

Privacy, Security & HIPAA: What it means for Rural Health IT

*Rural challenges and opportunities in security
and privacy.*

How to meld HIPAA and HIT.

Randall E. Sermons, Attorney at Law

130 E. Market St. | Johnson City | Tennessee | 37604 | Phone: 423-434-0885 | Fax: 423-929-8562 | Randy@RandallE.us | www.RandallE.us

Overview

- ✦ HIPAA – Are you hooked?
- ✦ HIPAA – Privacy & Security
- ✦ Health Information Technology
 - Resistance, Implementation & e-Communications
 - Contracting
- ✦ ONCHIT
 - NHIN
 - HISPC
 - HITSP
 - CCHIT
- ✦ Beyond HIPAA
 - What's wrong?
 - Legislation Update



HIPAA

In General



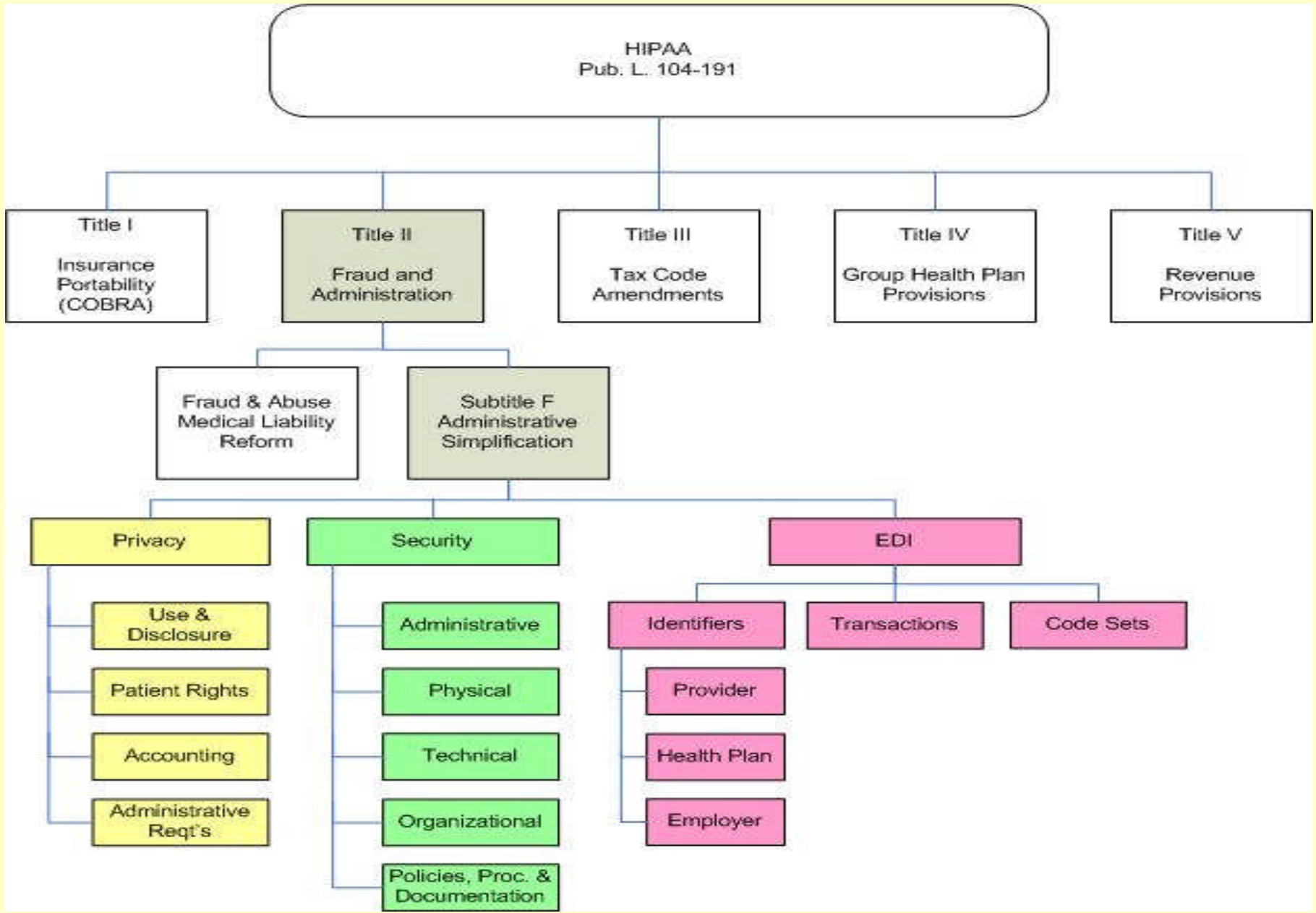
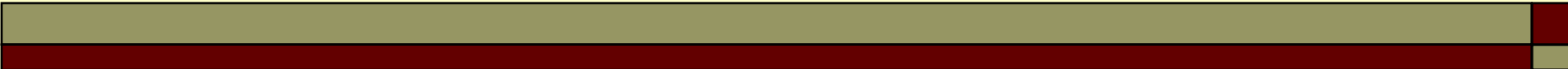
HIPAA Context

- ❖ HIPAA: The Health Insurance Portability and Accountability Act of 1996
 - AKA: Kennedy-Kassebaum Act
 - Public Law 104-191
 - For our purposes:
 - Title II, Subtitle F: Administrative Simplification
 - 45 CFR Parts 160 – 164
 - Privacy, Security, Electronic Data Interchange



HIPAA: The Basic Components

- Privacy
- Security
- Transactions
- Identifiers
- Enforcement





HIPAA – Applies to . . .

HIPAA applies to Health Care Providers who transmit health information in electronic form in connection with a transaction

- Health care claims or equivalent encounter information
- Health care payment and remittance advice
- Coordination of benefits
- Health care claim status
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification and authorization
- First report of injury
- Health claims attachments
- Other transaction that the Secretary may prescribe by regulation



HIPAA – Getting Hooked

- ❖ If any private insurers require you to transmit any health information in connection with a transaction
- ❖ If your office has more than 10 employees
 - You must file electronic claims for reimbursement of federal healthcare program business unless:
 - ◆ Medicare is a secondary payer
 - ◆ “Unusual Circumstances” which prevents you from filing electronically
- ❖ Where you physically cannot keep up with the number of CMS-1500 claim forms in your practice.



HIPAA: Privacy

- ❖ Defines Protected Health Information
- ❖ Defines
 - Covered Entities
 - Affiliated Covered Entities
 - Organized Healthcare Arrangements
 - Business Associates
- ❖ Sets rules for use and disclosure of Protected Health Information by the defined entities.

HIPAA: Privacy & Security

Distinguished

⊕ Privacy

- Determines what information is protected (PHI)
- Applies to PHI in ANY form
- Set rules for use and disclosure

⊕ Security

- Cover PHI in electronic form
- Outlines guidelines for protecting PHI in electronic form:
 - Administrative
 - Physical
 - Technical



HIPAA: Security Requirements

- Organizational
- Administrative
- Physical
- Technical



Required v. Addressable

- ✿ Required – must adopt
- ✿ Addressable –
 - Assess whether the specification is reasonable or appropriate for your practice
 - Implement if it IS reasonable and appropriate
 - If not reasonable or not appropriate – document the reasons. Implement an alternative if appropriate



Considerations

- ✿ Consider the following in evaluating “Addressable” specifications:
 - Size and complexity of the practice
 - Complexity of the IT infrastructure
 - Costs in light of the practice
 - Risks



HIPAA Security: *Partly Scalable*

- ❖ Organizational Requirements
 - Business Associate Contracts (Required)
 - Policies & Procedures (Required)
 - Documentation
 - Time Limit (Required)
 - Availability (Required)
 - Updates (Required)

HIPAA Security: *Partly Scalable,* cont.

⊕ Administrative

- Security Management
 - ◆ Risk analysis (Required)
 - ◆ Risk management (Required)
 - ◆ Employee violation & sanctions (Required)
 - ◆ Information System Activity Review (Required)
- Workforce Security
 - ◆ Authorization & Supervision for access (Addressable)
 - ◆ Workforce clearance procedure (Addressable)
 - ◆ Termination procedures (Addressable)

⊕ Administrative, cont'd.

- Security Officer (Required)
- Information Access Management
 - ◆ Isolating Health Care Clearinghouse Functions (Required)
 - ◆ Access authorization (Addressable)
 - ◆ Access Establishment and Modification (Addressable)

HIPAA Security: *Partly Scalable,* cont.

⊕ Administrative, cont'd.

- Security Awareness training
 - ◆ Security Reminders (Addressable)
 - ◆ Protection for Malicious Software (Addressable)
 - ◆ Log-in Monitoring (Addressable)
 - ◆ Password Management (Addressable)
- Security Incident Procedures
 - ◆ Response & Reporting (Required)

⊕ Administrative, cont'd.

- Contingency Plan
 - ◆ Data Backup (Required)
 - ◆ Disaster Recovery (Required)
 - ◆ Emergency Operation (Required)
 - ◆ Testing & Revision of Disaster Operation & Recovery Plan (Addressable)
 - ◆ Applications & Data Criticality Analysis (Addressable)
- Evaluation of security controls & processes (Required)
- Business Associates (Required)

HIPAA Security: *Partly Scalable,* cont.

⊕ Physical Safeguards

- Facility Access
 - Contingency Operations (Addressable)
 - Facility Security Plans (Addressable)
 - Access Control and Validation (Addressable)
 - Maintenance Records (Addressable)
- Workstation
 - Use (Required)
 - Security (Required)
- Device & Media Controls
 - Disposal (Required)
 - Media Re-Use (Required)
 - Accountability (Addressable)
 - Backup & Storage (Addressable)

⊕ Technical Safeguards

- Access Control
 - User Identification (Required)
 - Emergency access (Required)
 - Automatic Logoff (Addressable)
 - Encryption & de-encryption (Addressable)
- Audit controls (Required) (trending; random; provider focused compare access to provider records of pt visits)
- Data Integrity
 - Data authentication (Addressable)
- Person or Entity Authentication (Required)
- Integrity Controls (Addressable)
- Encryption (Addressable)



Administrative Safeguards: Security Management

- ❖ Risk Analysis (Required)
 - Assess potential risks to breach of confidentiality, integrity and availability of PHI
 - ◆ Balance costs against potential losses
 - ◆ Determine acceptable level of risk

- ❖ Risk Management (Required)
 - Implement security measures necessary to mitigate risks uncovered in Risk Analysis (Required)
 - ◆ Reduce risks to acceptable levels
 - ◆ Maintain (update) (e.g. update of virus software; update policies & procedures based on implementation of new software.



Administrative Safeguards: Security Management (cont'd.)

- ❁ Employee violation & sanctions (Required)
 - Define employee sanctions for violation of security policies & procedures (similar to privacy rule req'ts)
 - ◆ Make them clear & well defined
 - ◆ Communicate them clearly to staff at all levels
- ❁ Information System Activity Review (Required)
 - Regular review IT activity (audit logs; security incidents) (Remember – technical & physical)
 - ◆ Discover inappropriate access (audit logs; facility access logs)



Administrative Safeguards: Workforce Security

- ❖ Authorization & Supervision for Access (Addressable)
 - How to grant & revoke access
 - Role – based (?) personnel clearance or NOT?
 - Vendor access
- ❖ Workforce Clearance Procedures (Addressable)
 - Pre-employment pre-employment and professional reference checks
 - More, as necessary



Administrative Safeguards: Workforce Security, cont'd.

- ✦ Termination Procedures (Addressable)
 - Applies to both permanent & part-time employees
 - Examples:
 - ◆ Keys (physical security)
 - ◆ Inactivate user accounts (technical security)



Administrative Safeguards: Information Access Management

- ❖ Isolating Clearinghouse Functions (Required)
 - Not an issue for small practices
- ❖ Access Authorization (Addressable)
 - Who should have access
 - Access logs documentation
 - Role-based (?)
- ❖ Access Establishment & Modification (Addressable)
 - How to grant, review and maintain access based on changing job roles



Administrative Safeguards: Security Awareness Training

- ❖ Security Reminders (Addressable)
 - Periodic review & education of security policies
 - Staff meetings
 - Discuss security incidents
- ❖ Protection from Malicious Software (Addressable)
 - Disks, etc. brought from home
 - Installation of games
 - Downloads
 - VIRUS Protection



Administrative Safeguards: Security Awareness Training, cont'd.

- ❖ Log-In Monitoring (Addressable)
 - Log-in attempts typically limited
- ❖ Password Management (Addressable)
 - Procedures for creating, changing & safeguarding passwords
 - Education –
 - Not sharing
 - Not easily determined
 - Format (e.g. 8 characters including at least one number)



Administrative Safeguards: Security Incident Procedures

- ✦ Response & Reporting (Required)
 - Identify & mitigate security breaches
 - ✦ Define security breach
 - ✦ Require reporting by employees
 - Document security breaches

Administrative Safeguards: Contingency Plan

- ❁ Data Backup (Required)
 - Procedures for creating & maintaining data
- ❁ Disaster Recovery (Required)
 - Procedures for restoring data
 - ◆ Mitigate threat to patient health
 - ◆ Identify alternative hardware to be used
- ❁ Emergency Operation (Required)
 - How to operate your business without access to electronically stored PHI



Administrative Safeguards: Contingency Plan, cont'd.

- ❖ Testing & Revision of Disaster Operation & Recovery Plan (Addressable)
 - TEST your plan to
 - ◆ Use other hardware
 - ◆ Load your EMR software
 - ◆ Load data
 - ◆ Use alternative system

- ❖ Application & Data Criticality Analysis (Addressable)
 - What are your most crucial software applications
 - ◆ Used to inform other aspects of your contingency planning.

Administrative Safeguards: Evaluation of Security controls & processes (Required)

- Technical & non-technical evaluation of the practice's security policies & procedures
- Once a year
- Also, upon implementation of new software or changes in physical environment
- Review Administrative, physical & technical safeguards



Administrative Safeguards: Business Associate Agreements (Required)

- ✿ Probably already have these in place
- ✿ Security rule has some additional requirements



Physical Safeguards: Facility Access Controls

- ❖ Contingency Operations (Addressable)
 - Covers building access in the event of disaster recovery or emergency operations
- ❖ Facility Security Plan (Addressable)
 - Protection of the facility and equipment from unauthorized access
 - ◆ Doors
 - ◆ Locks
 - ◆ Alarms
 - ◆ ID badges



Physical Safeguards: Facility Access Controls, cont'd.

- ❁ Access Control & Validation (Addressable)
 - How is access to the facility controlled
 - ◆ Who has access?
 - ◆ What areas do they have access to?
- ❁ Maintenance Records (Addressable)
 - Document repairs & changes to the facility related to security
 - ◆ New locks or doors
 - ◆ Adding or moving walls



Physical Safeguards: Workstations

- ✦ Use (Required) & Security (Required)
 - Defines physical surroundings of computer workstations
 - ◆ Cannot be incidentally viewed by patients
 - ◆ Located in secure areas
 - ◆ Includes protection of laptops, PDAs, cell phones, etc.
 - ◆ Medical devices



Physical Safeguards: Device & Media Controls

- ❁ Disposal (Required)
 - Covers disposal of electronic PHI stored on computers, CDs, DVDs, disks, flash drives etc. when they are removed from service
 - DELETING FILES IS INSUFFICIENT
- ❁ Media Re-Use (Required)
 - Covers wiping of electronic PHI stored on computers, CDs, DVDs, disks, flash drives etc. when they are going to be re-used for other purposes or outside the practice



Physical Safeguards: Device & Media Controls, cont'd.

- ❖ **Accountability (Addressable)**
 - Policy & Procedure regarding transport and use of hardware both inside and outside the practice
- ❖ **Backup & Storage (Addressable)**
 - Similar to contingency planning requirements but specifically addresses backup & storage before movement and reconfiguration of hardware



Technical Safeguards: Access Control

- ❖ User Identification (Required)
 - Policy regarding assignment of usernames & passwords
- ❖ Emergency Access Procedure (Required)
 - Provide emergency access as necessary
- ❖ Automatic Log-Off (Addressable)
 - Policy regarding auto log off to prevent unauthorized access. How long?
- ❖ Encryption & Decryption (Addressable)
 - Policy regarding encryption/decryption of electronic PHI transmitted across the internet
 - E-mail!!!



Technical Safeguards: Audit Controls (Required)

- ✿ Record & *examine* activity in information systems containing electronic PHI
 - Hardware, software or procedure may be used.



Technical Safeguards: Data Integrity

- ✿ Authenticate electronic PHI (Addressable)
 - Methods to insure electronic PHI has not been altered or destroyed except as may have been authorized
 - ◆ Key issue – internet access; outside (vendor) access

Technical Safeguards:

Person or Entity Authentication (Required)

- ✿ Pretty much satisfied by username/password policy and procedures.



Technical Safeguards:

- ❖ Integrity Controls (Addressable)
 - Insure electronically transmitted PHI is not modified without your knowledge until disposed of.

- ❖ Encryption (Addressable)
 - Relates to encryption of both transmission of electronic PHI and electronic PHI stored wholly within the practice
 - ◆ Especially good idea for portable media that could be left in a public place such as a restaurant, airport, etc.



Providers & HIPAA Compliance

- ✚ Roadblocks to HIPAA Compliance**
 - “Changes/potential changes in regulations/deadlines”
 - “Organizational Constraints”
 - “No anticipated legal consequences for non-compliance”
 - “Our size limits resources available”
 - “Physicians [have] perception that privacy practices make them less efficient”
 - “[There is] lack of buy-in from senior leadership”

**HMSS / Phoenix Health Systems, US Healthcare Industry HIPAA Compliance Survey Results: Winter 2006,
www.hipaadvisory.com/action/surveynew,
last accessed 8/25/06.



Health Information Technology

HIT & HIPAA

Providers & Resistance to HIT Adoption**

- Payers don't reward efficiency or quality; they pay based on volume
- Adoption issues
 - There is a negative business case for typical health information technology adopter
 - There is a significant electronic health record adoption gap based on organization size
 - There is a first mover disadvantage for health information technology buyers
- High failure rate for electronic health record implementation
 - There is variable availability of IT expertise in physician offices
 - There is a high failure risk for business re-engineering
 - There is limited implementation support for 75,000 small practices
- Limited capacity for interoperability
 - Few health information technology products include standards
 - Standards are not rigorous and lag behind commercialization
 - There is no viable health information exchange infrastructure

**Office of the National Coordinator for Health Information Technology, Current Market Barriers and Challenges to Widespread Adoption of Health Information Technology, <http://www.hhs.gov/healthit/barrierAdpt.html>, last accessed 8/25/06.

Providers & Resistance to HIT Adoption

✦ Financial

- Up-front costs
- Uncertain ROI
- Physician time (productivity losses)

✦ Technological

- Inadequate technical support
- Inadequate data exchange
- Customization
- Lack of standards
- Selection process
- Security & Privacy concerns

✦ Cultural

- Providers & Office staff
- Technical competency
- Inadequate leadership
- Patient acceptance

✦ Organizational

- Changing workflows
- Barrier to physician-patient communication
- Migration from paper
- Staff training
- Legal concerns



HIPAA & HIT - Transitions

- ❖ Setting the tone of the transition
 - Make sure you have a clear vision of the end goal
 - Get input from all involved
 - Put it in writing!
 - Stay on course but be open to modification
- ❖ Operating in a hybrid environment:
 - Using your EHR and paper at the same time
 - Using EHR and manual workflows at the same time

HIPAA, HIT & E-Communications

⊕ Devices/methods

- E-Mail
- PDA
- TXT
- IM

⊕ Desired Uses

- Appointments
- Refills
- Results
- Patient Education

⊕ Problems

- PROPER ID OF Patient
- Privacy/Security
 - Interception
 - Forwarding
 - Storage
- Other
 - Response times
 - Lost / Rule mis-fires
 - Informality
 - Proof of receipt



Security Pitfalls

- ❖ Faulty risk analysis
- ❖ Not following good policies and procedures
- ❖ Lack of system audits
- ❖ Poor system for reporting and responding to security incidents



Why Do This?

- ❁ *Availability of data and data exchange*
- ❁ Tighter audit trails
 - Paper charts don't tell
- ❁ Best practices
 - Prompts
 - Auditing
- ❁ Pay incentives



Health Information Technology

Contracting Issues

What you are buying: Software Licenses

✦ Perpetual

- Capital expense
- Right to use software indefinitely (but watch out for support requirements)
- Still have maintenance & support

✦ Term

- Operating expense
- May only use during the term of the license
- Still have maintenance & support

Types of Software that will be required

- ✦ Primary EMR Application (may be comprised of multiple modules)
- ✦ Practice Management
- ✦ Document Imaging

- ✦ Operating Systems
- ✦ Interface engine
- ✦ Identity & security management

The License: Subparts

- ✦ Right to use
 - Source Code (probably not)
 - Object Code (machine readable)
- ✦ Locations
 - Primary Data Center
 - Local copies / Thin clients
 - Backup & Disaster Recovery
 - Hot Sites
- ✦ Licensed content
- ✦ Limitations / Basis for cost
 - Users or Concurrent Users
 - Physicians
 - Mid-level providers
 - Nurses
 - Administrative Personnel
 - Workstations or Servers
 - Exam rooms
 - Patient records
 - Transactions



What you are buying: Hardware

- ❁ Get definitive list from vendor but will generally include:
 - Servers
 - Routers (wired and/or wireless)
 - Desktops, laptops, tablet PCs
 - Printers
 - Scanners
 - Bar code readers
 - Uninterruptible power supply

Where to put it all: On-Site v. ASP

- ⊕ Hosting the application yourself

- On-Site
 - ◆ Personnel
 - ◆ Space & infrastructure
- Data Center options
 - ◆ Multi-site practices
 - ◆ “On-the-Wire” issues

- ⊕ Hardware requirements

- ⊕ Capital expenditures

- ⊕ Application Service Provider (ASP)

- EMR Vendor
- Third party providers

- ⊕ Basis for cost

- Processing fees
- Reporting

- ⊕ “On-the-Wire” issues

- ⊕ Reduced hardware requirements

- ⊕ Reduced capital expenditures

- ⊕ Bringing the system In-House later



What you are buying: Maintenance & Support

Ongoing guaranty that Warranties remain in force

✦ Maintenance

- Correction of warranty defects
- Updates, releases and versions
 - ✦ Minimum implementation times
- Interface upgrades (primary v. third party changes)
- Hardware & software upgrades

✦ Support

- 24X7X365 – Probably
- Escalation levels & response times
- Documentation
- Down-level support



What you are buying: Training

- ❁ On-Site v. Vendor's site
- ❁ Interrupting workflow
- ❁ Varying levels of training
- ❁ New staff
- ❁ Yearly training
- ❁ Training on upgrades

Warranties

- Right to grant licenses
- Will function in accordance with the documentation
 - “substantially” v. “in all material respects”
- Software, third party software, hardware & custom programming will function as a system
- Software conforms to applicable laws
 - Will not prevent compliance
- No threatening litigation
- Software free from worms, viruses, trojan horses, or other malicious code
- No disabling code
- Core functionality will not be removed
- Warranty pass through for third party hardware & software
- Interoperability requirements
- Certification



Warranty Disclaimers

- ✿ Responsibility for patient care
- ✿ Limitations to express warranties
- ✿ Internet



Warranties: Interoperability

- ✦ The vendor must warrant that its software will conform to any applicable interoperability standards enacted, promulgated or adopted by, or pursuant to recommendation of, the Department of Health and Human Services, as well as any generally-accepted standards commonly adopted and utilized by and among health information exchange solutions providers.



Warranties: Certification

- ❖ The vendor must warrant that its software will meet applicable certification requirements promulgated or adopted by, or pursuant to recommendation of, the Department of Health and Human Services.



Liability & Insurance

- ✦ Convergence of:
 - Indemnities (typically for Intellectual Property and Bodily Injury) – *should never be subject to limitations of remedies clauses*
 - Limitations of Remedies
 - ♦ Ideal – greater coverage during implementation
 - ♦ Minimum – all amounts paid under the contract
 - Damage Waivers (incidental/consequential/punitive)
 - Insurance – Protection against insolvency of vendor
 - ♦ Comprehensive General Liability with bodily injury property damage, personal injury, advertising injury, medical payments, products and completed operations
 - ♦ Professional Liability (Errors & Omissions) with an electronic data liability endorsement.
- ✦ Self Insurance – subject to actuarial review & reserves



Termination & Dispute Resolution

- ❖ Avoid possibility of premature termination before project is completed.
- ❖ Structure collaborative escalation methods with vendor executives
- ❖ Require mediation as a first step (not arbitration)
- ❖ Choice of law
- ❖ Choice of forum



Source Code Escrow

- ❖ Of dubious benefit
 - Access governed by agreement between vendor and source code escrow agent
 - Will not protect you in event the vendor becomes bankrupt
 - May protect you if vendor is sold or software is suddenly discontinued
 - What are you going to do with it?



The implementation timeline

- ❖ Attached to the contract?
- ❖ Considers total business operations and other IT projects?
- ❖ Coordination of delivery & acceptance
 - Failure to meet terms of documentation or functional requirements
 - Minimum re-testing time
 - Warranties in effect?



Statement of Work

- ❖ Describes tasks to be performed by both the practice and the vendor – largely a technical document
 - Interfaces
 - Education & training
 - Assignment of personnel
- ❖ **READ CAREFULLY!**
 - Personnel issues
 - Additional hardware & software issues
 - Hidden terms & conditions



Change Orders

- ❖ Require mutual agreement
- ❖ Require full disclosure of all additional costs
- ❖ Review the Statement of Work carefully



Vendor Personnel


- ❖ Require only the best!
- ❖ Control office access
- ❖ Protect your business operations during implementation
- ❖ Retain and exercise the right to remove personnel



Balancing Risk

- ✿ The best protection – YOUR functional requirements coupled with the Vendor's responses
- ✿ Establishing metrics –
 - Pre-installation v. post-installation metrics
 - Reduction in certain administrative costs
 - Decrease in accounts receivable
- ✿ Negotiating Metrics
 - Its all about control
- ✿ Tying metrics to performance
 - Penalties
 - Benefit funding models – ceding control for a short period of time
 - Interest free loans

Some of these options will not be available from smaller vendors.



How to keep your business running when things go wrong

- ❖ Backups
 - On-site, Off-Site, Mirrors
- ❖ Installing new software
- ❖ Design manual procedures **BEFORE** things go wrong
- ❖ Require vendor to provide assistance in event of failure of the system
 - Temporary help
 - Interest free loans



Office of the National Coordinator of Health Information Technology

ONCHIT Initiatives



ONCHIT

- ✿ Established by Executive Order

Mission:

The Office of the National Coordinator for Health Information Technology provides leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of health care and the ability of consumers to manage their care and safety.

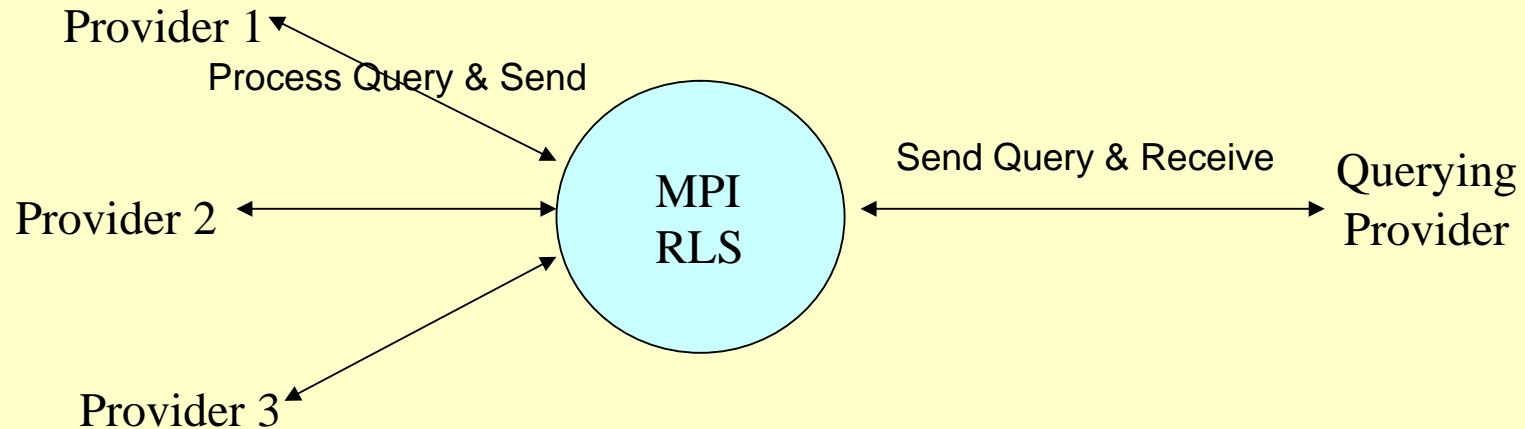


ONCHIT: Three Focus Areas

- ❖ Drive EHR adoption:
 - EHR Certification (CCHIT)
 - Standards for Interoperability (HITSP)
- ❖ Regional Health Information Organizations
- ❖ National Health Information Network
 - Demonstration Projects (NHIN)
 - Health Information Security & Privacy Collaboration (HISPC)

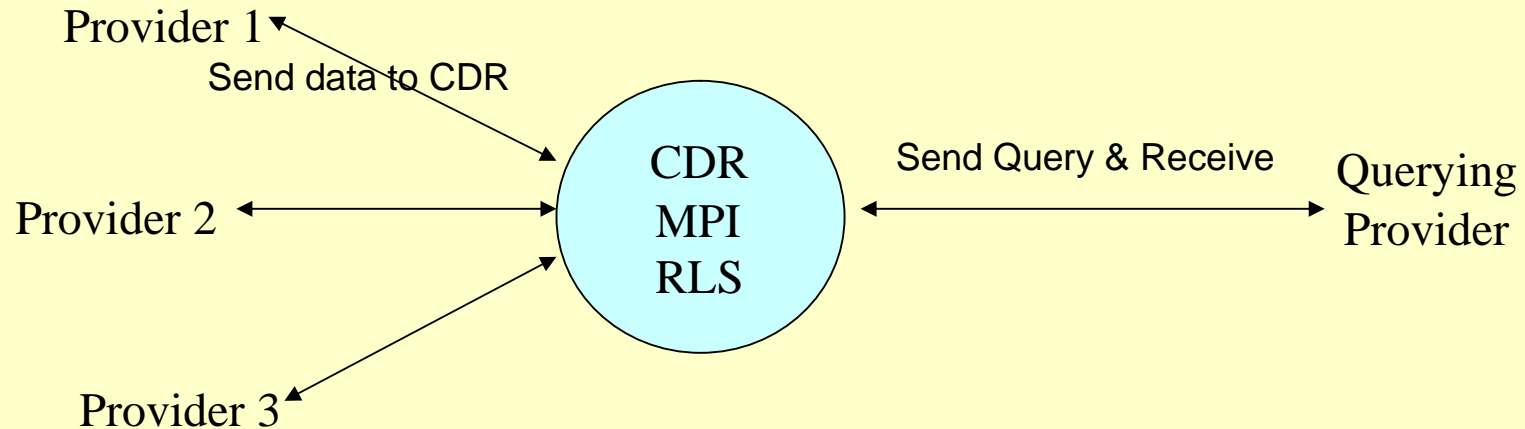
Health Information Exchange Models

❖ Distributed Model



Health Information Exchange Models

❁ Central Data Repository





Health Information Exchange Models

- ✿ Central Data Repository (Siloed or not)

HIT: NHIN Demonstrations (NHIN)

- Accenture
 - Eastern Kentucky
 - Northeast Tennessee / Southwest Virginia (CareSpark)
 - West Virginia
- CareScience
 - Indiana Health Information Exchange
 - MA-SHARE
 - Mendocino HRE
- Northrup Grumman
 - Santa Cruz RHIO
 - HealthBridge (Cincinnati)
 - University Hospitals Health System (Cleveland)
- IBM
 - Taconic Health Information Network and Community
 - North Carolina Healthcare Information and Communications Alliance (Research Triangle)
 - North Carolina Healthcare Information and Communications Alliance (Rockingham County)

HIT: Standards Harmonization (HITSP)

- ❖ American National Standards Institute (ANSI)
- ❖ A cooperative partnership between the public and private sectors for the purpose of achieving a widely accepted and useful set of standards specifically to enable and support widespread interoperability among healthcare software applications, as they will interact in a local, regional and national health information network for the United States.

HIT: Certification of EMRs (CCHIT)

- ✿ Certification Criteria complete May, 2006
 - Functionality
 - Security
- ✿ See list of certified products:

<http://www.cchit.org/>



HIT: Privacy & Security Solutions (HISPC)

- RTI & National Governor's Association
- 33 States
- Assess variations in organization-level business practices and policies and current state laws related to the privacy and security of health information



What's Missing?

- ✿ Federal support for RHIOs.
- ✿ Federal support for last mile connectivity
- ✿ Federal support for purchases of EMR systems
 - *Cf.* Stark Amendments



Beyond HIPAA

- ❁ HIPAA Shortcomings
 - Limited applicability
 - ◆ Clinical Research
 - ◆ RHIOs (?)
 - ◆ Personal Health Record systems operated by otherwise non-covered entities
 - Lack of robust enforcement (?)
 - ◆ Facilities
 - ◆ Individuals
 - Competing state laws



Legislative Update

- ❁ Wired for Health Care Quality Act (passed 11/18/05)
 - Patient control & consent over use
 - Ensure technology in place to track consent
 - Incorporate audit trails
 - Enforcement to follow the information
- ❁ Better Health Information System Act (passed 7/27/06)
 - Grants to underserved & rural communities for HIT



Thanks!

Randall E. Sermons, Attorney at Law

130 E. Market St. | Johnson City | Tennessee | 37604 | Phone: 423-434-0885 | Fax: 423-929-8562 | Randy@RandallE.us | www.RandallE.us