# HIPAA
# Policy & Procedure Strategies

David J. Butler
&
Christopher E. Coleman

Strategic Management Systems, Inc.

**The HIPAA Colloquium
at Harvard University**

August 22, 2002

# Drafting Policies & Procedures

- Privacy regulation requires that activities be documented

- Procedures must be carried out in accordance with regulatory standards

- Thus, policies and procedures should be developed that are
  - 1. Practical and Operational for your Organization, and
  - 2. Compliant with Federal, State, and Local Regulations

# Drafting Policies & Procedures

- Who will manage Policy & Procedure process?
  - Establish a Project Manager
  - Establish a Team for drafting and review
- How do Policies & Procedures get approval?
  - Executive committee review and approval?
  - Board review and approval?
  - Departmental review and approval?
- Consider Time Management
  - Prioritize roll-out of policies from most challenging to already existing

# Policies vs. Procedures

- Many of the Policies will be standard, as required by the HIPAA regulations
- Many Procedures should be TAILORED to your organization's operations
- Both Policies & Procedures must be operational and practical for your organization
- IT MUST BE "DO-ABLE"

# Privacy Policy Categories

- Administrative Requirements
- Individual Rights
- Consents and Authorizations
- Uses and Disclosures - General PHI
- Uses and Disclosures - Specific Applications
- Uses and Disclosures - Authorization Not Required
- Forms

# Administrative Requirements

- Designating a Privacy Officer
- Non-retaliation Policy
- Sanctioning of Employees Policy
- Conducting Training

- Consider the following when drafting:
  - many may already exist within Compliance Program
  - leverage existing policies and procedures
  - insert amendments to cover privacy requirements
  - use as opportunity to audit and update existing policies and procedures

# Individual Rights

- Granting Access to Inspect and Obtain Copies
- Requesting Amendments to Information
- Requesting Accountings of Disclosures
- Confidential Communications

- Consider the following when drafting:
  - Who will receive and process requests from patients?
  - Who will supervise patient's inspections?
  - Who will review requests for amendments?
  - Will we charge for copies?  How much?

# Consents and Authorizations

- Consent for Use and Disclosure during Treatment, Payment, and Operations
- Authorization
  - initiated by Provider, OR
  - initiated by Patient

- Policies and Procedures should be consistent with Consent Form

- Identify Scenarios for when you would need to obtain Authorization

# Uses & Disclosures - General PHI

- Identifying Protected Health Information
- Verifying the Identity and Authority of Requestors
- Minimum Necessary Disclosures
- De-identifying PHI

- Consider the following when drafting:
  - Do we treat all health information as protected?
  - How should we classify employees for access to PHI?
  - Do we ever need to de-identify PHI?
  - Use professional judgement !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

# Uses and Disclosures - Specific Applications

- Marketing
- Fundraising
- Notice of Privacy Practices
- Others involved in the Patient’s Care

- Consider the following when drafting:
  - Do we conduct marketing or fundraising?
  - Who will provide the Notice of Privacy Practices?
  - How do we notify Next-of-Kin?

# Uses and Disclosures - Authorization Not Required

- Research review by IRB (in most cases)
- Subpoena
- Health oversight release (Medicare review)
- Public Health release (CDC, State)

- Consider the following when drafting:
  - identify which situations will not apply to your organization
  - identify which polices and procedures can be consolidated (i.e., lessen # of procedures)
  - leverage existing procedures for release of information (e.g., complying with subpoena)

# Security Policies & Procedures

- Less in number than Privacy
- Written documentation for all aspects of Security
  - Administrative
  - Physical
  - Technical

- Access Controls
- Data Integrity
- Disaster Recovery

- Documentation…..Documentation…..Documentation

# Forms

- Consent
- Authorization
- Request for Amendment
- Business Associate Contract
- Chain of Trust Agreements

- Consider the following when drafting:
  - forms should be reviewed by legal counsel
  - leverage procedures for existing forms (e.g., consent for treatment)
  - will need to identify business associates (many vendors)

# Coordinate Privacy and Security

PRIVACY

- Minimum Necessary
- De-identification
- Disclosure Accounting
- Breach of Privacy
- Business Associate
- Training

SECURITY

- Access Controls
- Personnel Clearance
- Access Auditing
- Security Breaches
- Chain of Trust
- Training

# Take Home Message

- Policies & Procedures MUST
  - **BE TAILORED TO YOUR OPERATIONS**
  - **COMPLY WITH REGULATORY STANDARDS**
  - **WORK PRACTICALLY FOR YOUR FACILITY**