HIPAA Implementation: Physician Case Study

Joel V. Brill, MD
The BHNP Group LLC

Mary L. Kuffner, JD
American Medical Association

The HIPAA Summit West
San Francisco, California
June 2001

HIPAA Implementation Planning Schedule

- Initiate the Effort
- Compliance Assessment
- Process Improvement
- Monitor and Audit Activities

HIPAA Implementation
Phase 1 - Initiation

- Become familiar with regulations
- Coordinate/analyze impact on other laws
- Take inventory of computer systems
- Take inventory of paper-based systems
- Set objectives and scope of compliance effort
- Determine priorities

HIPAA Implementation Phase 2 - Assessment

- Take inventory of all security and privacy policies and procedures related to HIPAA
- Promote awareness and initial staff training
- Appoint Privacy and Security Compliance Officers
- Identify gaps and weaknesses in office practices versus HIPAA regulations
- Formulate implementation budget

HIPAA Implementation Phase 3 - Improvement

- Revise and improve existing security and privacy policies
- Deploy new physical and technical safeguards of medical data
- Train workforce on enhancements
- Document training
- Roll-out new processes and systems

HIPAA Implementation
Phase 4 - Monitor / Audit

- Create reporting and documentation procedures
- Maintain HIPAA Compliance Officer
- Implement ongoing changes
- Continuously train employees
- Maintain vigilance to deal with threats
- Document, document, document

Are You Ready for HIPAA?

- October 2002 - Electronic Transaction Standards
- April 2003 - Privacy and Patient Confidentiality
- Final security rule expected anytime
- Just around the corner!
- Familiarize your staff and yourself with the HIPAA requirements

Are You Ready for HIPAA?

- Electronic Transaction Standards
  - Simplify the exchange of patient information
  - Improve security
  - Lower costs
  - Lower error rates
  - Potential reduction in receivables

Are You Ready for HIPAA?

- Electronic Transaction Standards
  - Translate information to HIPAA standards
  - System upgrades
  - Relationships with clearinghouses
  - Education of staff
  - Education of billing / coding agencies

Are You Ready for HIPAA?

- Privacy of Patient Health Information
  - Keep information confidential and secure
  - Cornerstone of doctor-patient relationship
  - Changes daily activities in office
  - Requires tracking of consents and disclosures
  - Requires ongoing training

Are You Ready for HIPAA?

- Security / safeguards
  - Administrative procedures
  - Physical safeguards (office and equipment)
  - Technical security services (Software solutions - additional cost?)
  - Technical security mechanisms (network communication - need encryption?)
  - Business associates must handle patient information in a compliant manner

Privacy Standards

- Use and disclosure of health information
- Minimum necessary provisions
- Patient rights to copy and amend records
- Administrative requirements
- Business associate contracts
- Regulatory mandates

Privacy - Where to Start?

- Inventory/Evaluate
- Privacy Officer
- Analyze information Flow
- Gap Analysis
- Budget
- Develop Materials
- Train Employees
- Document

Privacy - Where to Start?

- Inventory
  - Current consents
  - Current signage
  - Current message systems
  - All policies and procedures
- Compliance questionnaire
- Evaluate/compare final rule and “more stringent” state laws

“Dr. Privacy Practice”

- Create an awareness in your practice
- Involve staff in the compliance process
- “Protecting patient data is the right thing to do”.
  - Moral imperative
  - Business imperative
  - Legal imperative

Privacy - Medical Records

- Evaluate medical record safeguards
  - Technical mechanisms
  - Physical mechanisms
- Contact software and hardware vendors

Be a Businessman!

- Initial compliance activities
  - Develop a budget
  - Develop a calendar
- Designate a Privacy Officer

Privacy Officer

- Coordinates the development and modification of the practice's privacy policies and employment handbooks.
- Coordinates education of all staff.
- Oversees the development and implementation of the practice's compliance strategy.

Privacy Officer

- Coordinates efforts with:
  - billing
  - information technology
  - medical staff
  - workforce
- Handles the day-to-day issues

Successful Privacy Officer

- Don’t assign this task to the busiest person in the office.
- Pick the right person:
  - detail-oriented
  - intelligent
  - patient
  - good manager
  - has authority

Privacy Officer and You

- Provide support
- Provide adequate time
- Provide adequate resources

Patient Information

- Analyze / flow chart how your practice handles patient information.
- Develop tracking mechanisms
- Update practice forms
- Update informational materials

Gap Analysis

- Assessment
- Evaluation
- Address the “gaps” found in your initial analysis
- Develop a detailed implementation plan
- Establish interim milestones

Be A Businessman!

- Analyze the overall impact of HIPAA compliance on your practice
  - Financial
  - Non-financial
- Develop a budget
- Set appropriate goals

Be A Businessman!

- HHS estimates cost of compliance $4000 per physician practice
- Estimate is probably too low.
- Costs vary tremendously, depends upon:
  - size of physician practice
  - equipment
  - current privacy practices
  - business associates, etc.

Business Associates

- List all contracts and relationships
- Develop a “Business Associate Contract”
- Let vendors know that you are concerned about privacy.

Develop Materials

- Develop “Notice of Privacy Practices”.
- Design “Consent for Release of Information” forms.
- Update “Authorization for Use and/or Disclosure of Information” forms.

Develop Materials

- Develop a training program and form to document training
- Create/update procedures and forms for
  - patient rights to access, amend and obtain an accounting of disclosures
  - patient complaints
  - employee sanctions

Notice of Privacy Practices

- Addresses your *potential* information practices
- Provide on date of first service after compliance date (direct treatment relationship)
- Post prominently in office
- Post on website
- Make available to any upon request

Consent for Release of Information

- For treatment, payment and operations
- Separate from other consents
- Written in plain language
- Refers patient to Notice
- Provides the individual with the opportunity to request restrictions
- Can revoke at any time
- Separately signed and dated

Authorization for Disclosure of Information

- For purposes other than treatment, payment, health care operations
- Specify what is to be released
- Specify what it is going to be used for
- Voluntary
- Has date of expiration
- Can revoke at any time

Create PHI “firewalls”

- Establish an “accounting” procedure to track uses and releases of PHI
- Limit access to those employees that require it. (“Minimum necessary”)

Create PHI "firewalls"

- "Minimum necessary" use:
  - must identify persons or classes of persons who need access to PHI to carry out their duties
  - must identify the categories of PHI for each person or class of persons

Create PHI "firewalls"

- "Minimum necessary" disclosures:
  - must implement policies and procedures for routine and recurring disclosures
  - must develop criteria for non-routine disclosures that are designed to limit PHI disclosed
  - case by case review of non-routine requests

Training Program

- All workforce employees
  - Physicians
  - Other health professionals
  - Volunteers
  - Students
  - Trainees
  - Part-time / registry staff

Maintain Documentation

- All necessary policies and procedures
- Ensure any changes to policies and procedures are not implemented until documented and appropriate persons are notified
- Maintain documentation for six years, unless a longer period applies

Maintain Documentation

- Business Associate contracts
- Consent forms
- Authorization forms
- Notices and amended notices
- Training of employees
- Patient complaints and their disposition

Privacy Issues

- Sign-in Sheets
- Fax transmissions
- Answering service
- Transcription service
- Patient reminder notices

Privacy Issues

- Prescriptions
- E-mail
- Computer guru
- Curbside consultations

Privacy Issues - Records

- Patient
- Other healthcare providers
- Insurers
- Managed care intermediaries
- Disease management vendors
- Pharmaceutical companies
- Hospitals

Privacy - Monitor / Audit

- Review state requirements
- Create a schedule for period review of privacy procedures
- Monitor laws and standards and implement changes in regulations

Privacy - Uncertainties

- Guidance to be issued
  - “to clarify some of the confusion regarding the impact this rule might have on health care delivery and access” - HHS Secretary, April 12, 2001
  - Will not have same force and effect as the regulation

Privacy - Uncertainties

- Modifications may be issued
  - “will consider any necessary modifications that will ensure the quality of care does not suffer inadvertently from this rule” - HHS Secretary, 4/12/2001
  - Not likely be issued before 4/14/2002
  - Might address prior consent, minimum necessary standards, and parental access to minors’ records

Security - Where to Start?

- Inventory/Evaluate
- Security Officer
- Gap Analysis
- Budget
- Develop Materials
- Train Employees
- Certify
- Document

Security - Privacy Overlap

- The privacy rule requires:
  - "appropriate administrative, technical, and physical safeguards" to protect the privacy of PHI
  - to "reasonably safeguard PHI from intentional or unintentional uses or disclosures" that violate the rule
- The security rule requires:
  - administrative, technical and physical measures to guard the integrity, confidentiality and availability of electronic data

Security - Privacy Overlap

- Coordinating gap analysis, assessments and implementation will create efficiencies:
  - policies
  - administrative procedures
  - budget
  - staff training and awareness
  - vendor and third party contracts

Security - Where to Start?

- Inventory - where are all records?
- Evaluate current physical and technical safeguards
- Assess potential risks and vulnerabilities
- Evaluate current policies and procedures
- Staff awareness
- Contact vendors
- Budget

Security - Administrative Procedures

- Certification
  - technical evaluation of extent computer systems or network design and implementation meet security requirements
  - internally or external accrediting agency

Security - Administrative Procedures

- Chain of trust partner agreement
  - Review contracts with third parties and vendors with whom you will exchange electronic (*or paper* ?) PHI
- Overlap with privacy:
  - “business associate” contracts

Security - Administrative Procedures

- Review / create contingency plans to respond to emergencies that must include:
  - Applications and data criticality analysis
  - Data backup plan
  - Disaster recovery plan
  - Plan for “emergency mode” operation
  - Testing and revision procedures

Security - Administrative Procedures

- Medical records processing - need policies and procedures for routine and non-routine:
  - receipt
  - manipulation
  - storage
  - dissemination
  - transmission
  - disposal

Security - Administrative Procedures

- Overlap with privacy:
  - “minimum necessary” policy for routine and non-routine disclosures
  - accounting of disclosures
  - determination of “designated record set”
  - records retention requirement

Security - Administrative Procedures

- Control of access to PHI - review/create formal policies and procedures granting different levels of access to PHI
- Personnel security - need policies/procedures for authorization, supervision and clearance
- Overlap with privacy:
  - “minimum necessary” use
  - sanction policies

Security - Administrative Procedures

- Internal audit - all systems (and paper?) activity
  - log-in/out, file access, disclosures, security leaks
- Overlap with privacy:
  - accounting for disclosures
  - “minimum necessary” use policies
  - policies for sanctions

Security - Administrative Procedures

- Personnel security - need policies/procedures for authorization, supervision and clearance
- Overlap with privacy:
  - “minimum necessary” use
  - sanction policies

Security - Administrative Procedures

- Security configuration management
  - procedures for security of information must be coordinated and integrated with each other
  - create a coherent system
    - comprehensive documentation
    - hardware/software installation and maintenance review
    - virus checking

Security - Administrative Procedures

- Security incident and management
  - reporting security breaches
  - risk management - prevention, detection
  - sanctions
- Overlap with privacy:
  - accounting for disclosures
  - mitigation responsibility
  - policies for sanctions

Security - Administrative Procedures

- Termination procedures
  - change locks
  - removal from access lists, accounts
  - key return
- Overlap with privacy:
  - mitigation responsibility
  - policies for sanctions

Security - Administrative Procedures

- Security training
  - awareness
  - periodic reminders
  - education
- Overlap with privacy:
  - combine training
  - coordinate/combine policies for sanctions

Security - Physical Safeguards

- Security Officer - management and supervision of:
  - use of security measures
  - conduct of personnel
- Overlap with privacy:
  - should collaborate with privacy officer
  - may be same person in small practice

Security - Physical Safeguards

- Media controls
  - formal, documented policies and procedures governing receipt and removal of hardware and software in and out of facility
    - backup copies
    - accountability
    - disposal

Security - Physical Safeguards

- Physical access controls (limited/appropriate)
  - disaster/emergency
  - equipment control/facility security
  - verifying access authorizations/“need-to-know”
- Overlap with privacy:
  - verification
  - minimum necessary
  - accounting for disclosures

Security - Physical Safeguards

- Work station controls
  - documentation of proper functions
  - physical attributes
  - secure work station
- Overlap with privacy:
  - minimum necessary

Technical Security Services

- Access controls
  - procedures for emergency access, and
  - context-based,
  - role-based, or
  - user-based access
  - encryption is optional
- Overlap with privacy:
  - “minimum necessary” use

Technical Security Services

- Audit controls
  - to record and examine system activity
- Overlap with privacy:
  - audit trails
  - accounting of disclosures
  - sanctions

Technical Security Services

- Authorization controls
  - consent for use/disclosure
  - role based or user based access
- Overlap with privacy:
  - minimum necessary
  - accounting of disclosures
  - sanctions

Technical Security Services

- Authentication of data
  - message authentication/digital signature
- Authentication of entities
  - automatic logoff
  - unique user ID
- Overlap with privacy:
  - verification

Technical Security Mechanisms

- Transmission of data over networks requires deployment of network controls
  - security standards must include:
    - integrity controls
    - message authentication (software?)
    - access controls or encryption
  - technical security mechanisms must include:
    - alarm
    - audit trail
    - entity authentication
    - event reporting

Security - Uncertainties

- What's covered? Electronic? Paper? Oral?
- Audit trails
- Certification
- Other definitions
  - business associate vs. Chain of trust partner agreement

Electronic Signature

- Expected to be removed from security rule as a separate final rule
- No electronic signatures currently required

Other HIPAA Rules

- Unique Health Identifiers
  - employer
  - health plan
  - health care providers
  - individual
- Claims Attachments
- Enforcement

Other HIPAA Info

- http://pweb.netcom.com/~ottx4/HIPAA.htm
- http://aspe.hhs.gov/admnsimp/
- http://www.hipaadvisory.com/

Ongoing Maintenance

- Train
- Educate
- Communicate
- Update
- Document

Questions?

The BHNP Group LLC

Joel Brill, MD (602) 418-8744

joel.brill@gte.net

Rick Nevins, MD (602) 430-4406

nevins2@aol.com