

Protecting Clients & Their Information

Health Tech NY
Security & Privacy Rights Panel Overview
HIPAA Opportunities
(and Mandates)

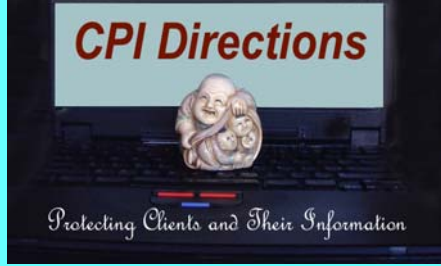
Held at the:

CUNY/BMCC Campus

199 Chambers Street

New York, NY

January 12, 2005



Protecting Clients & Their Information

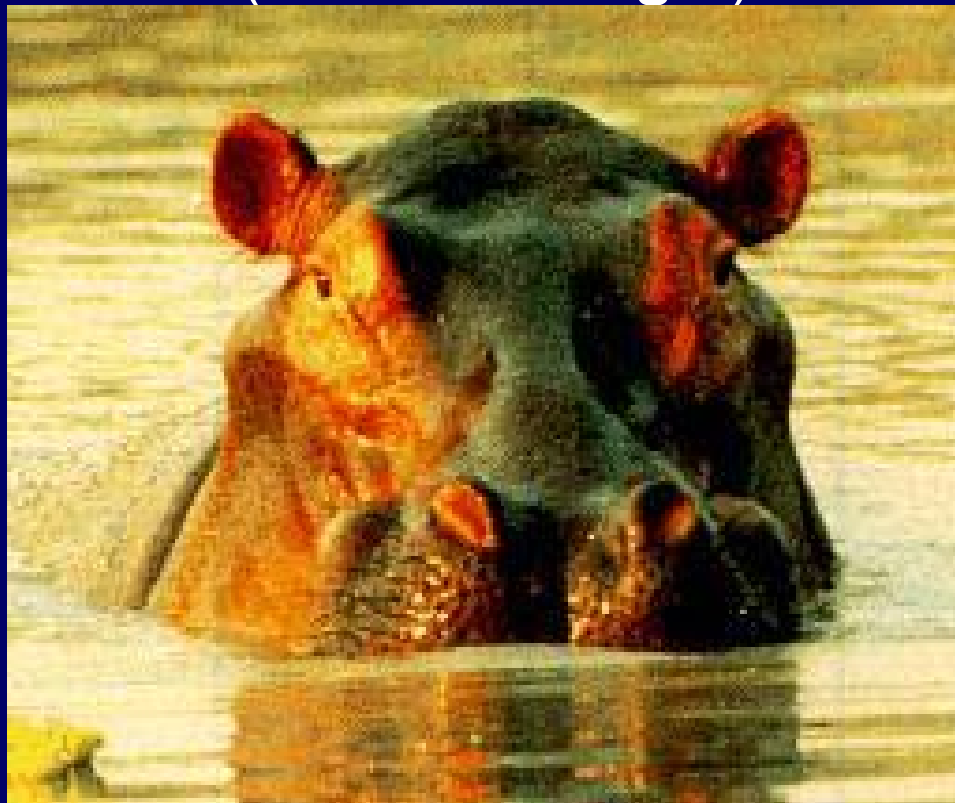
Panelists & Presentations

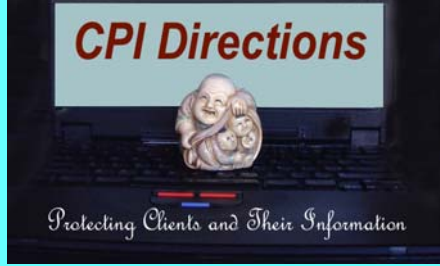
- **Dianne Faup, JD**, Advisor to the DHHS Office of HIPAA Standards, and Team Lead for HIPAA activities
- **Alicia Clay, PhD**, Deputy Chief, Computer Security Division, National Institute of Standards & Technology
- **Alan Goldberg, LL.M.**, Goulston & Storrs; Adjunct Professor, U. of Maryland School of Law, Suffolk University Law School (Boston); Past President of NHLA
- **Matt Rosenblum, MS**, Chief Operations Officer, CPI Directions, Inc.; Co-Chair, NYSIA Security & Privacy SIG



Protecting Clients & Their Information

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

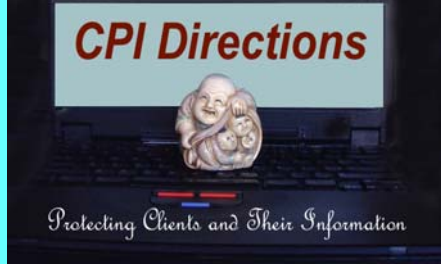




Protecting Clients & Their Information

Focus on 2 HIPAA Rule-Sets

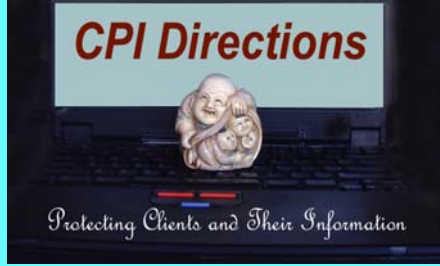
- **Privacy Standards**: provides that our ***PHI*** will be protected from ***bad*** uses and disclosures, and provides the patient/ client with certain ***controls*** and ***rights***
- **Security Standards**: aim is to provide administrative, technical, and physical-space safeguards



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

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

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	(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

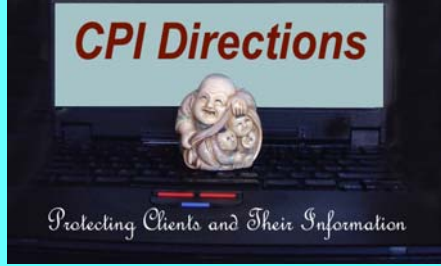
Physical Safeguards			
Standards	CFR Sections	Implementation Specifications (R)=Required (A)=Addressable	Required or Addressable
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation 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

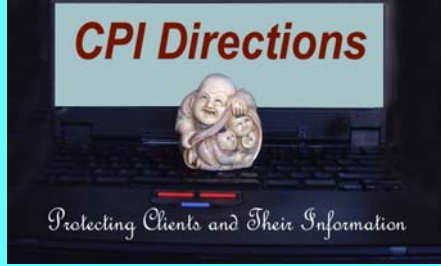
Standards	CFR Sections	Implementation Specifications	Required or Addressable
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption (data at rest)	(A)
Audit Controls	164.312(b)	Record and Examine Activity in Information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

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 over a decade



Protecting Clients & Their Information

“HIPAA is the catalyst that moves the healthcare industry from the paper- to the digital-age”

For additional information, please contact:

Matt Rosenblum

Chief Operations Officer

CPI Directions, Inc.

10 West 15th Street, Suite 1922

New York, NY 10011

(212) 675-6367

MRosenblum@att.net

<http://www.cpidirections.com>