

Hyper-HIPAA

Brad Smith

RN,BS,MCNSP,ASCIE,CISSP..

CIR Security dir@EndHack.com

Who are You



- Solo Practitioner, IT, Administrative
- Unix, Linux, Windows 4 / 2003
- More than 250 computers
- Multiple locations
- Sole maintenance, Staff over 10, Consultant

Agenda

- HIPAA Security Standards
- Risk Analysis
- Administrative safeguards
- Physical safeguards
- Technical safeguards



CIR Security www.EndHack.com

Basics of Security

- Confidentiality
 - Only those who need to see data, can see data
- Integrity
 - Same data that went in, comes out
 - Tough to enforce,
- Accessibility
 - Can who needs the data get the data

CIR Security www.EndHack.com

What You don't know about HIPAA

- Just standard security brought to hospitals
- Not as tight as GLB
- Hacking attempts are up, especially banks, medical
- Used to protect patients in the computer age, Identity Theft
- Used to warn of Biological attack
 - Atlanta, Washington DC, Chicago done

CIR Security www.EndHack.com

Figure 12. How Many Incidents? From Outside? From Inside?

How Many Incidents? by percentage	1 – 5	6 – 10	>10	Don't Know
2004	47%	20%	12%	22%
2003	38%	20%	16%	26%
2002	42%	20%	15%	23%
2001	33%	24%	11%	31%
2000	33%	23%	13%	31%
1999	34%	22%	14%	29%
How Many Incidents From the Outside?	1 – 5	6 – 10	>10	Don't Know
2004	52%	9%	9%	30%
2003	46%	10%	13%	31%
2002	49%	14%	9%	27%
2001	41%	14%	7%	39%
2000	39%	11%	8%	42%
1999	43%	8%	9%	39%
How Many Incidents From the Inside?	1 – 5	6 – 10	>10	Don't Know
2004	52%	6%	8%	34%
2003	45%	11%	12%	33%
2002	42%	13%	9%	35%
2001	40%	12%	7%	41%
2000	38%	16%	9%	37%
1999	37%	16%	12%	35%

CIR Security www.EndHack.com

Overview / Review

- **Who:** Anyone with Paper/ Electronic Protected Health Information (EPHI) in ELECTRONIC Form
- **How:** Reasonable and appropriate administrative, physical and technical safeguard.
 - Protect against any Reasonably Anticipated threat or hazard to the security or integrity of EPHI
- **When:** Effective April 21, 2003,
- **Why:** It's the law, ID theft, Bioterrorism alert, good business

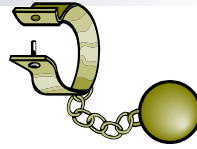
CIR Security www.EndHack.com

What is EPHI

- Information that might lead to identity theft
 - Age, Race, Handed, social security number, address, anything that might identify the patient
- Same as GLB
- Only electronic
 - Paper / Verbal is PHI

CIR Security www.EndHack.com

HIPAA Enforcement



- Fines aren't bad if compliance in progress
 - University of Pittsburg has worked 3 years on their plan
- Worse for no plan
- Worst for intentional violation (data selling)
- Whistle blower payment
 - Your staff, your patients, your competitors
- Loss of public image

CIR Security www.EndHack.com

HIPAA Guiding Principle



- Scalability: Not one size fits all (Great for rural areas)
- Comprehensiveness: Unified between all Covered Entities (CE) "Defense in Dept" attitude
- Technology neutral: No specific technology recommendations
- Internal and External security threats: must protect against both

CIR Security www.EndHack.com

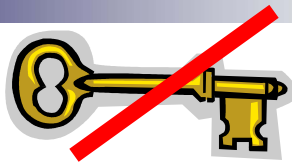
- **Minimum Standard:** Security rule only defines minimum, not maximum, so these are the baseline needed to comply
- **Risk Analysis:** How much to protect verses the value of that being protected
 - Required to conduct a thorough and accurate risk analysis
 - Expected to consider “all relevant losses”
 - Includes unauthorized use and disclosure and modification of data

CIR Security www.EndHack.com

HIPAA Key Concepts

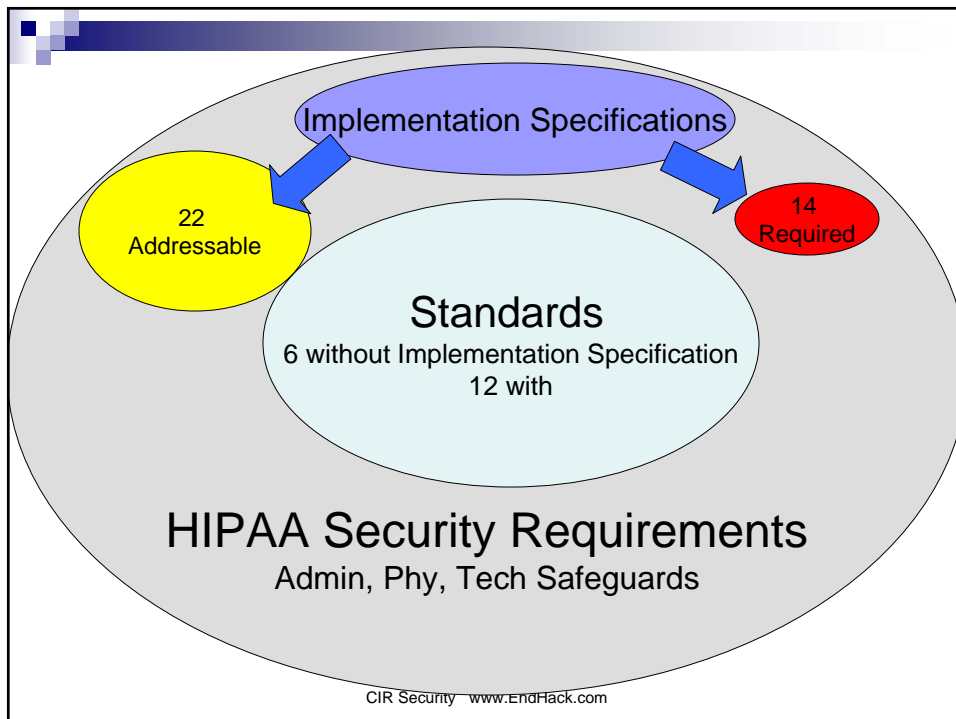
- **Principle based:** based on current security best practices
- **Reasonableness:** Balance resources and business risk of EPHI
- **Full Compliance:** All staff (management, off site, contract workers, Everybody) must comply
- **Ongoing Compliance:** Regular training, policy and procedure review

CIR Security www.EndHack.com



- Developed from multiple security guidelines and standards: Couldn't find "golden rule" to fit all
 - Customizable for our particular environment, What Mayo does doesn't fit frontier Montana and is not expected or needed.
 - Base on current best practice
- Documentation: Written processes, policies and procedures, Implementation and training, 6 years

CIR Security www.EndHack.com



CIR Security www.EndHack.com

22 Addressable

- 3 Choices,
 - Do it, Do it with change, Can't do it at all
 - Based on:
 - Size, Complexity, Capabilities, Budget,
 - Technical infrastructure: Hardware, Software, Security capabilities
 - Cost of security measure
 - Seriousness of risk potential,
 - Tools for Analysis:
 - Gap Analysis, Risk Analysis, Risk Management...

CIR Security www.EndHack.com

Addressable Choices

- Do it: If determined to be “reasonable and appropriate” must implement it
 - Document implementation
- Do it with Change: Not “reasonable and Appropriate” and the standard cannot be met without additional measures
- Don't Do it: Not “reasonable and appropriate” and the standard can be met WITHOUT alternative measures

CIR Security www.EndHack.com

Addressable Choices

- MUST Document ALL 22 Requirements!!
- MUST still meet in some way
- NOT the easy out, Paperwork, Paperwork
- Most are need and can be done with just Policy and Procedure (P/P) change
- Think about your size

CIR Security www.EndHack.com

Administrative Safeguards

- 50% of total standards
- Documentation
- Policies and Procedures
- Best time for business restructure
- Most volatile by state
- Delegation of duties, training

CIR Security www.EndHack.com

Administrative Section

- 9 Standards
 - 1 Security Management Process: 4 Required Specifications:, (asses, fix, policy, review,)
 - 2 Assigned Security Responsibility: Required, No implementation spec,
 - 3 Workforce Security: 3 Addressable Implementation Specifications, Should already have these with HR from Privacy

CIR Security www.EndHack.com

- 4 Information Access Management: 1 Required , 2 Addressable, Who can see what, (isolate clearing house)
- 5 Security Awareness Training: 4 Addressable Implementation, "Knowing is half the battle" GI Joe
- 6 Security Incident Procedures: 1 Required Implementation, "Am I being Hacked?"
- 7 Contingency Plan: 3 Required , 2 Addressable, Should be in place from Privacy, How do keep seeing clients in an emergency and how do you know you plan works?

CIR Security www.EndHack.com

8 Security Evaluation: Required, no specifications, "Keeping up with the Jones", Annual Risk Assessment, ensuring not a one time process

9 Business Associate Contracts and Other Arrangements: 1 Required, "...to create, receive, maintain, or transmit EPHI on the covered entity's behalf"

- 12 Required
- 11 Addressable

CIR Security www.EndHack.com

Administrative Rule Tips for All

- Make team, assign duties in area of specialization, make call list, document, short presentation to C's
- Do Gap analysis, IT Business Impact Analysis
- Risk Analysis with Mitigation plan,
- Budget: ROI, Penalties, Business Loss

CIR Security www.EndHack.com

Administrative Rule Tips for All

- Agree on final outcome, work backwards
- Start with highest risk for RA,
- Do Addressable first, easiest,
 - Usually only policy / procedure
- Document, Document, Document
- Train Everybody on security
- Create update milestones for all documents, checklist
- Rinse and Repeat

CIR Security www.EndHack.com

Administrative Rule Tips for Small

- Easiest with fewest computers
- Firewall if on Internet
- Virus / Bot protection
- Update software regularly
- Don't let accounting machines get e-mail
- Mainly Policies
- Engage passwords for everybody
- Look at log weekly, document

CIR Security www.EndHack.com

Administrative Rule Tips for Large

- Need to meet more addressable
 - Should have most done
- Log monitoring randomly on random files or high profile files, log files would be huge
- Auto scan everything, e-mail, attachment, saves \$

CIR Security www.EndHack.com

Physical Safeguards

- Protects against unauthorized entry / usage
- Protects media (disks, tape) from compromise
- Applies to
 - Facility
 - Computers
 - Data



CIR Security www.EndHack.com

Physical Safeguards

- 4 Standards
 - 10 Implementations Specifications
 - 6 Addressable
 - 4 Required
- Most Policies and locks

CIR Security www.EndHack.com

More than 1 Way

- Multiple requirements based on parent organization
 - Control Object for Information and Related Technology (COBIT) by Information Systems Audit and Control Association (ISACA)
 - ISO 17799: global security management standard
 - NIST 800-66 mapped all together

CIR Security www.EndHack.com

Standards

- 1 Facility Access Controls: control of who can use facility, remote facilities AND EPHI
- 2 Workstation Usage: control of who can use workstations
- 3 Workstation Security: physical things to keep the wrong people from using/seeing EPHI
- 4 Device and Media Controls: how hardware, data is physically moved in/out of facility

CIR Security www.EndHack.com

Purpose of Physical Standards

- Cheaper to hire a crowbar cowboy than hacker
- Protect hardware, physical data media, and building from problems
- Must mitigate areas in Risk Analysis
- Form 3 layer security model
 - Facility, Workstation, Data media
- Larger more difficult than small

CIR Security www.EndHack.com

Physical Definitions

- Facility is Physical location and any remote locations
- Divide into security domains:
 - Perimeter
 - Public Area: lobbies, docks
 - Private Area: employees work space
 - Restricted Area: critical function area, lab, computer room
- Control Objects are doors, computers, locks, etc



CIR Security www.EndHack.com

Maintenance Records

- Addressable
- "...to document repairs and modifications to the physical components of a facility that are related to security..."
- Already have in Maintenance department
 - Great help if understand why and process
 - Area of Specialization
- Need for Physical Asset accounting



CIR Security www.EndHack.com

Large: Asset Documentation

- Define accountability requirements
- Assign device and media assets to information custodian
- Process of accountability for media, asset life cycle
- Train staff on accountability
- Consider technical solutions
 - Bar codes, tracker chips,

CIR Security www.EndHack.com

Small: Asset Documentation

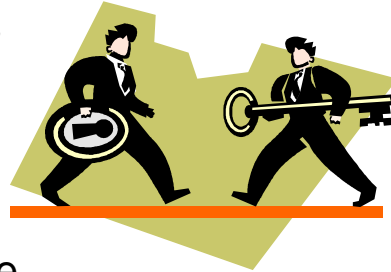
- Inventory
- Ask accountant
- Don't be lax in device security
- Shred everything



CIR Security www.EndHack.com

Technical Safeguards

- Process to protect data and control access
- Authentication controls
- Encryption
- Transmission
- Most changeable
- Should have most done



CIR Security www.EndHack.com

Technical Standards

- 4 Standards
 - 4 Required, 5 Addressable, Very addressable by size
 - Defense in Depth: firewalls, antivirus, Intrusion Detection Software, Intrusion Prevention Software, Filtering software/hardware, testing mechanism
- Access Control: Controls who can access data, decide on type of access control
- Audit Controls: Making sure only authorized access occurs, log file review

CIR Security www.EndHack.com

1 Access Control

- *Unique User Identification: Required*
- Password
 - 6 characters, better than bsmith or brads
 - Alert if two users are logged on with same name
 - Create fast for new users
 - Remove quickly for leaving users
- Minimum usage, not everybody uses same application

CIR Security www.EndHack.com

1 Access Control

- *Emergency Access Procedure: Required*
 - Establish procedure to allow access to EPHI during an **emergency**
 - Only level 2 nurses can see local staff records, all 2's are in emergency, level 1 needs records
 - Activate procedure and DOCUMENT WHY
 - Should be part of Disaster Recovery Plan, Part of Business Continuity Plan

CIR Security www.EndHack.com

Business Continuity Plan (BCP)

- Business Impact Analysis: Where are our critical resources and what happens when there is a problem?
- IT BCP: data, critical services, “1st up”
- Emergency Continuance Plan: continue in emergency
- Disaster Recover Plan: how to get everything up and running

CIR Security www.EndHack.com

Disaster Recover Plan (DRP)

- What applications do we retrieve pt data with?
- Are they backup up and verified?
- How long could we go without admitting patients? Maximum acceptable downtime

CIR Security www.EndHack.com

DRP

- Develop acquisition plan: where is backup? Key?
- Written restore that ANYONE can do
- DRP team names and numbers
- Test access authorization, total plan
- Revise, Redocument and Redo on Milestone date
- Change with upgrades, staff change

CIR Security www.EndHack.com

2 Audit Controls

- Required
- Federal Information Systems Controls and Audit Manual (FISCAM)
 - User access and account activity
 - Exception reports
 - Dormant account reports
 - System resource monitoring
 - Data integrity controls
 - Failed log-in reports

CIR Security www.EndHack.com

- Users switching user IDs during an on-line session
- Attempts to guess passwords
- Attempts to use privileges that have not been authorized
- Modifications to production application software
- Modifications to system software
- Changes to user privileges
- Changes to logging subsystems

CIR Security www.EndHack.com

Why Encryption

- FBI report: 2003
 - 80 % of organizations that had firewalls and antivirus
 - 1/2 had perimeter security breached
 - External now equals Internals attacks
- Start considering OS upgrades
 - MS Small Business Server (75)
 - Novell Suse: out soon

CIR Security www.EndHack.com

Concepts of Strategic Planning

- Goal: Set by Entity
- **Strategic Plan:** How to achieve goal
- **Tactical Plan:** Steps to reach strategic Plan, Birthplace of Policies
- **Operational Plan:** Day to day operations, Procedures fit here
- Operational = Strategic!

CIR Security www.EndHack.com

Plan for Success

- Identify the project boss, management supporters
- Assemble HIPAA team
 - **Large:** All departments and remote
 - **Small:** At least 2 people
- Schedule regular team meeting,
 - Train members
 - Structure

CIR Security www.EndHack.com

Plan for Success

- Prepare for Risk Assessment
 - Break down tasks
 - Estimate level / duration of effort
 - Assign responsibilities
 - Develop timeline
 - Do budget
- Do Baseline P/P, system, inventory
 - ALL P/P, complete system inventory
 - IT Business Continuity plan
 - Interview Staff (Gap Analysis)

CIR Security www.EndHack.com

Plan for Success

- Who are your ePHI partners
 - Check who gets / gives data
 - Where data is stored
 - Which programs access data
- Do Administrative, Technical, and Physical review
 - More Gap Analysis
 - Situation Inventory Checklist for ALL Sections (enclosed)
 - Document everything

CIR Security www.EndHack.com

Plan for Success

- Review old P/P for changes r/t security
- Identify gaps between current P/P, systems and application
 - Use all collected data
 - Use form enclosed
- Do security Risk Analysis (RA)
 - Pick methodology to use
 - Qualitative VS Quantitative
 - Automated tools

CIR Security www.EndHack.com

- Identify value of assets
- Degree of Exposure
- Consequences
- Likelihood of Occurrence
- Remediation methods
- Cost of remediation VS threat
- Do Impact analysis
 - With RA
 - Reputation, financial

CIR Security www.EndHack.com

- Do final RA report
 - Look for business improvement opportunities
 - Areas of biggest threat
 - Must meet strategic goals
- Re-read security rule
 - Especially addressable areas
- Develop security plan
 - Reasonable for facility size
 - Timeline / Cost for completion
 - Fixes Gap, closes security risks from RA

CIR Security www.EndHack.com

- Implement solutions
 - Detailed plan, who, when, where, why
 - Monitor plan for deviation
- Document
 - Addressable decisions
 - All analysis that get you here
 - All rational for decisions
 - Keep C's in loop
- Reassess periodically

CIR Security www.EndHack.com

Review

- Review of Standards
- Compliance Issues
- Enforcement Issues
- General Path

- Questions?

CIR Security www.EndHack.com

Questions

- What needs to be in every policy?
- Why don't some required have implementation standards?
- HIPAA-CISSP group on Yahoo
- CMS web site

- Thanks

CIR Security www.EndHack.com

