

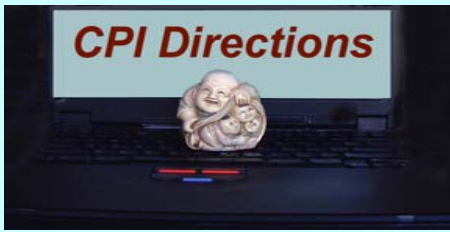
## ***Protecting Clients & Their Information***

# ***Medical Records Law: HIPAA Privacy Regulations*** (Lorman Education Services)

Presented in New York City on February 24, 2005 by:

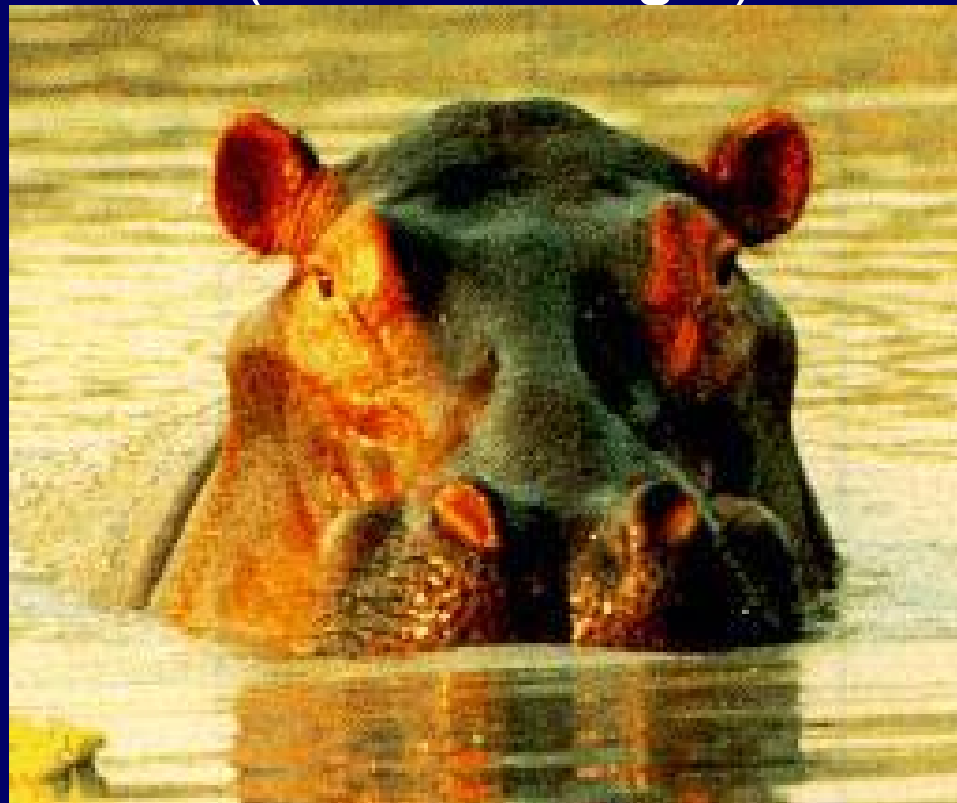
**Matthew Rosenblum**  
Chief Operations Officer  
& Senior Consultant for  
Privacy, Regulatory Affairs & Quality Management

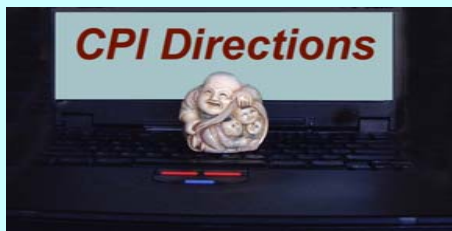
***CPI Directions, Inc.***  
10 West 15th Street, Suite 1922  
New York, NY 10011  
<http://www.CPIdirections.com>  
[CPIdirections@att.net](mailto:CPIdirections@att.net)  
(212) 675-6367



## ***Protecting Clients & Their Information***

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



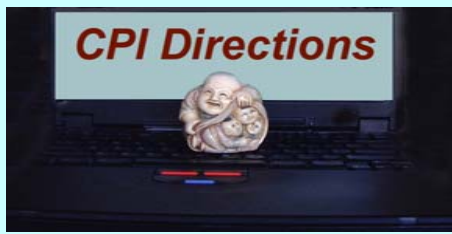


## ***Protecting Clients & Their Information***

### ***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***: may require 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

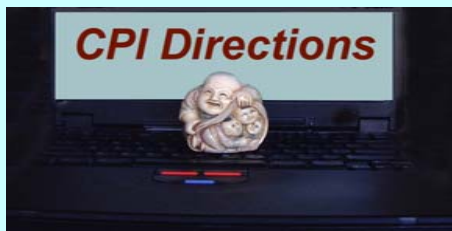


## ***Protecting Clients & Their Information***

### ***HIPAA Privacy Costs (Average per Year)***

<b>SIC</b>	<b>Industry</b>	<b>Yr 1</b>	<b>Yrs 2-10</b>
8010	Doctors Office	\$3,703	\$2,086
8050	Nursing Care	\$8,301	\$4,676
8060	Hospitals	\$101,999	\$38,244
8070	Medical & Dental Labs	\$3,169	\$1,785
5910	Pharmacies	\$6,436	\$3,625

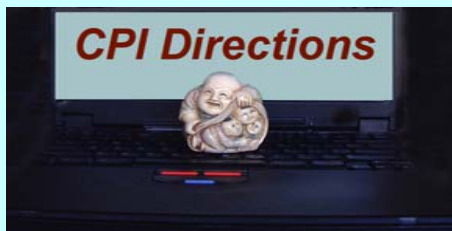
**\*Source: Office of Advocacy, U.S. Small Business Administration, from data provided by the Bureau of the Census, Statistics of U.S. Businesses, 1997**



## ***Protecting Clients & Their Information***

### Some recent **HORROR** stories

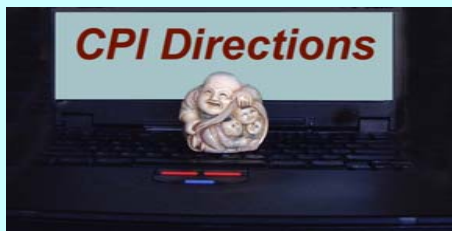
- Large Pharmaceutical Company: Revealed >600 patient e-mail addresses when it sent a message to every individual registered to receive reminders about taking Prozac.
- Major Medical Research University: 1) Mistakenly posted the MH records of 20 children on a public Web site. 2) Mailed a survey to 1200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

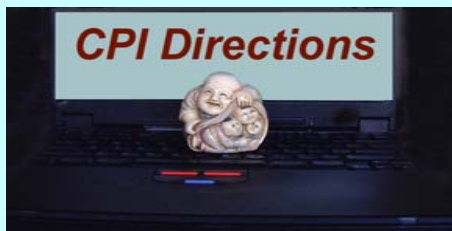
- **Transaction Standards (TCS)**: standardizes and reduces the current # of electronic formats (claims, eligibility, etc.)
- **Privacy Standards**: provides that our *PHI* will be protected from *bad* uses and disclosures, and provides the patient/client with certain *controls* and *rights*
- **Security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

### ***HIPAA Timeline & Deadlines***

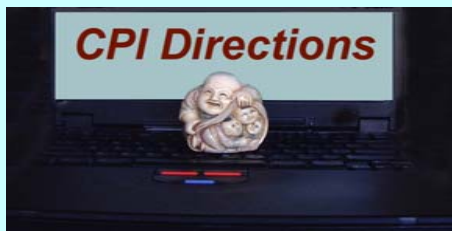
- **August 1996:** Congress passes HIPAA
- **1998-9:** Proposed HIPAA rules formulated & published
- **August 2000:** Final *Transaction Rules* published
- **December 2000:** Final *Privacy Rules* published
- **December 2001:** ASCA - Final *TCS Rule* extension to 10-2003, if implementation plan filed 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 **4-20-2005**
- **April 17, 2003:** Interim *Enforcement Rules* published, effect. **5-19-2003**
- **January 23, 2004:** Final *NPI rules* published, comply by **5-23-2007**



## ***Protecting Clients & Their Information***

### ***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***

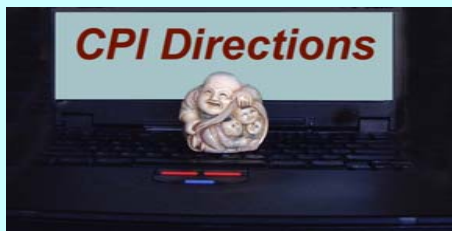
# ***Uses & Disclosures of PHI***

### **Minimum necessary principle**

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

- **For disclosures to providers for treatment purposes**
- **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***

### ***Designated Record Set***

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

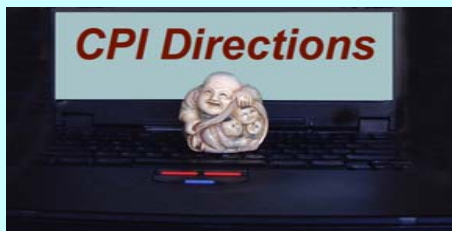
- The medical records and billing records about individuals maintained by or for a covered health care provider, or
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan, or
- Used, in whole or in part, by or for the CE to make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



## ***Protecting Clients & Their Information***

HIPAA mandates (only) two types of disclosures of PHI:

- Disclosures to patients
- Disclosures to Federal HHS, CMS, OCR (pursuant to a patient complaint)



## ***Protecting Clients & Their Information***

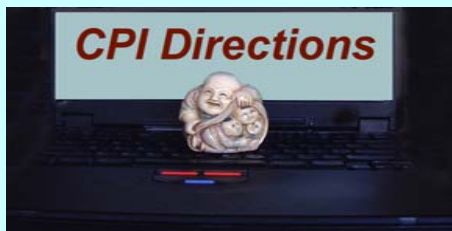
### **TPO: What is meant by Treatment?**

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

- **Coordination or management of healthcare by a provider with a 3<sup>rd</sup> 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.**

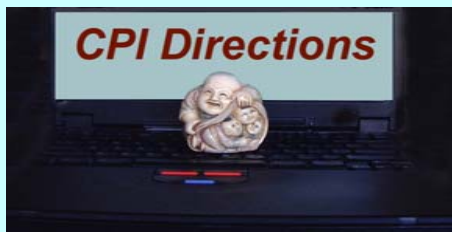
**Indirect treatment relationship: E.g., remote consults, diagnoses, laboratory work-ups, and radiological readings.**



## ***Protecting Clients & Their Information***

### **TPO: What is meant by Payment?**

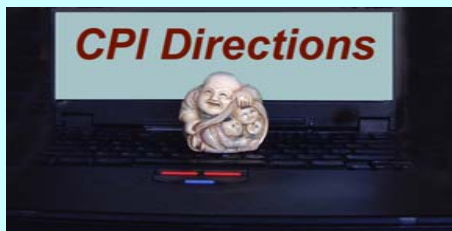
- Review of care for medical necessity, health plan coverage, appropriateness of care, justification of charges
- UR activities, pre-certification and preauthorization of services, concurrent and retrospective review of services
- Determinations of eligibility or coverage, coordination of benefits and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

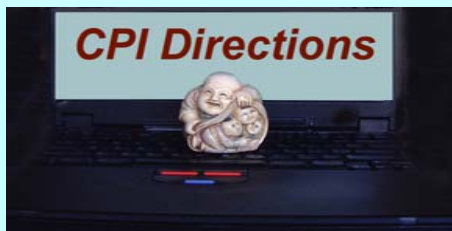
- **Case management/coordination, contacting providers & patients re treatment alternatives, related functions**
- **Workforce evaluation, training, activities re accreditation, certification, licensing, credentialing**
- **Peer review, legal services, auditing functions re fraud, abuse detection, compliance**
- **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***

# ***HIPAA Requirements***

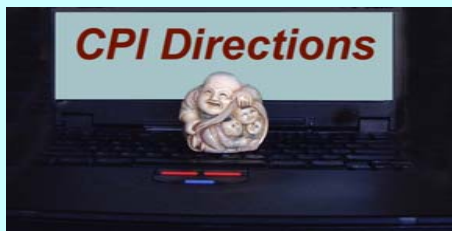
- **Policies and procedures**: Create & implement a privacy P&P set. Having a “a policy” is NOT adequate; P&P set must take into account the CE’s size and type of operations
- **Privacy & Security Officials**: Requires (documented) appointment of individual(s) to be accountable for the development implementation of privacy AND security 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.



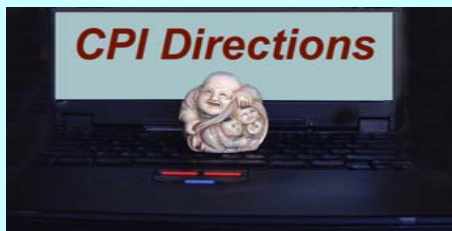
## ***Protecting Clients & Their Information***

### ***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.

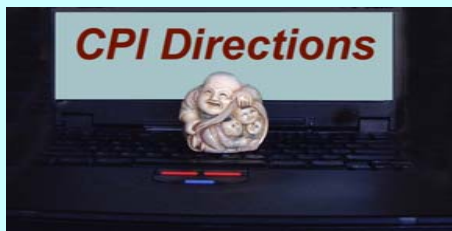
**Right to accounting of disclosures of PHI:** Right to an accounting of PHI disclosures within the last 6 years, or since compliance was first required for the CE. Exceptions for disclosures for **TPO**, disclosures pursuant to an authorization



## ***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***

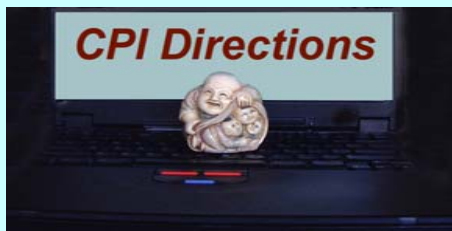
### ***And yet even more Rights and P&P's***

**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

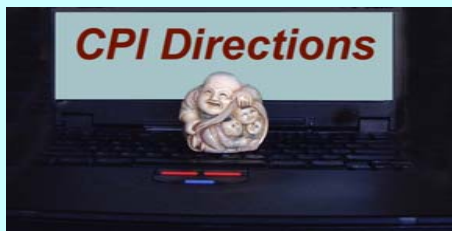


## ***Protecting Clients & Their Information***

# ***Privacy: Authorizations***

## **Components of an Authorization Form:**

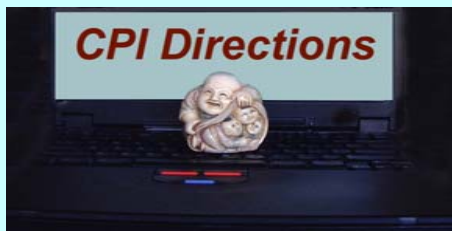
- A description of the information to be used or disclosed
- ID's the persons authorized to make use or disclosure
- ID's the persons who use, or to whom the CE may make the disclosure
- Description of each purpose of the use or disclosure.  
May be as simple as, "at the request of the individual".
- 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***

# ***HIPAA Security Rule related to other Regulatory rules & guidelines, Accreditor standards***

- HIPAA Privacy & Security
- FDA research data
- SAMHSA & AIDS/HIV
- NIST
- JCAHO
- URAC
- Etc. etc. etc



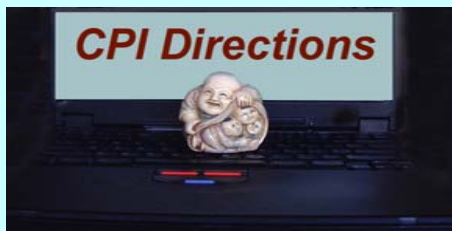
## ***Protecting Clients & Their Information***

### ***Some Overlap with State HIV/MH/CD Laws & Federal SAMHSA Regulations***

- Uses & disclosures for treatment, payment, operations
- Minimum necessary
- Need for consents & authorizations

### **However, HIPAA directly covers additional matters, e.g.:**

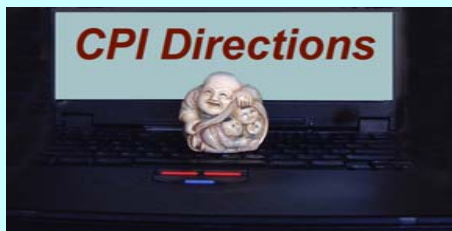
- More expansive definition of protected information
- Privacy Official, Security Official, and “Offices”
- Business associate terms
- Notice of privacy practices (NPP)
- Confidential communications
- Complaints to HHS; oversight by OCR
- Accountings of disclosures
- Access & amendment of PHI, etc., etc., etc.



## ***Protecting Clients & Their Information***

# **Special status for “Psychotherapy (Process) Notes”**

- Recorded by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session, and
- Maintained separate from the medical record, and
- Must exclude:
  - Medication prescription and monitoring
  - Counseling session start and stop times
  - The modalities and frequencies of treatment furnished
  - Results of clinical tests
  - Summary of diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date



## ***Protecting Clients & Their Information***

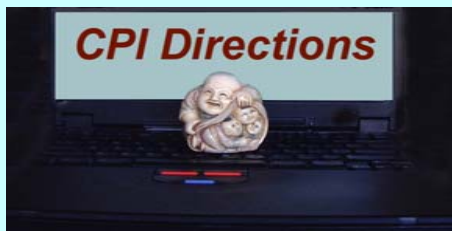
# Special status for “Psychotherapy Notes”

- HIPAA requires a covered entity to obtain a patient’s written authorization, prior to disclosing the contents of psychotherapy notes for treatment, payment, or healthcare operations (TPO).
- HIPAA does NOT require access by individual that is the subject of the “psychotherapy notes”
- May be used by writer of the note for “legal defense”
- May be disclosed to supervisor during training



## ***Protecting Clients & Their Information***

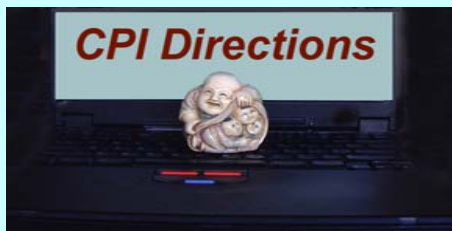
**Use of ICD diagnostic code sets, as opposed to the DSM-IV, in standardized electronic transaction reports (e.g. claims & payments)**



## ***Protecting Clients & Their Information***

### ***And Yet More Required P&P's!***

- **Sanctions**: Corrective & disciplinary actions
- **Mitigation**: Positive actions to minimize *harmful effects* of Privacy breaches. BA's to notify CE of breaches
- **Safeguards**: *Appropriate & reasonable* administrative, technical, and physical safeguards
- **Contingency Plans**: Assess systems for anticipated risks; plan to detail how data will be maintained and duplicated
- **Complaints**: Complaints to CE & HHS/OCR

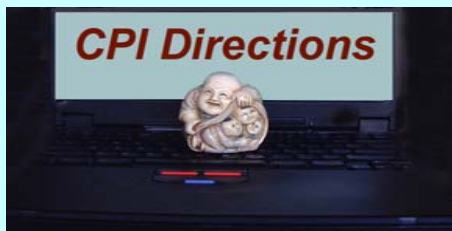


## ***Protecting Clients & Their Information***

# ***Business Associate Contracts (BAC)***

## ***Privacy Rule Specifications:***

- 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)

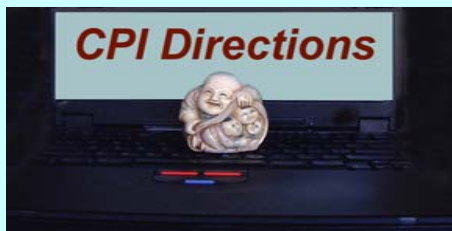


## ***Protecting Clients & Their Information***

### ***Additional BAC Specifications***

*Added under Security Rule:*

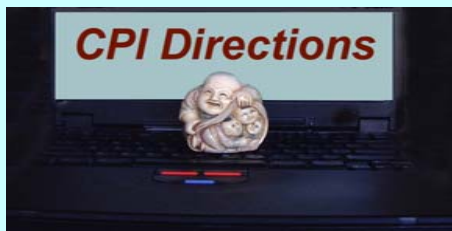
- BA safeguards to protect confidentiality, integrity, and availability of the ePHI
- Subcontractor(s) to implement reasonable and appropriate safeguards
- BA to report security incidents to CE
- Availability of BA's "electronic security" policies & procedures (to HHS)
- Authorize BAC termination by CE if BA has violated a material term of the contract



## ***Protecting Clients & Their Information***

# ***Research, as Defined by HIPAA***

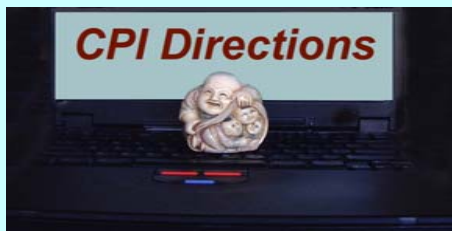
**“.....a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.”**



## ***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*



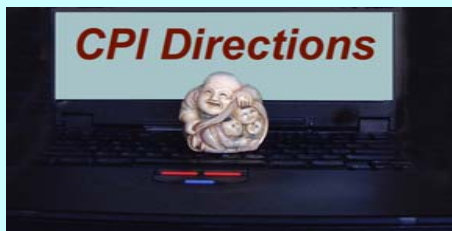
# *Protecting Clients & Their Information*

## Identifier

## De-ID'd

## LDS

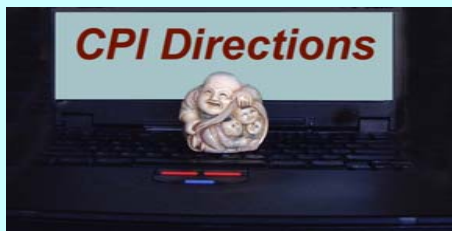
• Name	X	X
• Address components	X	Town, State Zip code OK
• All elements of dates	X	Dates OK
• Telephone or fax number	X	X
• E-mail, URL, IP addresses	X	X
• Social Security number	X	X
• Driver's license number	X	X
• Medical record number(s)	X	X
• Health plan numbers	X	X
• Account numbers	X	X
• Certificate, 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***

### ***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

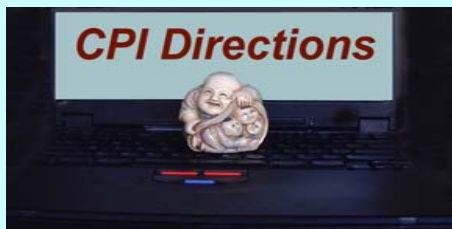


## ***Protecting Clients & Their Information***

### ***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:*

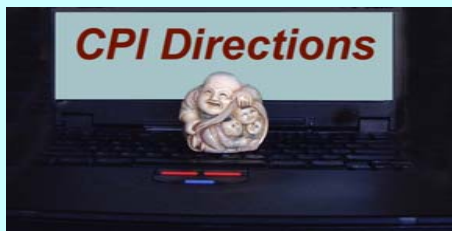
- Descriptions of products or services
- Replacements or enhancements of products or services
- Treatment communications
- Most face-to-face communications
- Providing items of nominal value (e.g., calendars, pens with provider's name)



## ***Protecting Clients & Their Information***

# ***HIPAA-Required Electronic Security Policies & Procedures***

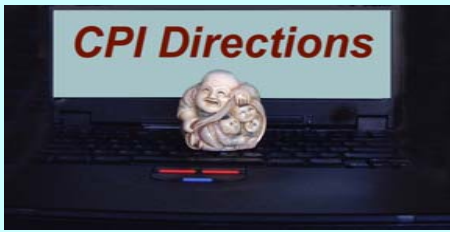
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards



# *Protecting Clients & Their Information*

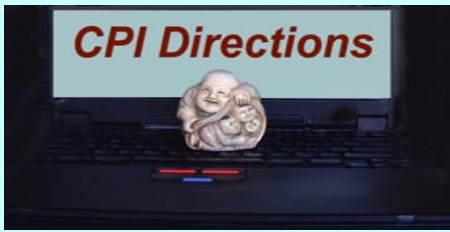
## Administrative Safeguards

Standards	CFR	Implementation Specifications	Required or Addressable
Security Management Process	164.308(a)(1)	Risk Analysis & Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)	Security Official	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure, Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Healthcare Clearinghouse Function	(R)
		Access Authorization, Establishment, and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software (and Viruses!)	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan & Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)	<i>(as per Security Management, above)</i>	(R)
Business Associate Contracts	164.308(b)(1)	Written Contract or Other Arrangement	(R)



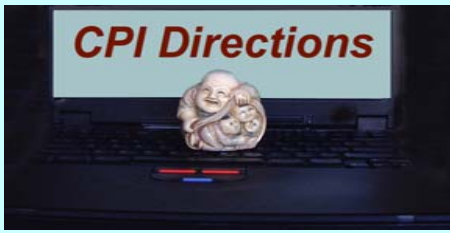
# ***Protecting Clients & Their Information***

<b>Physical Safeguards</b>			
<b>Standards</b>	<b>CFR Sections</b>	<b>Implementation Specifications</b>	<b>Required or Addressable</b>
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)	<i>(as per Security Management, Awareness, and Access Controls, above)</i>	(R)
Workstation Security	164.310(c)	<i>(as per Security Management, Awareness, and Access Controls, above)</i>	(R)
Device and Media Controls	164.310(d)(1)	Media Disposal	(R)
		Media Re-use	(R)
		Media Accountability	(A)
		Data Backup and Storage (during transfer)	(A)



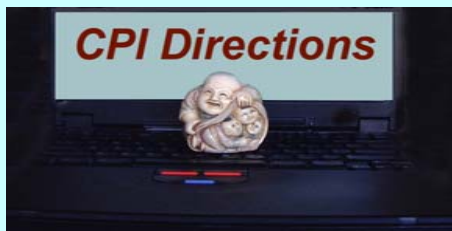
# *Protecting Clients & Their Information*

<b>Physical Safeguards</b>			
<b>Standards</b>	<b>CFR Sections</b>	<b>Implementation Specifications</b>	<b>Required or Addressable</b>
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)	<i>(as per Security Management, Awareness, and Access Controls, above)</i>	(R)
Workstation Security	164.310(c)	<i>(as per Security Management, Awareness, and Access Controls, above)</i>	(R)
Device and Media Controls	164.310(d)(1)	Media Disposal	(R)
		Media Re-use	(R)
		Media Accountability	(A)
		Data Backup and Storage (during transfer)	(A)



# *Protecting Clients & Their Information*

<b>Technical Safeguards</b>			
<b>Standards</b>	<b>CFR Sections</b>	<b>Implementation Specifications</b>	<b>Required or Addressable</b>
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption (data at rest)	(A)
Audit Controls	164.312(b)	Record and Examine Activity in Information Systems	(R)
Integrity	164.312(c)(1)	Protection Against Improper Alteration or Destruction of Data	(A)
Person or Entity Authentication	164.312(d)	Verification of user	(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption (FTP and Email over Internet)	(A)



## ***Protecting Clients & Their Information***

### ***Penalties for Privacy Breaches***

#### **➤ Civil monetary fines:**

Up to \$100 per person, per violation

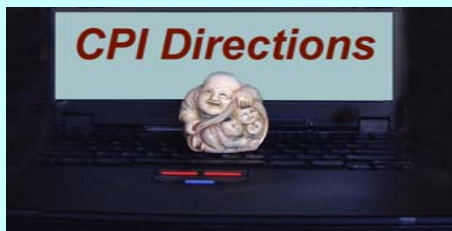
Up to \$25K per person, per standard, per year

#### **➤ Criminal penalties:**

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

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

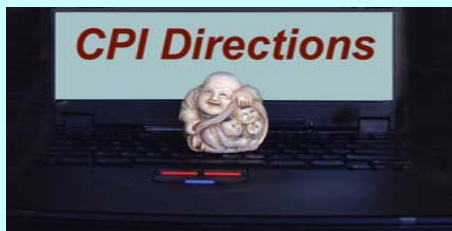
Up to \$250K + 10 yrs prison: (sale, malicious harm)



## ***Protecting Clients & Their Information***

### ***“Administrative Simplification” & Implementation Management***

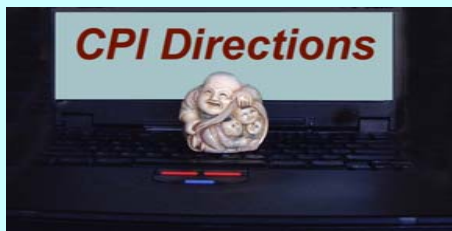
- Identification of Risks: Risk Analysis, FMEA, RCA
- Data Collection: Automated Applications & Paper Forms
- Data Aggregation & Tracking: Useable reports
- Feedback mechanisms & Continuous Performance Improvement (CPI)



## ***Protecting Clients & Their Information***

### ***Quality Management & Testing Effectiveness of P&Ps***

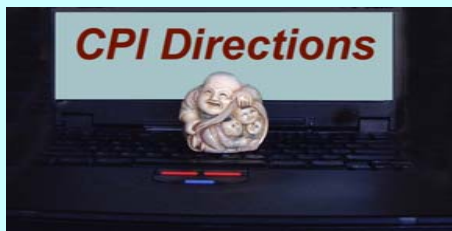
- Audit logs
- Supervision
- Continuous performance evaluations
- “Complaints”
- Patient perception
- Workforce recommendations



## ***Protecting Clients & Their Information***

### ***Tracking the HIPAA HIPPO***

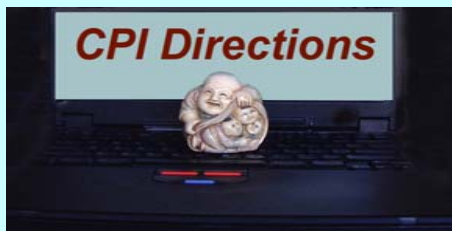
- Requests to amend/access PHI; CE denials; complaints
- NPPs & Acknowledgements
- Authorizations
- Workforce awareness training
- Disclosure accountings
- Patient requests for confidential communications
- Agreed-upon restrictions
- Opt-outs from fundraising
- Opt-outs from facility directory
- Business associate contracts
- Data use agreements
- 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***

### ***CE's Internal Considerations***

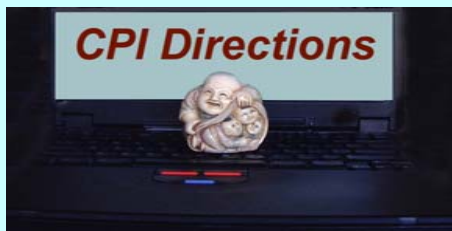
- Limited resources: personnel, time, budget
- Gaps in HIPAA expertise
- Ongoing responsibilities of workforce
- New Projects, not related to HIPAA
- Ability to remain current on HIPAA legislation and all related laws



## ***Protecting Clients & Their Information***

### ***Information Needed About a CE***

- Sharing of PHI among and within CEs & BAs
- Workflows, policies, and procedures
- Software applications & complementary products
- Data storage
- Workforce awareness of HIPAA
- Audit trails, monitoring uses & disclosures of PHI
- Physical security and access controls
- Encryption
- De-identification of PHI



## ***Protecting Clients & Their Information***

# ***CPI's Assessments & Risk Analyses***

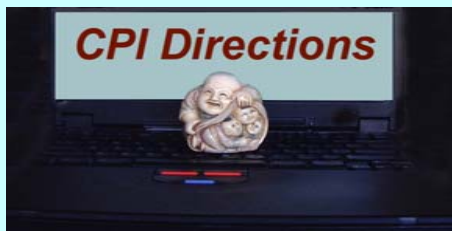
### **Assessment Analysis**

- **Entities Assessment**
- **Business Associate (BA) Assessment**
- **Transaction & Code Sets Assessment**
- **Assessment of Software & Complementary Products**
- **Privacy Assessment**
- **Security Assessment & Risk Analysis**
- **Workforce Awareness Assessment**

### **Deliverables**

- **Entities and BA HIPAA Relationship Model**
- **High Level Gap Analysis**
- **Scope & Schedule for Risk Analysis**
- **Definitive List of Short-Term Compliance Actions\***
- **Project Plan for Long-Term HIPAA Compliance Actions\***

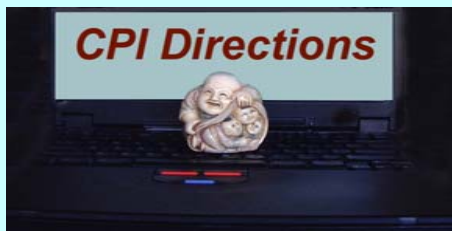
\*Considering remediation recommendations for software & IT, complementary products, education & training, HIPAA documents, physical-plant, administrative P&P, subject matter expertise, etc.



## ***Protecting Clients & Their Information***

# ***CPI's HIPAA Services & Work-Products***

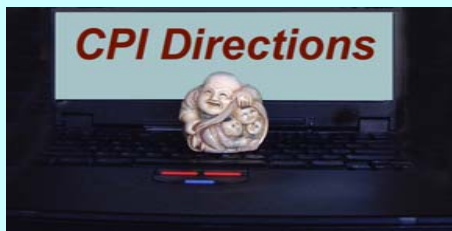
- Templates, checklists, and "roadmaps"
- Security & Privacy awareness training, seminars, workshops for all levels of the workforce
- Templates for the Notice of Privacy Practice, Acknowledgement & Authorization Forms, Business Associate Contracts, Trading Partner Agreements, Data Use Agreements
- Privacy & Security policy & procedure outlines
- E-mail Q&A service and HIPAA advisory
- Security & Privacy Official services



## ***Protecting Clients & Their Information***

### ***CPI's HIPAA Services & Work-Products***

- Practice-specific policies and procedures
- Workflow, gap and risk analyses for the TCS, Privacy, Security, and Unique identifier rules
- Remediation reports for TCS, Privacy, Security, and Unique identifier rules
- Statistical services, including de-identification of PHI
- Electronic databases and applications for tracking and reporting use and disclosure of PHI
- Secure Email & Electronic medical records (EMRs)

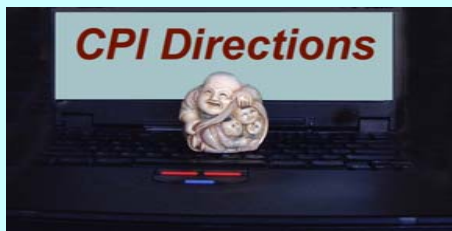


## ***Protecting Clients & Their Information***

### **Two HIPAA Realities:**

***“HIPAA is driving the health industry out of the paper-age, and into the digital age”***

***“HIPAA is a marathon, not a 100-yard dash, and it will require the same internalization into organizational process as did the Medicare & Medicaid regulations, and that took a decade”***



## ***Protecting Clients & Their Information***

For additional information, please contact:

**Matt Rosenblum**

**Chief Operations Officer**

**Privacy, Security, QM & Regulatory Affairs**

***CPI Directions, Inc.***

**10 West 15<sup>th</sup> Street, Suite 1922**

**New York, NY 10011**

**(212) 675-6367**

**MRosenblum@att.net**

**<http://www.CPIdirections.com>**