

Preparing Your Laboratory for HIPAA Compliance



Tamtron Users Group April 2001

HIPAA's Components

- Administrative Simplification
 - Transaction Standards
 - EDI standards for claims, enrollment, authorizations
 - Effective Date: August 17, 2000
 - Compliance Date: October 16, 2002
 - Privacy Rules
 - Appropriate use of protected health information (PHI)
 - Patient's rights for access, corrections and disclosures
 - Effective Date: April 14, 2001
 - Compliance Date: April 14, 2003
 - Security Rules
 - Integrity, confidentiality and availability of PHI
 - Effective Date: TBD
 - Compliance Date: TBD




Are you covered by HIPAA?

- Covered Entities:
 - All Health Plans
 - All Health Clearinghouses
 - All providers who transmit health information electronically



What information is covered?

- The current privacy rules covers individually identifiable health information
 - Electronic
 - Written
 - Oral




HIPAA Compliance Steps

- Appoint a Privacy Officer
- Evaluate existing information disclosure practices
- Develop appropriate policies and procedures
- Develop and implement Chain of Trust Agreements
- Develop and conduct employee training
- Evaluate and possibly upgrade information systems and networks
- Conduct a self evaluation

Information Disclosure Practices

- CLIA supercedes HIPAA's requirements for reference labs (45 CFR § 164.524(1)(iii))
 - Does require that information be protected
 - Does require a Chain of Trust Agreement with Business Associates
 - Does not require information disclosure to patients (unless required by state law)
 - Does not require laboratories to establish patient initiated correction processes



Compliance for Information Disclosures

- Evaluate who has access to your protected health information
 - Billing service
 - Accountant
 - QA or inspection teams
 - Vendors
 - Consultants and contractors
 - Marketing organizations

Chain of Trust Agreement

- Agreement between a covered entity and an outside organization that has access to PHI
- Outlines requirements for a Business Associate's use and protection of PHI
- Describes sanctions and penalties if PHI is disclosed
- HIPAA has no authority over Business Associates



Polices and Procedures

- HIPAA Policies and Procedure Requirements
 - Integrated with your existing policies and procedures
 - Designed to reduce the risk of unapproved information disclosure
 - Must also support the availability, confidentiality and integrity of health information



Employee Training

- Initial Privacy and Security Training
 - Must be conducted at all organizational levels
 - Authorized disclosures
 - Unauthorized disclosures
 - Patient's rights to access and correction
 - Penalties and sanctions
- Organizations must provide periodic awareness training to all employees



IT Evaluation

- Applications and networks must support the availability, confidentiality and integrity of PHI
 - Evaluate network security
 - Application security and user authentication
 - Perform periodic system audits
 - Implement standard back up procedures
 - Implement disaster recovery procedures



Compliance Evaluation

- Compliance enforcement: HHS Office of Civil Rights
 - Compliance assistance
 - Scheduled and spot inspections
 - Evaluation of patient complaints
 - Fines
- Criminal Investigations: Justice Department



Resources

- Enclosed CD
 - Sample policy
 - Project plan
 - HIPAA preparation checklist
- OMI Web Site
 - Monthly updates
 - Links to other HIPAA resources
- Administrative Simplification Web Site
 - Full text of the regulations
 - FAQ
- HIPAA-REGS list server
 - Announcements and updates to all three rules



Questions?