Integrating HIPAA into Your Managed Care Compliance Program

The First National HIPAA Summit

October 16, 2000

Mark E. Lutes, Esq.
Epstein Becker & Green, P.C.
1227 25th Street, N.W., Suite 700
Washington, DC 20037
(202) 861-1824
mlutes@ebglaw.com

Start With What You Have

- Evaluate how the new requirements can be incorporated into the existing corporate compliance program.
- Policies and procedures for compliance program could be enhanced to accommodate HIPAA & GLBA requirements.
- Assess where internal clients stand in comparison with the proposed rule; current accreditation standards, GLBA, NAIC model reg. etc.

Compliance Integration

Seven Elements of a Corporate Compliance Program

- Policies and Procedures
- Assignment of Oversight Responsibilities
- Training and Education
- Lines of Communication
- Enforcement and Discipline
- Auditing and Monitoring
- Response and Corrective Action

HIPAA Security Requirements

- Administrative Procedures
- Assigned Security & Privacy Responsibility
- Training and Education
- Report Procedures; Event Reporting
- Sanctions
- Internal Audit
- Response Procedures; Testing & Revision

HIPAA Privacy Requirements

- Documentation of Policies and Procedures
- Designated Privacy Official
- Training
- Complaint Processing
- Sanctions
- Accounting for Disclosures
- Duty to Mitigate

Managed Care Risk Areas

Compliance

- Marketing and Enrollment
- Underutilization of Services
- Provider Relationships
- Reporting Obligations

HIPAA

- Confidentiality
- Integrity
- Availability

Hospital Risk Areas

- Billing and Coding
- Cost Reporting
- Stark/Anti-kickback
- EMTALA

- Confidentiality
- Integrity
- Availability

Policies and Procedures

- **Security Policies & Procedures**
  - "Documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data"
    - All aspects/elements of HIPAA compliance: administrative, physical and technological safeguards
    - Do not simply rely on your vendors
    - Know all authoritative sources

Policies and Procedures

Security Policies & Procedures, examples:

- Contingency
- Access and Authorization
- Encryption
- System Configuration Management
- Security Incident Handling
- Network Hook-Up
- Escalation Procedures for Security Incidents
- Third Party Network Connections Policy
- Training & Auditing

Policies and Procedures

- **Privacy Policies & Procedures**

  “A covered entity must document its policies and procedures for complying with the applicable requirements…”

  - Chain of Trust Agreements
  - Use and Disclosure practices that are tailored to organization
  - “Minimum Necessary” Guidelines
  - Individual Rights
  - Administrative Requirements
  - Policy Modifications

Assignment of Oversight Responsibilities

Security

- Documented assignment of security responsibility to an individual or an organization whose responsibilities include:
  - The use of security measures to protect data; and
  - The conduct of personnel in relation to protection of data

Privacy

- "The covered entity must designate a privacy official who is responsible for the development and implementation of the privacy policies and procedures for the entity."

Training and Education

Security

- Awareness Training
- Periodic Security Reminders
- User education concerning virus protection
- Monitoring and reporting
- Password management

Privacy

- Privacy Policies & Procedures
- All members of workforce
- Signed certification
- At least every 3 years and when policies change

Lines of Communication

Security

- “Formal, documented instructions for reporting security breaches, so that security violations are reported and handled promptly.”
- Event reporting--”a network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a specific task”

Privacy

- Health plans and providers “must develop and implement procedures under which an individual may file a complaint alleging that the covered entity failed to comply”
- Contact person
- Records of complaints and dispositions

Enforcement and Discipline

Security

- Sanction Policies and Procedures that notify employees, agents, and contractors of (1) civil or criminal penalties for misuse or misappropriation of health information, and (2) that violations may result in notification to law enforcement officials and regulatory, accreditation, and licensure organizations

Privacy

- "A covered entity must develop and apply when appropriate sanctions against members of its workplace [and business partners] who fail to comply with the policies and procedures of the covered entity or the requirements of this subpart..."

Auditing and Monitoring

Security

- Applications & Data Critically Analysis
- In-house review of the records of system activity (logins, file accesses, security incidents)
- Physical safeguards testing and revision
- Security Testing
- Audit Trail

Privacy

- Covered entities must be able to provide an accurate accounting of disclosures made by the entity as long as such information is maintained by the entity

Response and Corrective Action

Security

- Response Procedures--”documented formal rules or instructions for actions to be taken as a result of a security incident report”

Privacy

- Duty to Mitigate--”A covered entity must have procedures for mitigating, to the extent practicable, any deleterious effect of a use or disclosure of protected health information in violation of the [regulations].”

Getting Started

- Assess:
  - Corporate E-Strategies
  - IT structure
  - Policies & Procedures
- Assign:
  - Privacy and Security Task Forces
  - Individual Responsibilities
- Develop:
  - Information Flow Charts
  - Policies & Procedures
  - Job Descriptions
  - IT Solutions