

Protecting Clients & Their Information

Practical HIPAA Security: Policies, Procedures, Workforce Training & Testing (Lorman Education Services)

Presented in East Brunswick NJ on June 16, 2004 by:

Matt Rosenblum

Chief Operations Officer

Privacy, Security, Regulatory Affairs & Quality Management

CPI Directions, Inc.

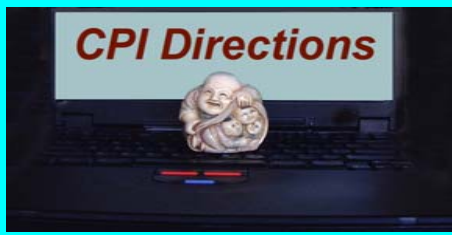
10 West 15th Street, Suite 1922

New York, NY 10011

<http://www.CPIdirections.com>

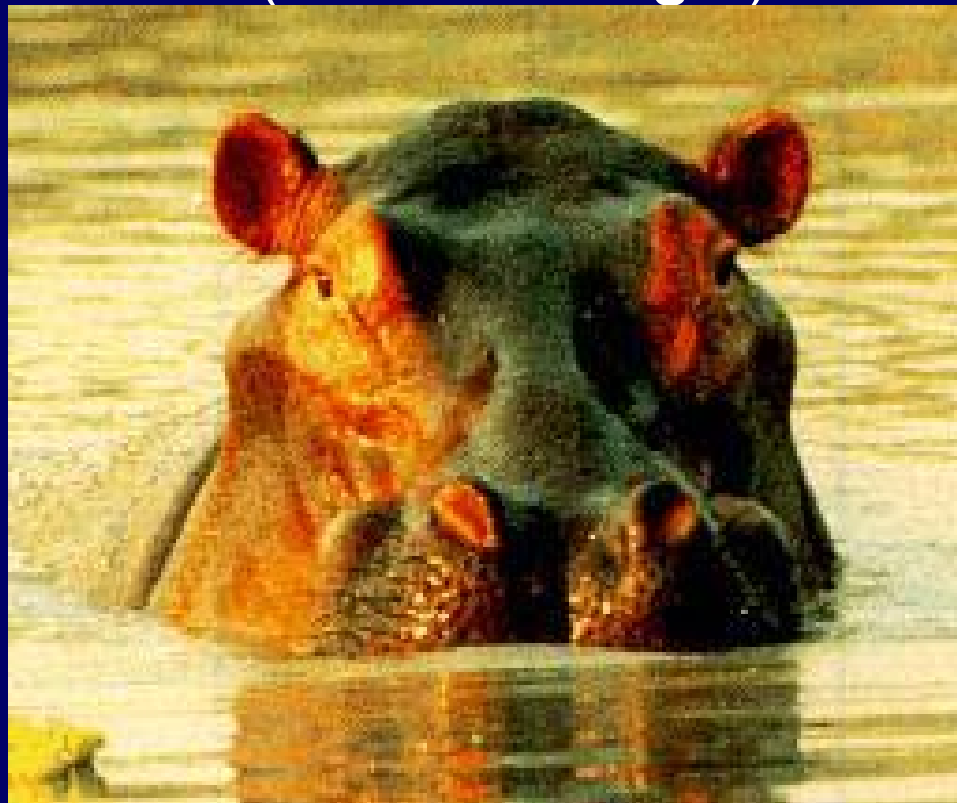
CPIdirections@att.net

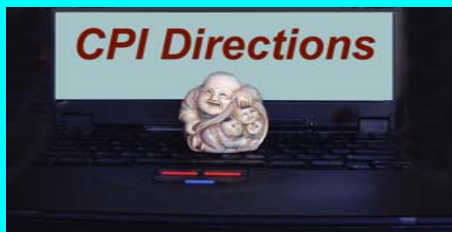
(212) 675-6367



Protecting Clients & Their Information

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

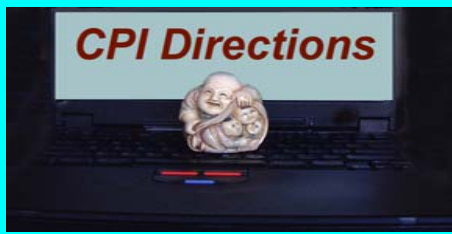




Protecting Clients & Their Information

“HIPAA is the catalyst to transform health care industry from Paper-Age to Digital-Age”

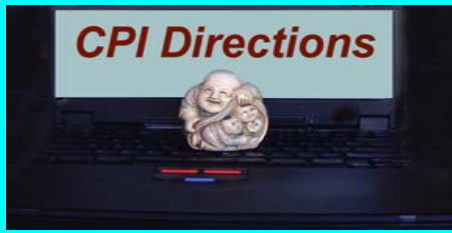
- Driving administrative simplification through standardized transaction formats
- Establishing standards for privacy & security that enable low cost electronic transactions through channels such as the Internet
- CMS estimates that over \$220 billion is spent annually on administrative expenses in healthcare. A study in 1994 suggested that over \$70 billion could be saved through electronically enabled transactions.



Protecting Clients & Their Information

Some recent **HORROR** stories

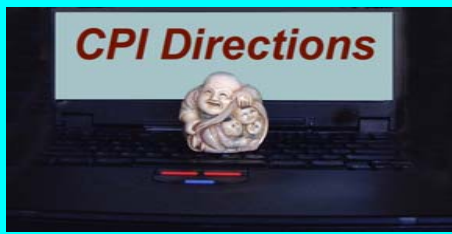
- Large Pharmaceutical Company: Revealed >600 patient e-mail addresses when it sent a message to every individual registered to receive reminders about taking Prozac.
- Major Medical Research University: 1) Mistakenly posted the MH records of 20 children on a public Web site. 2) Mailed a survey to 1200 transplant recipients participating in a long-term research study and mistakenly revealed the names of those who had donated their kidney to the recipients.



Protecting Clients & Their Information

Be Reasonable

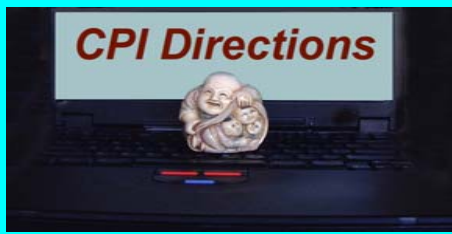
- No single correct methodology to HIM strategy
- Mutual and competing interests in (and outside) of entity
- Cultural shifts
- Technological evolution



Protecting Clients & Their Information

Good HIPAA & Bad HIPAA

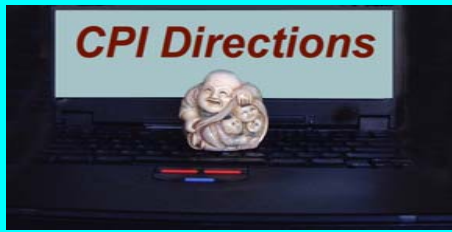
- Incidental disclosures vs. HIPAA breaches
- Accidents happen
- Knowing (Up to \$50K + 1 yr prison)
- Pretense (Up to \$100K + 5 yrs prison)
- Malicious (Up to \$250K + 10 yrs prison)



Protecting Clients & Their Information

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

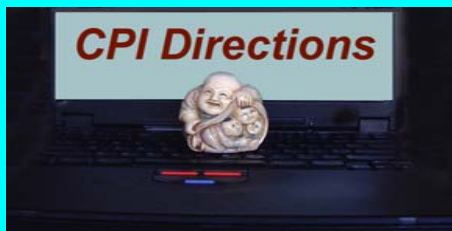
- HIPAA Privacy & Security
- FDA research data
- SAMHSA & AIDS/HIV
- NIST
- JCAHO
- URAC
- Etc. etc. etc



Protecting Clients & Their Information

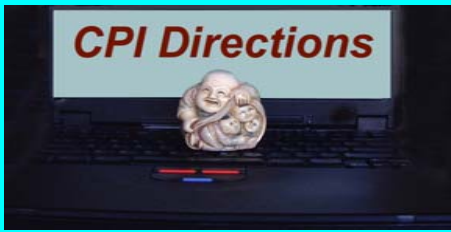
HIPAA-Required Policies & Procedures

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards



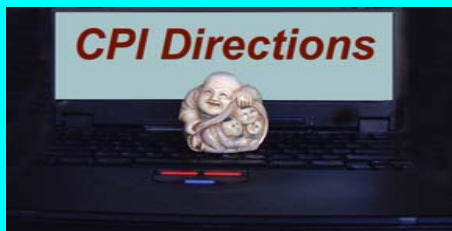
Protecting Clients & Their Information

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)	(as per Security Management , above)	(R)
Business Associate Contracts	164.308(b)(1)	Written Contract or Other Arrangement	(R)



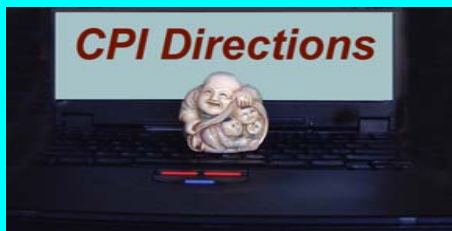
Protecting Clients & Their Information

Physical Safeguards			
Standards	CFR Sections	Implementation Specifications (R)=Required (A)=Addressable	Required or Addressable
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)



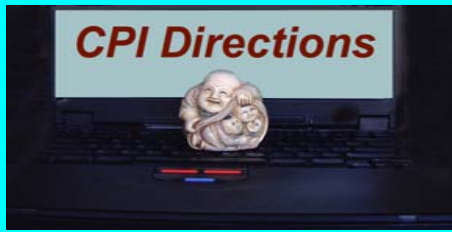
Protecting Clients & Their Information

Physical Safeguards			
Standards	CFR Sections	Implementation Specifications (R)=Required (A)=Addressable	Required or Addressable
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

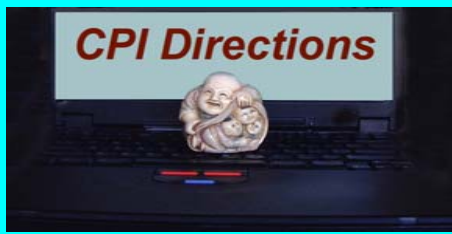
Technical Safeguards			
Standards	CFR Sections	Implementation Specifications	Required or Addressable
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption (data at rest)	(A)
Audit Controls	164.312(b)	Record and 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

Assignment of Responsibility

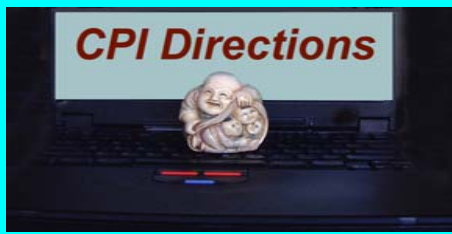
- Security Official
- Supportive Office & Staffing
- Job description components for all levels of workforce
- Use of vendors and consultants



Protecting Clients & Their Information

Security Awareness and Training

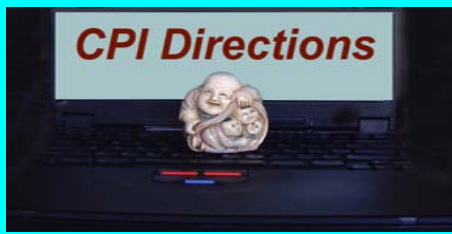
- Security reminders
- Incident reporting
- How to protect and guard the system from malicious software
- Procedures for detecting and reporting malicious software
- Procedures for monitoring log-in attempts and reporting discrepancies
- Password management and use



Protecting Clients & Their Information

Security Awareness & Training Presentation Materials

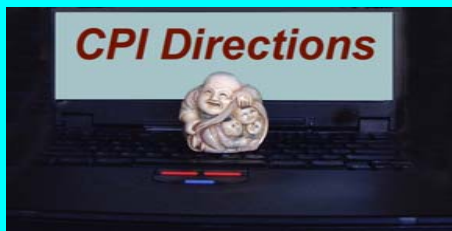
- Case studies
- Frequency Mode Effect Analysis (FMEA): Proactive Method
- Root Cause Analysis (RCA): Retrospective Method
- Resources & Supports: posters, distribution of information security trinkets, security messages and slogans available for computer screensavers & mouse pads, and occasional facility-wide e-mail messages and advisories



Protecting Clients & Their Information

Security Awareness & Training Presentation Materials

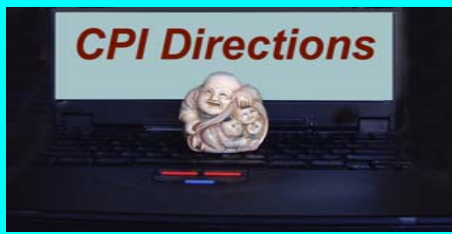
- Case studies
- Frequency Mode Effect Analysis (FMEA): Proactive Method
- Root Cause Analysis (RCA): Retrospective Method
- Resources & Supports: posters, distribution of information security trinkets, security messages and slogans available for computer screensavers & mouse pads, and occasional facility-wide e-mail messages and advisories



Protecting Clients & Their Information

Workforce Security

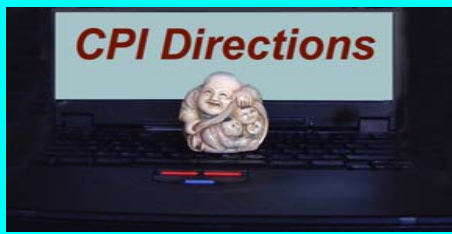
- Authorization and/or Supervision
- Workforce Clearance Procedure
- Termination Procedures



Protecting Clients & Their Information

Contingency Plan

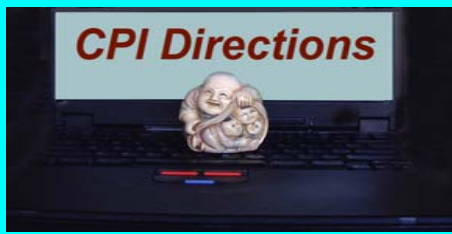
- Data Backup Plan & Disaster Recovery Plan
- Emergency Mode Operation Plan
- Testing and Revision Procedure
- Applications and Data Criticality Analysis



Protecting Clients & Their Information

Contingency Plan

- Data Backup Plan & Disaster Recovery Plan
- Emergency Mode Operation Plan
- Testing and Revision Procedure
- Applications and Data Criticality Analysis

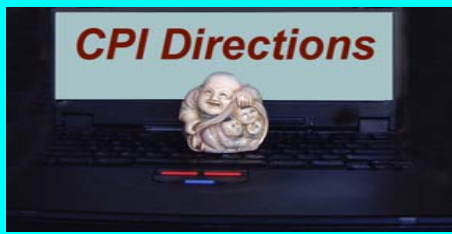


Protecting Clients & Their Information

Business Associate Contracts (BAC)

Privacy Rule Specifications:

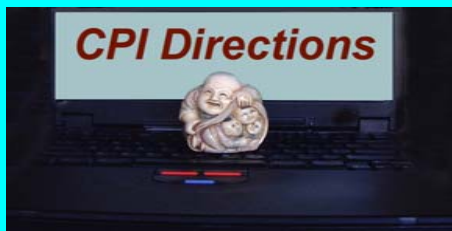
- Signatures, contract start/expiration or review dates
- Terms & conditions, including conditions for disclosure of PHI, data rights of each party, minimum security
- Procedures for reporting breaches and time frame
- Method of recording breaches: incident logs
- Penalties: intentional vs. unintentional 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 & Supportive BAC Terms under Security Rule

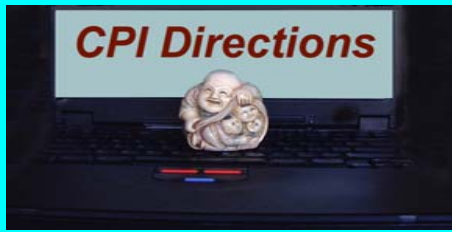
- BA safeguards to protect confidentiality, integrity, and availability of the ePHI
- Subcontractor(s) to implement reasonable and appropriate safeguards
- BA to report security incidents to CE
- Availability of BA's policies & procedures (to HHS)
- Authorize BAC termination by CE if BA has violated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



Protecting Clients & Their Information

Facility Access Controls

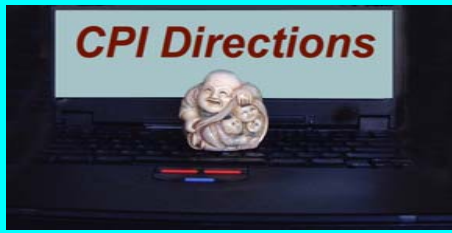
- Contingency Operations & Vulnerabilities
- Facility Security Plan
- Access Control and Validation Procedures
- Maintenance Records



Protecting Clients & Their Information

Device and Media Controls

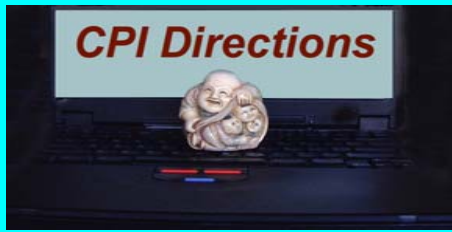
- Media Disposal
- Media Re-use
- Media Accountability
- Data Backup and Storage (during transfer)



Protecting Clients & Their Information

Device and Media Controls

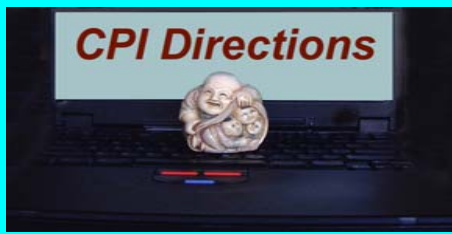
- Media Disposal
- Media Re-use
- Media Accountability
- Data Backup and Storage (during transfer)



Protecting Clients & Their Information

Data Encryption

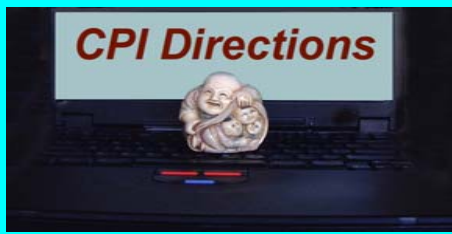
- What will encryption protect?
- What will encryption not protect?
- Email (data in transit)
- Storage (data at rest)



Protecting Clients & Their Information

Workstation Use & Access Control

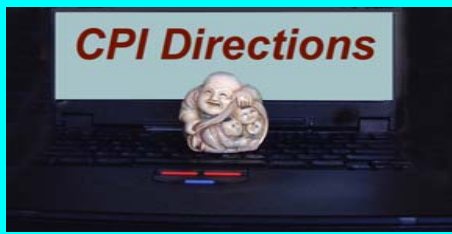
- Identify workstation types and functions & uses
- Identify expected performance of each type of workstation
- Analyze physical surroundings for physical attributes



Protecting Clients & Their Information

“Administrative Simplification” & Implementation Management

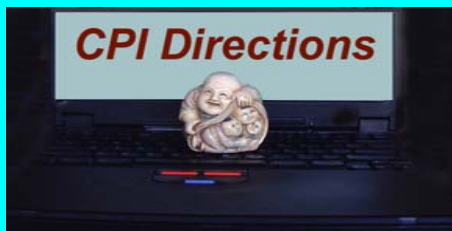
- Identification of Risks: Risk Analysis, FMEA, RCA
- Data Collection: Automated Applications & Paper Forms
- Data Aggregation & Tracking: Useable reports
- Feedback mechanisms & Continuous Performance Improvement (CPI)



Protecting Clients & Their Information

Quality Management & Testing Effectiveness of P&Ps

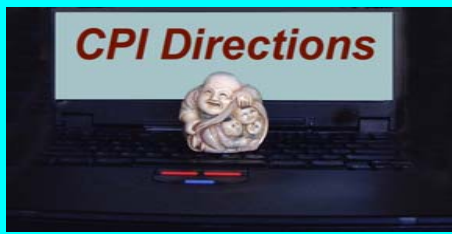
- Audit logs
- Supervision
- Continuous performance evaluations
- “Complaints”
- Patient perception
- Workforce recommendations



Protecting Clients & Their Information

Tracking the HIPAA HIPPO

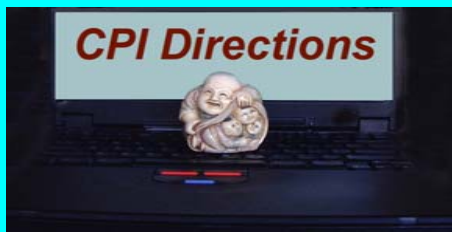
- Requests to amend/access PHI; CE denials; complaints
- NPPs & Acknowledgements
- Authorizations
- Workforce awareness training
- Disclosure accountings
- Patient requests for confidential communications
- Agreed-upon restrictions
- Opt-outs from fundraising
- Opt-outs from facility directory
- Business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

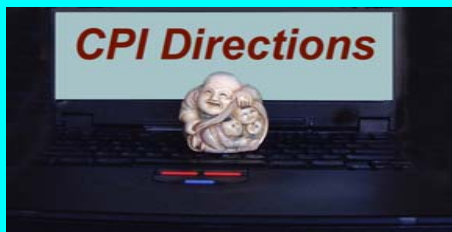
- Limited resources: personnel, time, budget
- Gaps in HIPAA expertise
- Ongoing responsibilities of workforce
- New Projects, not related to HIPAA
- Ability to remain current on HIPAA legislation and all related laws



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

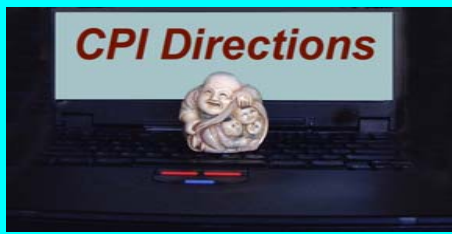
Assessment Analysis

- **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***

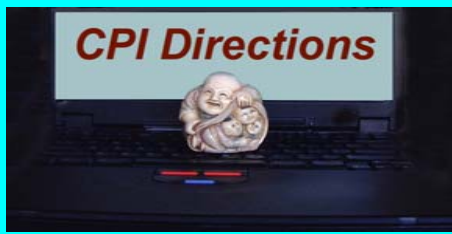
*Considering remediation recommendations for software & IT, complementary products, education & training, HIPAA documents, physical-plant, administrative P&P, subject matter expertise, etc.



Protecting Clients & Their Information

CPI's HIPAA Services & Work-Products

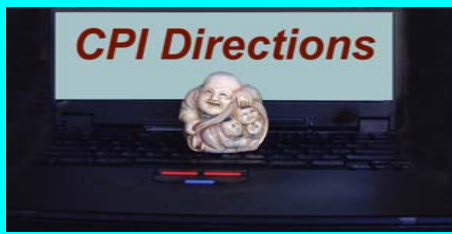
- Templates, checklists, and "roadmaps"
- Security & Privacy awareness training, seminars, workshops for all levels of the workforce
- Templates for the Notice of Privacy Practice, Acknowledgement & Authorization Forms, Business Associate Contracts, Trading Partner Agreements, Data Use Agreements
- Privacy & 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)



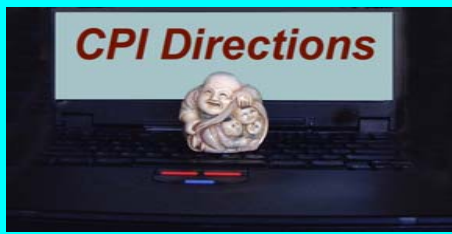
Protecting Clients & Their Information

Hip HIPAA Hippo PHI™

Posters & Workplace HIPAA Reminders

Featuring the Hip HIPAA Hippo™,
CPI Directions, Inc. makes
available a number of posters and
workplace HIPAA reminders that
continuously reinforce the HIPAA
“awareness” concepts important
for workforce compliance with the
Rules!



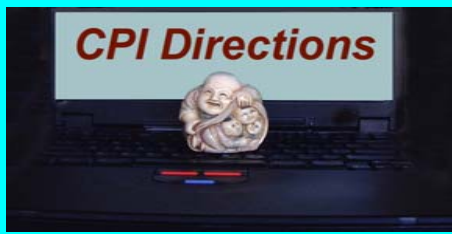


Protecting Clients & Their Information

Two HIPAA Realities:

“HIPAA is a marathon, not a 100-yard dash”

“HIPAA 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 15th Street, Suite 1922

New York, NY 10011

(212) 675-6367

MRosenblum@att.net

<http://www.CPIdirections.com>