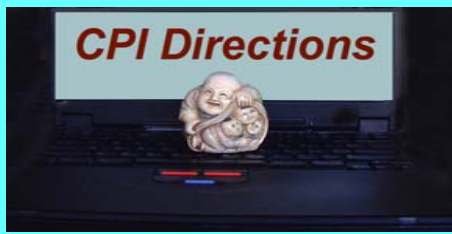
- Locate fax machines in secure, limited-access areas
- Use a *For-specified-eyes-only* fax cover-sheet
- Stamp *Confidential* on each document-sheet faxed
- Notify the recipient that a fax containing PHI is being sent
- Verify the fax number before faxing the PHI
- Test *programmed* fax numbers prior to sending
- Verify fax requests from unfamiliar sources
- Confirm that fax was received by the intended recipient
- Periodically ask trading partners if fax #'s have changed
- Store fax reports to allow for access audits



Protecting Clients & Their Information

CPI's HIPAA Services & Work-Products

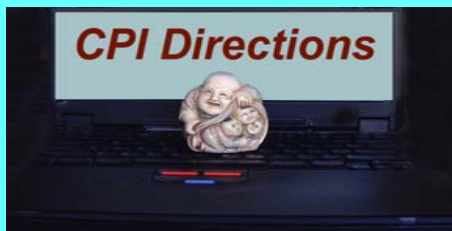
- Practice-specific HIPAA policies and procedures
- Workflow, gap and risk analyses for the HIPAA transactions, privacy, security, and unique identifier rules
- Remediation reports for HIPAA transactions, privacy, security, and unique identifier rules
- Statistical services, including de-identification of protected health information
- Electronic HIPAA databases and applications for tracking and reporting use and disclosure of PHI
- Development and implementation of electronic medical records (EMRs)



Protecting Clients & Their Information

CPI's HIPAA Services & Work-Products

- “Roadmaps” & checklists
- HIPAA awareness orientation and training, seminars, workshops for all levels of the workforce
- Templates for the Notice of Privacy Practice, Acknowledgement & Authorization Forms, Business Associate Contracts, Trading Partner Agreements, Data Use Agreements
- Policy & procedure outlines
- E-mail Q&A service and HIPAA advisory
- Privacy Officer services, including administration of consumer “rights” and resolution of complaints



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>