Introduction and Overview- *The HIPAA Security Rule*

John Parmigiani
National Director
HIPAA Compliance Services
CTG HealthCare Solutions, Inc.

Presentation Outline

ctg HealthCare Solutions

- Introduction
- Overview of HIPAA Security and its Impact
- Steps Toward Compliance
- Tools for Compliance
- Conclusions

Introduction

John Parmigiani

- CTGHS Director of HIPAA Compliance Services
- HCS Director of Compliance Programs
- HIPAA Security Standards Government Chair/ HIPAA Infrastructure Group
- Directed development and implementation of security initiatives for HCFA (now CMS)
  - Security architecture
  - Security awareness and training program
  - Systems security policies and procedures
  - E-commerce/Internet
- Directed development and implementation of agency-wide information systems policy and standards and information resources management
- AMC Workgroup on HIPAA Security and Privacy;Content Committee of CPRI Security and Privacy Toolkit; Editorial Advisory Board of *HIPAA Compliance Alert's HIPAA Answer Book*

Overview of HIPAA Security & its Impact

Title II: Subtitle F Administrative Simplification Goals

ctg HealthCare Solutions

- Reduce healthcare administrative costs by standardizing electronic data interchange (EDI) for claims submission, claims status, referrals and eligibility
- Establish patient's right to Privacy
- *Protect patient health information by setting and enforcing Security Standards*
- Promote the attainment of a complete Electronic Medical Record (EMR)

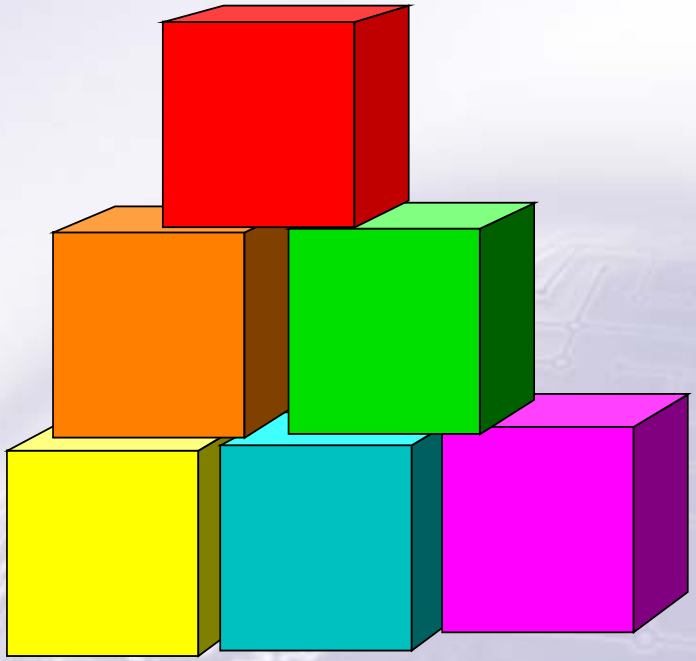
HIPAA Characteristics

ctg HealthCare Solutions

- HIPAA is forever and compliance is an ever-changing target
- HIPAA is more about process than technology
- HIPAA is about saving $$ and delivering improved healthcare
- HIPAA is policy-based (documentation is the key)
- HIPAA advocates cost-effective, reasonable solutions
- HIPAA should be applied with a great deal of "common sense"

Security Goals

- Confidentiality
- Integrity
- Availability



of protected health information

Security is Good Business

ctg HealthCare Solutions

- No such thing as 100% security
- "Reasonable measures" need to be taken to protect confidential information (due diligence)
- A balanced security approach provides due diligence without impeding health care
- Good security can reduce liabilities- patient safety, fines, lawsuits, bad public relations

Benefits of Security

- Security can protect confidential information {Can have security by itself, but *Cannot have Privacy without Security*}
- Health care organizations can build patient trust by protecting their confidential information.
- Trust between patient and provider improves the quality of health care

HIPAA Security Framework

ctg HealthCare Solutions

Flexible - Scalable - Technology Neutral

- **Each affected entity must assess own security needs and risks**

&

- **Devise, implement, and maintain appropriate security to address business requirements**

HIPAA Security Standards

ctg HealthCare Solutions

- **NPRM- 8/12/1998**
  - **Administrative Requirements (12)**
  - **Physical Requirements (6)**
  - **Technical Requirements [data at rest](5)**
  - **Technical Requirements [data in transit](1)**
  - **Electronic Signature**
  - **Implementation Features (70)**

BS 7799/ISO 17799

ctg HealthCare Solutions

- Security Policy
- Security Organization
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance

Standard Areas of Business Security

Security – The Privacy Rule

- **164.530 (c)**
  - **Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information**
  - **Implementation specification: safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.**

HIPAA Statutory- Security [USC 1320d-2(d)(2)]

ctg HealthCare Solutions

"Each covered entity who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards : (A) to ensure the integrity and confidentiality of the information; and (B) to protect against any reasonably anticipated (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information; and (C) otherwise to ensure compliance with this part by the officers and employees of such person"

Is in Effect Now!

Security Standards

ctg HealthCare Solutions

- **What do they mean for covered entities?**
  - **Procedures and systems must be updated to ensure that health care data is protected.**
  - **Written security policies and procedures must be created and/or reviewed to ensure compliance.**
  - **Employees must receive training on those policies and procedures.**
  - **Access to data must be controlled through appropriate mechanisms (for example: passwords, automatic tracking of when patient data has been created, modified, or deleted).**
  - **Security procedures/systems must be certified (self-certification is acceptable) to meet the minimum standards.**

HIPAA Security-The Final Rule

ctg HealthCare Solutions

- Final Rule in clearance- expected to be published Fall (Q4) 2002
- What to expect
  - Streamlining- Same core values- more specificity as to mandatory (must do)/discretionary (should do)
  - Fewer standards
  - No encryption on private networks
  - Business Associate Contracts/Chain-of-Trust
  - Synchronization with Privacy
- What not to expect
  - No Electronic Signature but…not dead for health care

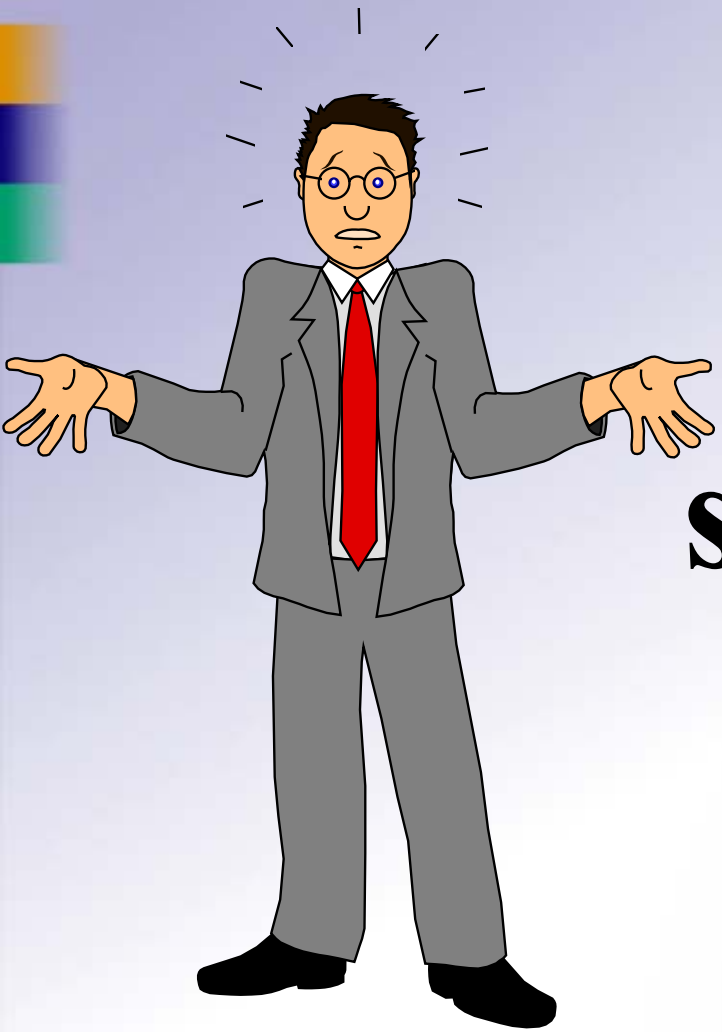
Electronic Signature Standard

ctg HealthCare Solutions

- Comments to Security NPRM indicated a lack of consensus; industry continues to work on, monitored by NCVHS
- NCVHS necessary before regulation developed
- Transaction standards do not require
- Security NPRM specified digital signature (authentication, message integrity, non-repudiation requirements)
- NIST rather than DHHS will probably develop
- PKI-HealthKey Bridge effort / interoperability problems

Steps Toward Compliance

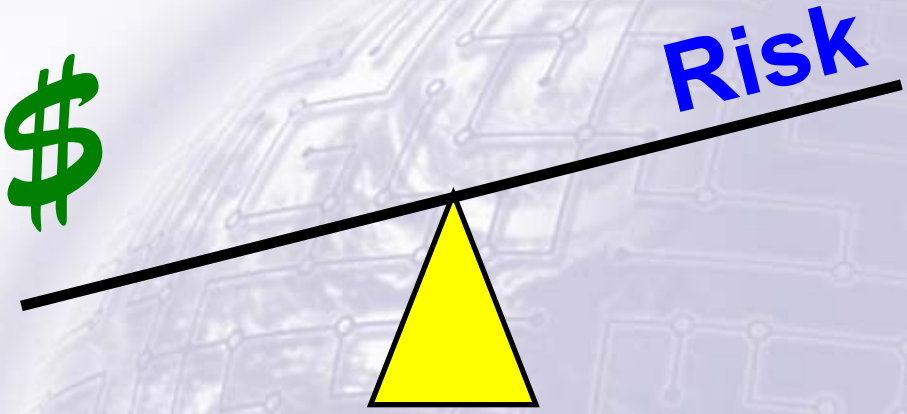
$$$$$$$$$!!!???



So how much security do you really need?

A Balanced Approach

- Cost of safeguards vs. the value of the information to protect
- Security should not impede care
- Your organization's risk aversion
- Due diligence



Security Measures

ctg HealthCare Solutions

In general, security measures can grouped as:

- Administrative
- Physical
- Technical (data in transit and data at rest)

Administrative Procedures Checklist

- Contracts with every business partner who processes PHI
- Contingency Plans
- Written Policies regarding routine and non-routine handling of PHI
- Audit logs and reports of system access
- Information Systems Security Officer
- HR policies re security clearances, sanctions, terminations
- Security Training
- Security Plans for each system-all phases of SDLC; periodic recertification of requirements
- Risk Management Process
- Security Incident reporting process

Physical Safeguards Checklist

- Policies and Procedures re data, software, hardware into and out of facilities
- Physical access limitations- equipment, visitors, maintenance personnel
- Secure computer room/data center
- Workstation policies and procedures
- Workstation location to isolate PHI from unauthorized view/use

Technical Security (data @ rest) Checklist

- Authentication Policies and Procedures- one factor/two factor/three factor
- Access Controls
- Data (Integrity) Verification and Validation Controls
- Audit Controls
- Emergency Access (Availability) Procedures

Technical Security Mechanisms (data in transit) Checklist

- VPN or Internet; Intranet/Extranet
- Closed or Open System
- Encryption Capabilities
- Alarm features to signal abnormal activity or conditions- event reporting
- Audit trails
- Determine that the message is intact, authorized senders and recipients, went through unimpeded
- Messages that transmission signaling completion and/or operational irregularities

Tools for Compliance

Security Compliance Areas:

- Training and Awareness
- Policy and Procedure Review
- System Review
- Documentation Review
- Contract Review
- Infrastructure and Connectivity Review
- Access Controls
- Authentication
- Media Controls

Security Compliance Areas…:

- Workstation
- Emergency Mode Access
- Audit Trails
- Automatic Removal of Accounts
- Event Reporting
- Incident Reporting
- Sanctions

Who needs to be trained? Everyone!

- Management
- Clinical
- Non-Clinical
- Board of Directors
- Vendors
- Contractors
- Volunteers
- Physicians
- Educators
- Researchers
- Students
- Patients

Includes: Full-time, part-time, PRN, Temps, etc.

Security Training Areas-from the Security NPRM

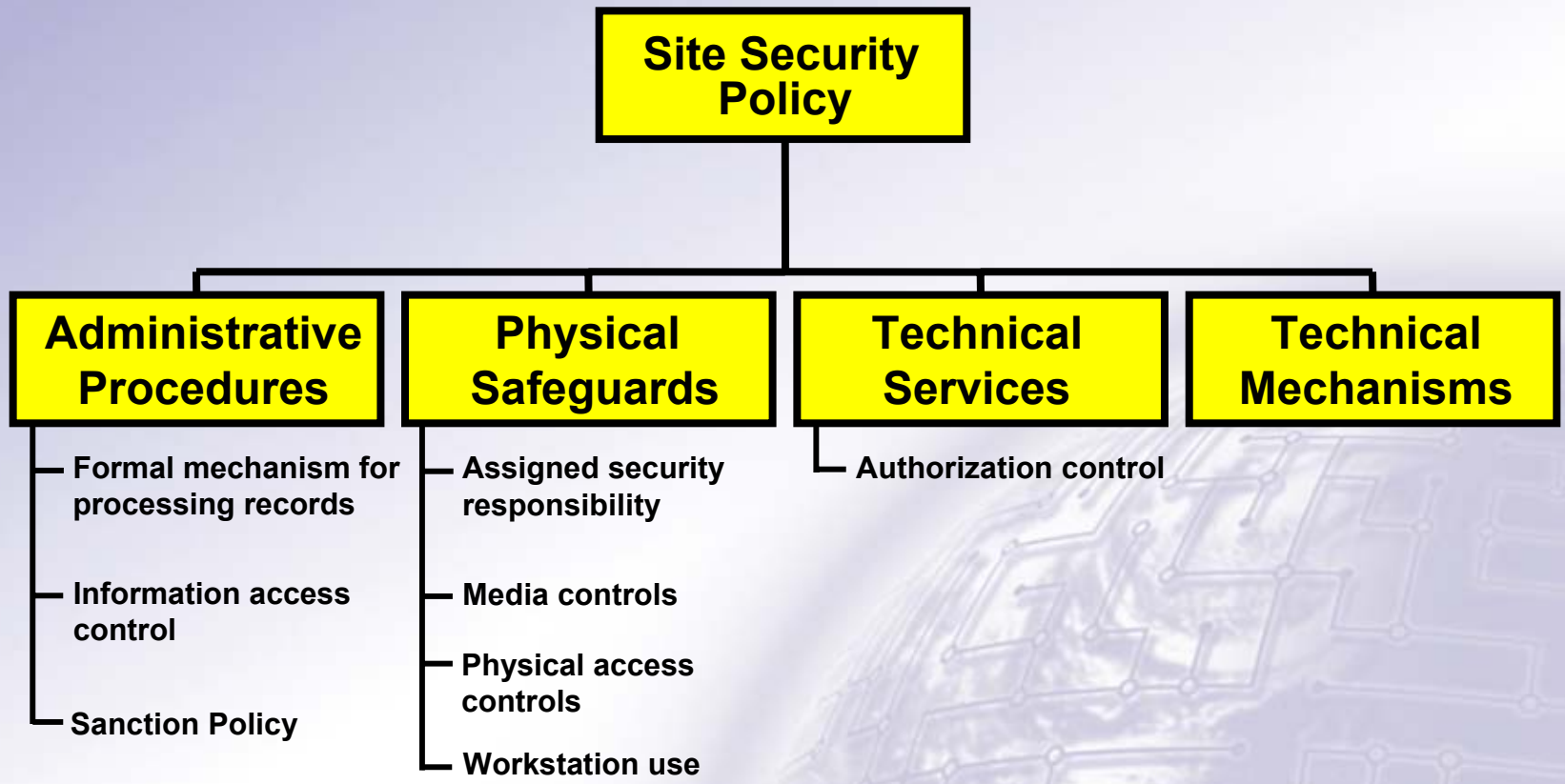
- Individual security responsibilities
- Virus protection
- Workstation Use
- Monitoring login success and failure
- Incident reporting
- Password management

Other Security Topics to Consider

ctg HealthCare Solutions

- Confidentiality, Integrity, Availability
- Sensitivity of health data
- Threats to information security
- Countermeasures (physical, technical, operational)
- Sanctions for security breaches

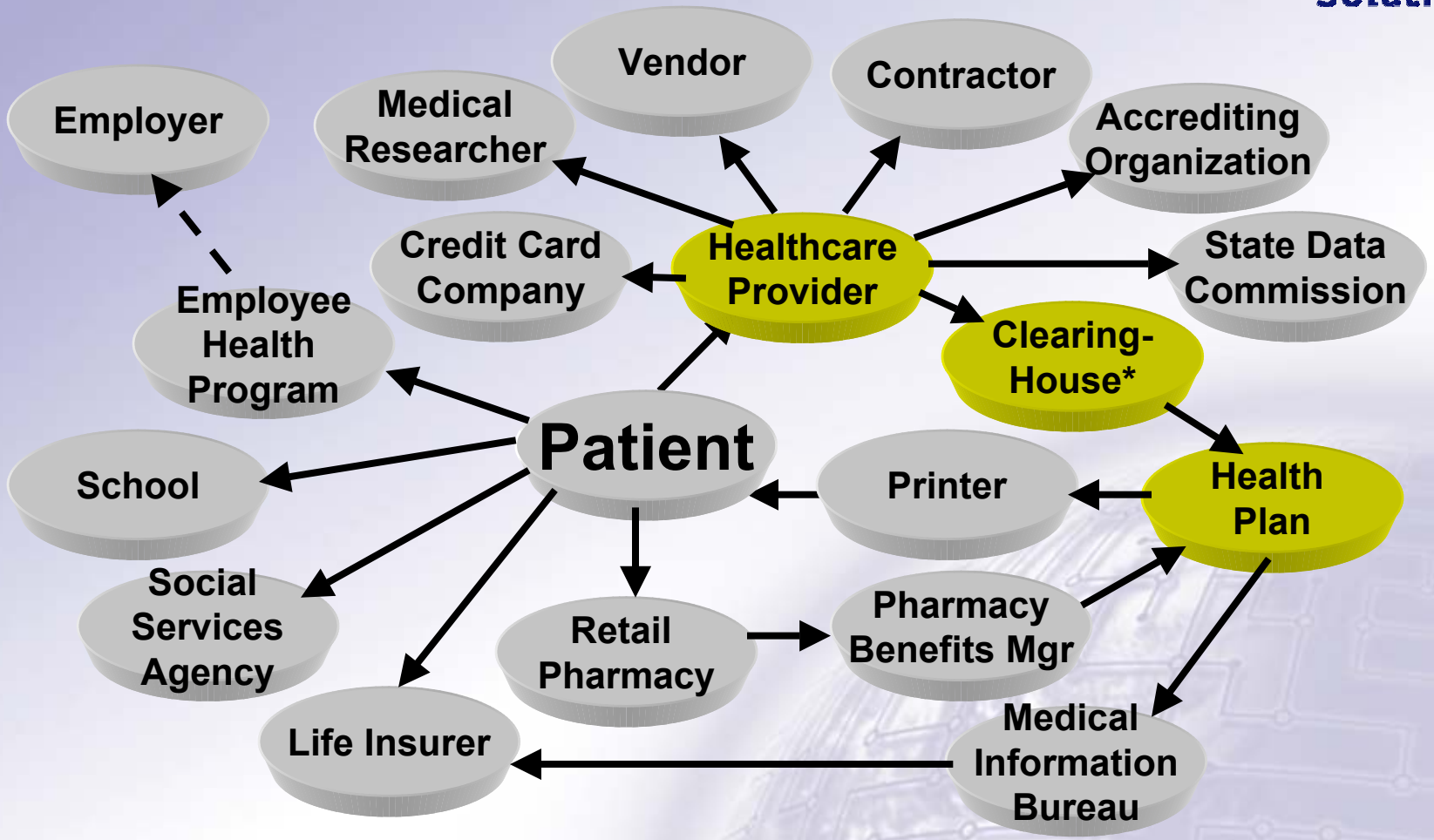
Security Policies



System Review

- Inventory of Systems (updated from Y2K)
- Data flows of all patient-identifiable information both internally and externally
- Identify system sources and sinks of patient data and associated system vendors/external business partners

Sharing Patient Information-The HIPAA Perspective



Documentation Review- "if it has been documented, it hasn't been done"!

- Policies and Procedures dealing with accessing, collecting, manipulating, disseminating, transmitting, storing, disposing of, and protecting the confidentiality of patient data both internally (e-mail) and externally
- Medical Staff By-laws
- Disaster Recovery/Business Continuity Plans

Contract Review

- Vendor responsibility for enabling HIPAA compliance both initially and with upgrades as the regulations change
- Business Associate Contracts/Chain of Trust not only with systems vendors but also with billing agents, transcription services, outsourced IT, etc.
- Confidentiality agreements with vendors who must access patient data for system installations and maintenance (pc Anywhere)

Infrastructure & Connectivity Review

- System Security Plans exist for all applications
- Hardware/Software Configuration Management/Change Control Procedures- procedures for installing security patches
- Security is one of the mandated requirements of the Systems Development Life Cycle
- Network security- firewalls, routers, servers, intrusion detection regularly tested with penetration attempts, e-mail, Internet connectivity
- E-commerce initiatives involving patient data
- PDAs

Access/Authorization Controls

- Only those with a "need to know"- principle of least privilege
- Based on user, role, or context determines level
- Must encrypt on Internet or open system
- Procedure to obtain consent to use and disclose PHI
- Physical access controls- keypads, card reader/proximity devices, escort procedures, sign-in logs

Media Controls

- Policy/Procedure for receipt and removal of hardware and software (virus checking, "foreign" software); wipe or remove PHI from systems or media prior to disposal
- Disable print capability, A drive, Read Only
- Limit e-mail distribution/Internet access
- E-fax as an alternative
- Encourage individual back-up or store on network drive/ password protect confidential files

Workstation* Use

ctg HealthCare Solutions

* (Applies to monitors, fax machines, printers, copy machines)

- Screen Savers/Automatic Log Off
- Secure location to minimize the possibility of unauthorized access to individually identifiable health information
- Install covers, anti-glare screens, or enclosures if unable to locate in a controlled access area
- Regular updates of anti-virus software

Server Checklist

- In a locked room?
- Connected to UPS?-surge protector?- regular tests conducted?
- Protected from environmental hazards?
- Are routine backups done?- how often?- where are they stored?- tested regularly?- has the server ever been restored from backup media?
- Anti-virus software running on server?
- Is access control monitored? etc., etc.

Strong Passwords (guidelines)

ctg HealthCare Solutions

- At least 6 characters in length (with at least one numeric or special character)
- Easy to remember
- Difficult to guess (by a hacker)
- Don't use personal data, words found in a dictionary, common abbreviations, team names, pet names, repeat characters
- Don't index your password each time you change it

Risk Analysis Process

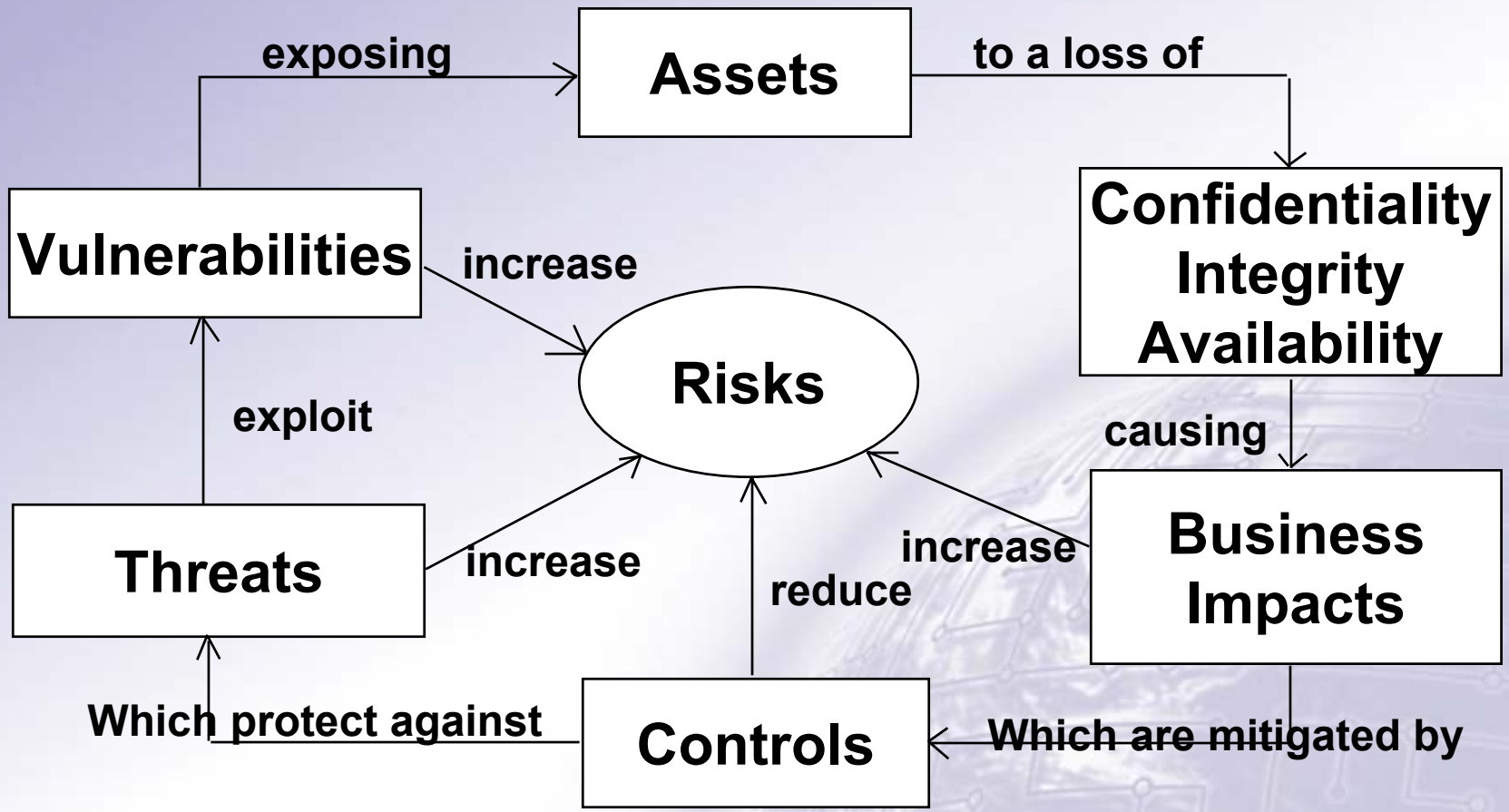
- Assets- hardware, software, data, people
- Vulnerabilities- a condition or weakness (or absence of) security procedures, physical controls, technical controls, … (the NIST Handbook)
- Threats- something that can potentially harm a system
- Risks- caused by people, processes, and practices
- Controls- policies, procedures, practices, physical access, media, technical, administrative actions that mitigate risk

Threats/Risk Mitigators

ctg HealthCare Solutions

- **Acts of Nature**
  - Some type of natural disaster; tornado, earthquake, flood, etc.- Backup/Disaster Recovery Plans/Business Continuity Plans
- **Acts of Man**
  - Unintentional - Sending a fax containing confidential information to the wrong fax machine; catching a computer virus- Policies & Procedures
  - Intentional - Abusing authorized privileges to look at patient information when there is no business "need-to-know"; hackers- Access/Authentication Controls, Audit Trails, Sanctions, Intrusion Detection

Risk Analysis Process



Source: Ken Jaworski, CISSP

Termination Procedures

- Documentation for ending access to systems when employment ends
- Policies and Procedures for changing locks, turning in hardware, software, remote access capability
- Removal from system accounts

Sanctions

- Must be spelled out
- Punishment should fit the crime
- Enforcement
- Documentation
- "Teachable Moment"- Training Opportunity

Incident Report and Handling

ctg HealthCare Solutions

Security Incident Reporting: Categorizing Incident Severity & Resolution

- Can staff identify an unauthorized use of patient information?
- Do staff know how to report security incidents?
- Will staff report an incident?
- Do those investigating security incidents know how to preserve evidence?
- Is the procedure enforced?

Business & Technology Vendors

- Billing and Management Services
- Data Aggregation Services
- Software Vendors
- Application Service Providers/Hosting Services
- Transcription Services

Vendor Questions

ctg HealthCare Solutions

- What features specifically have you incorporated into your products to support HIPAA Security and Privacy requirements; e.g., session time-outs, access controls, authorizations, backups and recovery, reporting of attempted intrusions, data integrity, audit trails, encryption algorithms, digital signatures, password changes?
- Will any of these features have an adverse impact on system performance- response time, throughput, availability?
- Are these capabilities easily upgradeable without scrapping the current system as HIPAA matures?; Will I have to pay for them or will they be part of regular maintenance?
- Are you participating in any of the national forums like WEDI SNIP, CPRI, NCHICA, etc. that are attempting to identify best practices for HIPAA compliance?

ctg HealthCare Solutions

Conclusions

Reasonableness/Common Sense

- Administrative Simplification Provisions are aimed at process improvement and saving money
- Healthcare providers and payers should not have to go broke becoming HIPAA-compliant
- Expect fine-tuning adjustments over the years

HIPAA Security Readiness Scorecard

The clock is running. What is your readiness?

Key: ✓ = Done • = In Progress

Task	Status
Designate a privacy and security officer or manager	
Communicate the privacy and security officer designation to the workforce	
Appoint a HIPAA project manager	
Appoint a cross-functional HIPAA project steering committee	
Establish HIPAA subcommittees	
Conduct a HIPAA readiness assessment	

- HIPAA Security Readiness Scorecard Doc2.doc

Remember:

ctg HealthCare Solutions

Due Diligence!

Thank You

Questions?

john.parmigiani@ctghs.com / 410-750-2497