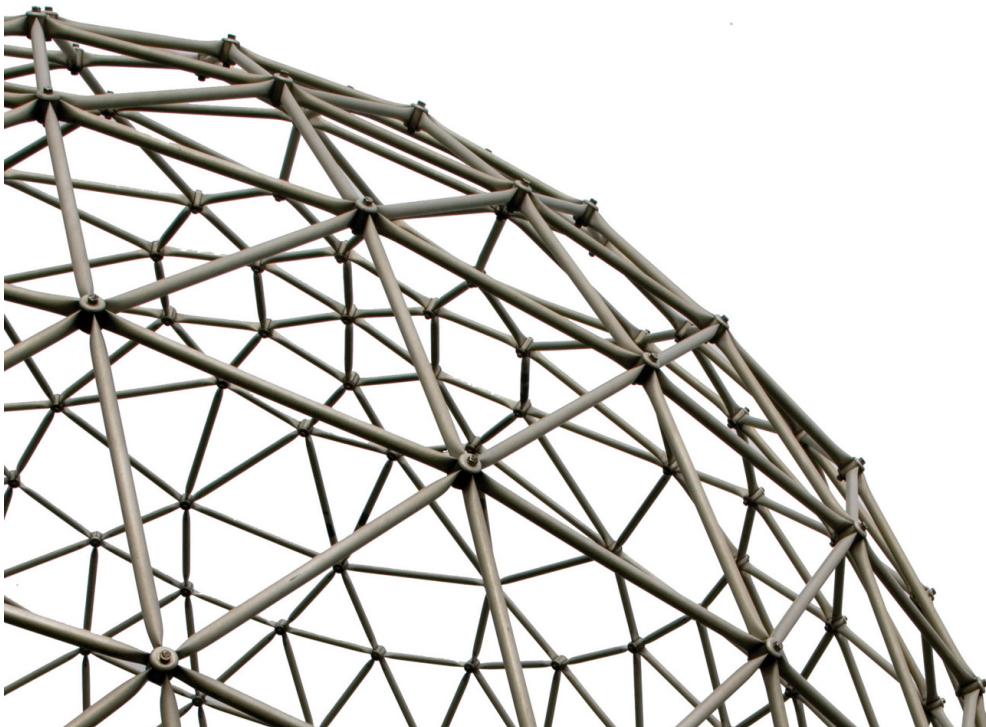# Regulation of Healthcare Information Technology

Avoiding HIPAA's Pitfalls

Advice for Auditors

Bill Pankey
SF ISACA

November 18, 2008

Agenda

Session Agenda

1. **Historical context**
   - Healthcare transactions
   - Healthcare's control environment

2. **Major provisions of the HIPAA rules**
   - What's important
   - What's hard and why
   - Where things may have gone wrong

3. **HIPAA Compliance audits**
4. **CMS complaint driven audit process**
5. **What's ahead**
   - HIPAA2
   - NHIN
   - Attachments

Healthcare's Reimbursement Transactions

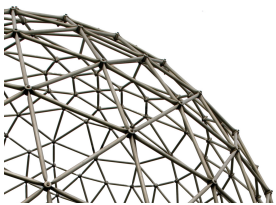Administrative workflows around a set of complicated transactions

- *Employer:* **Enrolment of member into health plan**
- *Provider:* **Verification of patient's insurance eligibility**
- *Provider:* **Request for authorization or referral~ specialized treatment \diagnosis, hospitals stay, etc**
- *Health plan:* **request for additional information**
- *Provider:* **claim for reimbursement**
- *Health plan:* **request for additional information**
- *Health plan:* **coordination of benefits**
- *Provider:* **request for status of claim**
- *Health plan:* **EOB and funds transfer**
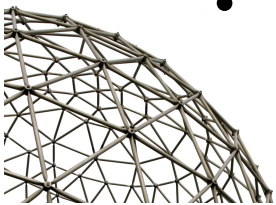
Reimbursement Transactions circa 1996

High transaction costs either to negotiate EDI format or process paper.

- **40% of healthcare cost attributed to 'administration'**

- **Most reimbursement transactions conducted through paper or non-standard electronic transactions**
  - Healthcare's small / medium enterprise problem
    - 80% of institutional claims via multiple EDI formats ~ 20% of volume
    - Very little electronic submission by individual practitioners ~80% of volume
  - Use of a few standard formats for paper claims

- **1993 WEDI study estimated annual industry savings of $43B if industry broadly implemented EDI for insurance related transactions**

IT Control Environment circa 1996

High trust of credentialed workforce; significant distrust of business partners

- **Reimbursement contingent on the health plans' determination of the medical necessity of treatment**
  - Plans would typically request 'the entire medical' record to make payment decisions
  - Providers resistance jeopardized reimbursement

- **Within provider organizations, security assumed very significant levels of 'trust'**
  - Medicine's culture of privacy
  - Significant scrutiny of staff during credentialing process

- **Health plan identified significant proprietary value in various claim databases**
  - Denied consumer confidentiality interest
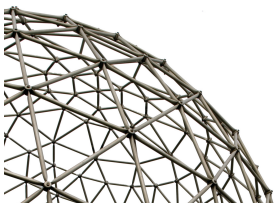
Reimbursement politics circa 1996

Simplification costs and benefits are often misaligned: provider cost – plan benefit

- **Provider (i.e. physician) resistance to an EDI mandate**
    - Interpreted EDI as a ploy to get physicians to bear the plan's data entry costs
    - Skeptical of assertions that EDI would lead to more timely reimbursement
    - Distrust of health plan use of electronic information
        - Evidence that plans applied stricter standards to electronic claims than claims submitted on paper

- **Medicare & commercial health plan concerns over provider's false claims & 'gaming the system'**

- **Privacy advocates distrust of health plan / institutional use of patient data**
    - Sales of large databases
    - Use of claims data to make adverse decisions

- **1996 IOM 'For the Record' study**
    - Anecdotal study of the industry's poor information practices
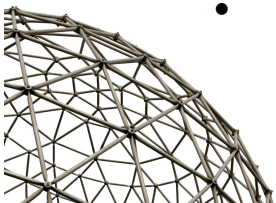
1996 HIPAA Law

## Administration Simplification provisions created an EDI mandate

- **Health Information Portability & Accountability Act | Administrative Simplification**
  - Public Law 104-191 | SubTitle F
  - http://aspe.hhs.gov/admnsimp/pl104191.htmhttp://aspe.hhs.gov/admnsimp/pl104191.htm

- **Required HHS to select and promulgate standards for:**
  - Transaction format and content
  - Healthcare code sets
    - Diagnosis, treatments, drugs, labs
  - Identifiers
    - Providers, health plans, purchasers, patients
  - Electronic signature
  - Information security
  - Health information privacy and practice

- **Mandated industry's exclusive use of standard transactions**

- **Mandated restrictions over use of personal health information**

- **Mandated industry maintain 'reasonable & appropriate' [security] safeguards**
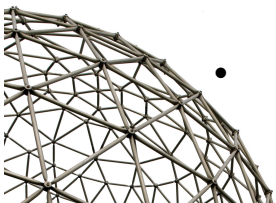
After 12 Years

HIPAA remains a work in progress

- **Transaction mandates have not created significant cost savings**
  - Transaction standards remain incomplete.
  - ~~Use of standard formats 'required' but *officially* 'no enforcement action at this time'~~
  - Congressional action has blocked creation of national patient identifiers
  - Fundamental EDI cost / benefit equation has not changed
    - Some EDI cost savings; but reimbursement workflows not changed significantly by HIPAA standards
    - HIPAA did not address the healthcare EDI SME problem

- **Industry privacy and security practices have substantially improved, but with persistent compliance and cost issues**
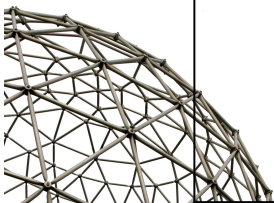
Transaction Formats & Code Sets

Major effect of transaction rule has been to restrict EDI activity to a few formats and code sets

- **Transactions and Code Sets Rule**
  http://www.cms.hhs.gov/TransactionCodeSetsStands/
  02_TransactionsandCodeSetsRegulations.asp

- **Administrative Simplification?**
  - Mandate for the use of X12N formats that were built for the [early] 90s
    - Terse format designed to minimize 'kilo-character' transmission charges
    - Context dependency of format makes application integration difficult
  - Mandate use of increasingly complicated code sets
    - 170k ICD-10 diagnostic codes 10 times the number of codes in ICD-9
    - 70k codes for LOINC codes for labs & other measures
  - Little done to simplify the content of the re-imbursement transactions
    - X12.837 Professional claims ~ 1000 page standard, *but …*
    - Also must use health plan specific implementation guides
  - Golden rule of EDI still applies post HIPAA
    Better to be a receiver than a sender
    - Most of the industry still relies upon EAI / translation software
    - Most of the industry relies upon 3rd party claims 'clearinghouse' services to manage transmission and translation
    - Some transactions still not widely adopted in electronic format so lifecycle cannot be fully automated

Transaction Rules- Auditor Guidance

Reimbursement transaction process is very specialized and very high risk

- **Characteristic coding errors expose provider organizations to assertions of 'fraud & abuse'**
  - Risk of prosecution under the Federal False Claims Act
    - *Fraud*: intentional false claim, e.g.
      - Up-coding: Billing for more expensive services than what was provided
      - Billing for service provided by unqualified person
    - *Abuse*: practices leading to unnecessary cost to Medicare / Medicaid or medically unnecessary services, e.g.
      - Unbundling: Billing separately for globally covered services
      - Kickbacks to patients
  - Coding Risk dwarfs any concerns about transactions formats
    - Consistent target of Provider Internal Audit
    - Characteristic industry practice violates the letter of False Claims Act

- **HIPAA exacerbates risk of coding error**
  - Expected mandate for use of ICD-10
    - 10x precision / complexity of ICD-9
      - 1100 codes for angioplasty; 45 codes to describe sprained ankle
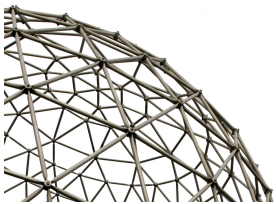
Transaction Controls

Internal audit focuses on utilization and coding of disease and treatment

- Transaction formatting performed thru EAI
  - Plans will reject in-appropriately formatted transactions
  - Well formed transaction rules built into popular EAI engines
  - ClarEDI has service to validate transactions

- Computer assisted medical coding
  - Some enterprise business rules / lexicon built-in

- Medical coding subject of internal audit activity
  - "scope" audits manually validate coding for a sample of procedures.
  - Statistical studies to detect anomalies for detailed investigation
    - Alert where more than expected types and numbers of procedures, diagnosis

- SOD: physicians describe conditions and purpose of procedures, procedures documented by 'patient accounting' systems; coded by technicians
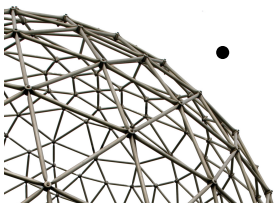
Privacy Rule

Mandate based on OECD Fair Information practices

- **HIPAA Final Privacy Rule**
  - http://www.hhs.gov/ocr/hipaa/finalreg.html

- **Consumer / patient rights**
  - Notice of information practices
  - Right to inspect; right to 'amend'
  - Right to an accounting of disclosures

- **Usage restricted to business purpose**
  - Allows use / transmission of only the 'minimum necessary' information
  - Treatment, payment and / or health operations (aka TPO)

- **Limited disclosure for other than TPO**
  - With patient authorization
  - Where required by law
  - When the information has been de-identified

Privacy Rule ~ Auditor Guidance

Rules apply to information in any format: electronic, paper and / or verbal

- **Identify uses and disclosure of personal health information**
  - Map 'phi flows'
    - Where is the information maintained
    - Who uses it
    - For what purpose

- **Examine basis for any use of the patient info**
  - What is the TPO purpose of the use? If no TPO purpose, then
    - Did the patient authorize the use?
    - Is the use or disclosure required by law?
    - Has the data been 'de-identified'

- **Examine the accounting of disclosures**
  - Record keeping related to information released to 3rd parties
    - Target, patient identity, disclosed information, basis of disclosure
    - Patient authorization

- **Records regarding publication of 'notice of privacy practice'**
  - Review adequacy of notice
  - Proof of distribution
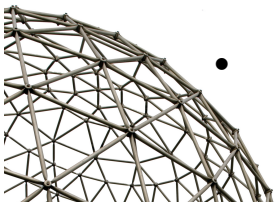
Security Rule

Standard contains sweeping but ambiguous mandate to engage in security related activities

- **Final Security Rule**
  - http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf

- **Requires healthcare companies to "ensure the confidentiality, integrity and availability' of electronic health information**
  - Allows use of any measures to comply with further mandates

- **"Implement security measures sufficient to reduce risks and vulnerabilities to a _reasonable and appropriate_ level."**
  - Parrots the congressional language of the HIPAA law
  - Regulator resists call to provide further guidance ala FFEIC IT Handbook
  - HHS view is that further definition can only come from administrative Law courts
  - Unlikely that there _can_ be clarity from that source

- **Required Level of care varies with organizational characteristic**
  - Size and complexity
  - Technical infrastructure, hardware and software security capabilities
  - Cost of security measures … but cost does not excuse failures

Security Rule

Requires <u>defined</u> policy & procedures for a variety of security activities

- **Administrative**
  – Security Management
  – Personnel security
  – Access management
  – Security awareness & training
  – Incident response procedures
  – Contingency planning
  – Compliance evaluation
  – Service providers

- **Physical**
  – Facility access control
  – Workstation standardization and security
  – Device and media controls

- **Technical**
  – Access control
  – Audit controls
  – Integrity
  – Source and user Authentication
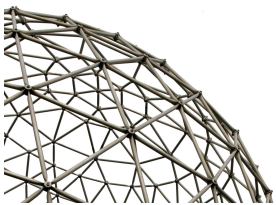 – Transmission

Additional activities defined for each of the above categories

Some Security Rule Challenges

Application infrastructure, medical practice, and rule ambiguity make some provisions more difficult than others

- Security Management | risk analysis
- Information access management
- Security incident procedures
- Device and media control
- 3rd party service providers

Risk Analysis

Conduct an <u>accurate and thorough</u> assessment of the potential risk and vulnerabilities to the confidentiality, integrity and vulnerability of electronic health information held by the covered entity

- **Security rule does not define 'risk'**
  - What is the standard of accuracy in estimating the occurrence and cost of future CIA compromise?
  - What is the measure of thoroughness of risk analysis?
  - From whose perspective is the risk analysis conducted?

- **Security industry lacks good risk assessment models for health scenarios**,
  - Confidentiality nominally has high values but the holder has no proprietary interest & uncertain liability
  - Highly variable consequence of integrity errors (unlike financial)
  - Availability requirements are context dependent
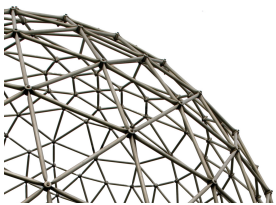
Risk Analysis

Little agreement how to conduct the required risk analysis

- **Most large organizations have adopted a 'bottom up', application focused approach**
  - Use some variant of 'expected loss' formula
  - Use results of 'control' assessment to define vulnerability / threat
  - Coarse estimate of impact / cost of compromise

- **Encounter significant difficulty when reporting risk at enterprise levels**
  - 100s of enterprise applications X (100 or 500 'controls') X (10 or 100 threats)

- **Industry well advised to lesson of AS5 and adopt a 'top down' approach to HIPAA risk assessment (imho)**

Information Access Management

Implement policies and procedures for authorizing access to ePHI that are consistent with [minimum use provisions of Privacy Rule] … policy and procedures for granting access … establish, document, review and modify user's right of access to workstation, transaction, program or process.
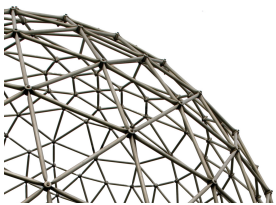
- **HIPAA effectively requires role based access control**
  - Access has to be authorized and supervised
  - Authorization is bound to requirements of workflow in which individual participates

- **HIPAA does not define required level of granularity of access control**
  - Industry confusion of role types leads to overly complex role models
    - Typically either 3, 7 or 1000s of roles

- **Confusion of data 'ownership'**
  - Practitioner workforce role maybe transient but information access requirements persist after workforce separation
    - Continuity of care requirements.
    - Information to support reimbursement
    - Quality reviews & Litigation

Information Access Management

HIPAA exacerbates access control issues

- **Vendor applications implement idiosyncratic RBAC models**
  - Motivated by desire for "HIPAA compliant" system
  - Potentially N+1 access control schemes

- **Rights defined relative to identity of patient**
  - 'Break glass' in emergency situation
  - Sharing patients / covering for another physician

- **HIPAA does not recognize requirements to persist rights for persons no longer in workforce**
  - Every hospital has physicians with access rights but who no longer practice at the hospital [guaranteed]

- **Some benefits in an emerging Industry standard [HL7] RBAC scheme**
  - Functional roles defined relative to participation in characteristic healthcare workflows
  - Rights defined relative to workflow requirements
  - Associate individuals with functional roles

Security Incident Procedures

Policy & procedures to address security incidents …identify and respond to suspected or known security incidents; mitigate harmful effects … document incidents and their outcomes

- **HIPAA includes overly broad definition of "security incident"**
  - *Attempted or successful unauthorized use, disclosure, modification or destruction of information or interference with system operation*
  - Requirement to document even routine reconnaissance scans
  - Auditor is unlikely to find a consolidated IRT function, eg network intrusion addressed with distinct procedures from say misaddressing

- **HIPAA does not provide guidance regarding the acceptable level of mitigation**
  - Rule implies that something should always be done, but what?
  - Harmful effects of confidentiality breach are generally uncertain … wait until the effect is certain?
  - Notification only shifts mitigation burden to information subject, is that enough?

Device and Media Control

Implement policies an procedures that govern the receipt and removal of hardware and electronic media that contain ePHI and out of a facility and the movement of these items … maintain a record of the movements … remove ePHI before reuse

- **Some special challenges in tracking media containing ePHI**
  - Floppy disk and other portable media provide the only way to capture data in some medical devices, such as EKG
  - Biomed devices maintain histories, travel with patients, except when they do not
  - [Independent] Practitioners may use flash drive and other media to copy patient records for use on the practitioner's systems

- **Standard does not require that information be securely stored on the media**

3rd Party Service Providers

Contract between covered entity and business associate [service provider] must provide that the business associate will …. reasonably and appropriately protect … ensure that their agents will reasonably and appropriately … report to the covered entity any security incident
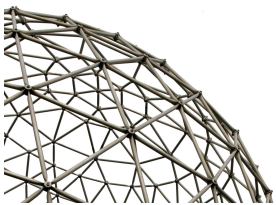
- **Business associate provisions multiply the ambiguity of the Standard 3-fold**
  - Must define 'reasonable and appropriate' relative to the security / threat environment of service provider
  - Must define 'reasonable and appropriate' relative to the security / threat environment of the service provider's service providers

- **Must now process and respond to the incident reports of service providers**
  - Require policy and procedures to appropriately respond to such reports

- **Obligation to obtain assurance**
  - Required level of assurance is left to covered entity
  - Service providers typically are small business unable to indemnify and do not have resources to respond to an intrusive audit

Security Rule Compliance

Most important activity is to relate identified risks to mitigation activity and to document security policy and procedure,

- Rule generally calls for *safeguards* rather than *controls*
  - 'protect' rather than 'prevent'

- Rule requires that procedures be 'effective' with only a weak audit requirement to ensure that effectiveness
  - No certification requirement

- Standard calibrates required level of effort on covered entity's assessment of its risk
  - Is it the risk assessment inadequate? Or is the mitigation activity inadequate? i.e., what provision of the Rule is being violated?

- Unambiguous requirement to define and implement specified 'policy and procedures'
  - Risk management plan points to the P&P that mitigates each identified risk.

NIST HIPAA Guidance

Secretary of Commerce and NIST have a statutory role vis a vis the HIPAA Security Standard.

- ## NIST SP 800-66
  - 'An Introductory resource Guide for Implementing The Health Insurance Portability and Accountability Act (HIPAA) Security Rule"'
  - Revision 1, October 2008
  - http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

- ## Provides basis for a HIPAA compliance assessment. For each provision of the Standard:
  - Identifies key activities
  - Assessment question for each key activity

Enforcement of HIPAA

Congress allocated to HHS responsibility for HIPAA enforcement but no funds ~ is HIPAA 'toothless' ?

- **HIPAA Public Law included nominal penalties for non-compliance**

- **HHS has adopted a 'complaint driven' voluntary compliance process**
  - OIG investigates consumer \ whistleblower complaint
  - Covered entity disputes or responds with correction plan
  - Egregious cases of willful non-compliance referred to Justice for prosecution

- **Very few complaints related to security rule violations**
  - Not surprising as security rule regards process and not outcomes. Visible outcome of security rule violation is a privacy rule one.

- HHS OIG review of CMS' Security Rule Oversight
  - http://www.oig.hhs.gov/oas/reports/region4/40705064.pdf

- Providence Health's consent resolution with CMS following compliant and finding of non-compliance
 - http://www.hhs.gov/ocr/privacy/enforcement/resolution.html
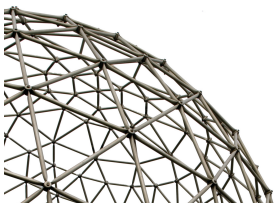
HHS Compliance Audit Document Request

PWC under contract to perform 20 compliance audits … in response to complaints about security rule violations.

http://www.cms.hhs.gov/Enforcement/Downloads/InformationRequestforComplianceReviews.pdf

- Policy & Procedure addressing:
  - Prevention, detection, containment & correction of security violations (incident handling)
  - Detecting, reporting & responding to security incidents (?)
  - Employee background checks
  - Authentication mechanisms
  - Individuals & contractors with ePHI access
  - Monitoring (authorized & unauthorized) system use
  - Encryption & decryption of PHI
  - Use of wireless
  - Sanctions for workforce members violating [security] policy
  - Termination of system access
  - Software used to control access to Internet
  - Emergency Access

- Other evidence:
  - Entity wide security plan
  - Risk Analysis
  - Risk Management Plan
  - Secuirty violation monitoring reports
  - Vulnerability scan plans
    - Recent results
  - Network penetration policy & procedure
    - Recent results
  - List of all user accounts w/ ePHI access
  - Configuration standards including patch management
  - Disaster recovery plan
  - Disaster recovery test plans & results
  - BIA
  - List of primary domain controllers
  - Inventory log of media and devices containing ePHI
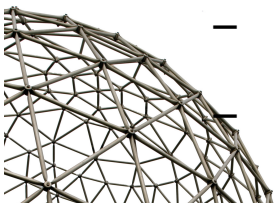
Enforcement Stats

Congress allocated to HHS responsibility for HIPAA enforcement but no enforcement funds ~ is HIPAA 'toothless' ?

- 40,000 Complaints (since April 2003)
    - ~ 30K outside scope of HIPAA
    - ~ 10K investigated by HHS
        - ~ 7500 corrective action; primarily in a change in target's policy and \ or procedures
        - ~ 2500 found no fault
        - ~ 260 referred to CMS \ Medicare (for security rule violation)
    - ~ To date, no civil penalty levied by HHS
    - ~ 440 cases referred to Justice for criminal prosecution
        - ~ No evidence of any criminal prosecution spurred by complaint

- Most common complaints:
    - Impermissible uses and disclosures of PHI
    - Lack of safeguards of PHI;
    - Lack of patient access to their PHI;
    - Uses or disclosures of more than the Minimum Necessary PHI; and
    - Lack of or invalid authorizations for uses and disclosures of PHI

- More Statistics
    - http://www.melamedia.com/HIPAA.Stats.home.html
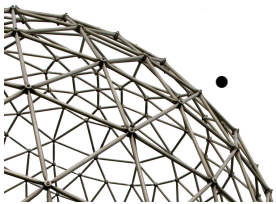
California Law supersedes HIPAA

California medical information privacy law provides significantly greater protection than does actual or proposed Federal law and regulation.

- Medical Records Confidentiality Act
  - http://www.oispp.ca.gov/consumer_privacy/laws/code/cc56.asp?codesection=civ&codebody=&hits=20
  - Enumerates the allowed disclosures of medical information
  - Strict liability for any inappropriate disclosure
  - Criminal (misdemeanor) penalty against both healthcare organization and 3rd parties who sought inappropriate access.

- Defines patient's / health plan member's right to private action
  - Nominal damages of $1000 *absent any harm*
  - Punitive damages of $3000 + compensatory damage where there was harm

- Breach notification requirement is applied to personal health information
  - Notify subject individuals
  - Notify the State *Office of Health Information Integrity* at DHS

- Significant 'administrative penalty' o.e. $100k
  - City, County and State prosecutors can file and recover

- Covered entity status based on possession of health information
  - Applies to business associates, other parties not part of 'organized medicine'
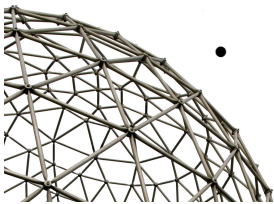
On the [near] Horizon: "HIPAA2"

Easy Congressional target to expand the applicability of HIPAA Privacy and Security Rules and catch up with State regulation.

- Federal Health-e IT Act of 2008
  - http://www.house.gov/stark/news/110th/legislation/200809-HIT/billtext.pdf
  - New incentives to adopt electronic medical records

- Privacy and Security Provisions
  - Extends HIPAA privacy and security mandates to HIPAA Business Associates
    - **FTC to regulate** !!!
  - Requires patient notification in the event of breach of security of ePHI
  - Requires accounting to patients of details of TPO usage
  - Clarifies and strengthens 'minimum usage' requirements

- Significant question:
  - Will new federal rules preempt stronger State law?

On the [distant] Horizon: NHIN

HHS and Congress have been convinced that broad health IT adoption is a near panacean solution for healthcare's ills (escalating cost, quality issues).

- National Health Information Network (NHIN)
  - http://www.hhs.gov/healthit/healthnetwork/background/
  - Allow broad, near-time sharing of electronic health information among health providers
  - Intended to ensure continuity of care, eliminate duplicate testing, appropriate recognition of histories, patient safety, better health planning, etc.
  - Does not leverage existing HIPAA EDI infrastructure (!!!)

- There will be very strong assurance requirements for:
  - Appropriate patient identification
  - Appropriate authorization to release information
  - Appropriate use of SOAP notes, surgical reports, discharge summary
    - Question of data quality, lab calibration, purpose of report

Over the Horizon: "Claim Attachments"

Health plans routinely request clinical information in order to make a determination of the 'medical necessity' and compliance of the treatment for which reimbursement has been requested.

- "Attachments" are subject to HIPAA standardization

- *Clinical* information is maintained in record systems that typically follow HL7 messaging standard
  - EMR integrated with lab & pharmacy systems
  - Provide practitioner access to patient status

- Proposed attachment standard encapsulates HL7 message inside an arbitrary BIN segment of X12 transaction

- General provisioning of attachment request and response completes reimbursement lifecycle
  - Allows for 'auto-adjudication' of healthcare claims
  - Promised administrative simplification and cost saving

- For more information
  - http://www.wedi.org/cmsUploads/pdfUpload/WEDIBulletin/pub/ASIGWhitepaperonClaimsAttachments_0504.pdf
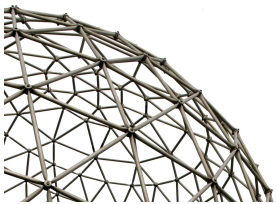
Take Away

- ## HIPAA Standard is immature
  - "legalistic" character awaits clarification
  - HIPAA's privacy and security requirements have been \ will be superseded by more stringent law

- ## HIPAA 'audit' requires significant auditor interpretation of rules
  - Minimal guidance from a non-responsive regulator

- ## Increasing risk as health further integrates medical record systems
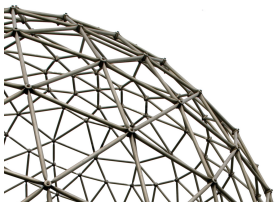
Questions ????

Bill Pankey, CISA, CISSP
Partner, Tunitas Group
bpankey@tunitas.com
209-256-0690

About Tunitas Group
Tunitas Group is a healthcare specific IT consulting firm specializing in IT governance, compliance and risk management. Tunitas Group clients include major hospital corporations, health plans, State and Federal government agencies, vendors and professional associations. Tunitas Group began life in September of 1998 with its sponsorship of a series of workshops exploring the then just released HIPAA Security Standard NPRM.