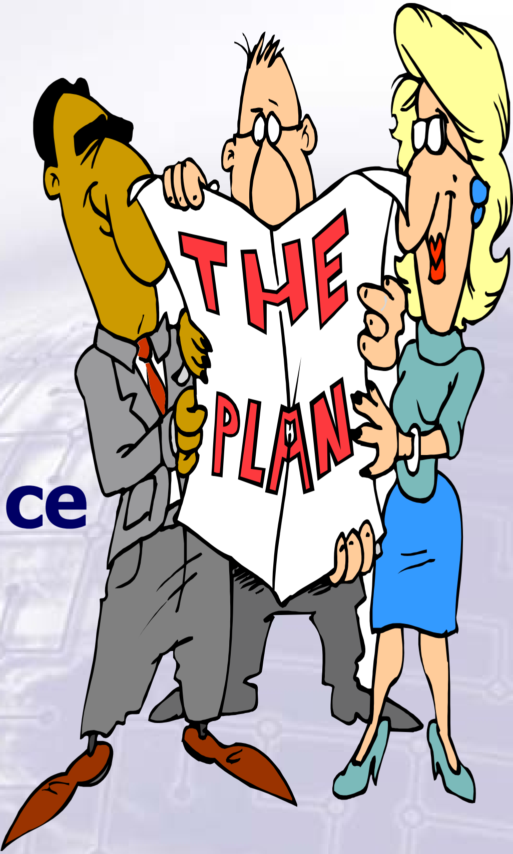
HIPAA’s Security Regulations

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

Presentation Overview

ctg HealthCare Solutions

- Introduction
- HIPAA and Privacy/Security
- Impacts and Benefits
- Steps & Tools Toward Compliance
- Conclusions



Introduction

John Parmigiani

- CTGHS National 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 Boards of *HIPAA Compliance Alert's HIPAA Answer Book* and *HIPAA Training Line;* Chair,*HIPAA-Watch* Advisory Board; *Train for HIPAA* Advisory Board

HIPAA and Privacy/Security

Title II: Subtitle F Administrative Simplification

- 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

- 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”

Privacy vs. Confidentiality vs. Security

ctg HealthCare Solutions

Privacy - information about one person

"A right"

Confidentiality - keeping private information shared with a second person a secret

"A condition"…and a responsibility

Security - controls used to protect confidential information from unauthorized people

"A safeguard"

Privacy vs. Confidentiality vs. Security

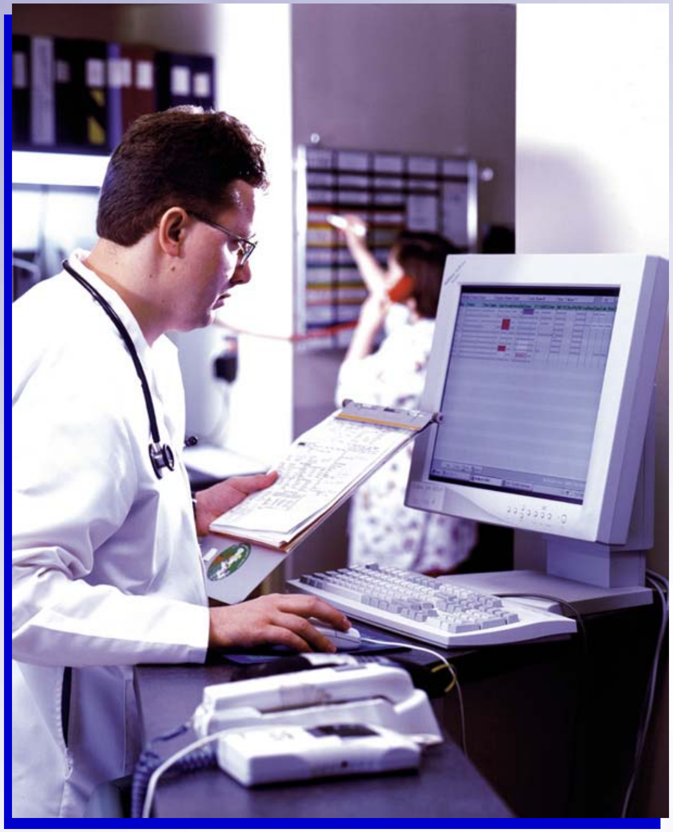
If __SECURITY__ fails,

a breach of __CONFIDENTIALITY__ occurs,

and __PRIVACY__ of the individual is breached.

Protecting Confidential Information

ctg HealthCare Solutions



Providing patients with quality healthcare also includes protecting their confidential information.

Security – The Privacy Rule

ctg HealthCare Solutions

- 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)]

"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!

Final Privacy vs. Security

ctg HealthCare Solutions

"There should be no potential for conflict between the safeguards required by the Privacy Rule and the final Security Rule… First, while the Privacy Rule applies to protected health information in all forms, the Security Rule will apply only to electronic health information systems that maintain or transmit individually identifiable health information. Thus, all safeguards for protected health information in oral, written, or other non-electronic forms will be unaffected by the Security Rule."

Therefore, PHI in both electronic and paper formats must be secure !!

Privacy Rule vs. Security Rule

Privacy Standard

- Minimum use- payment & operations, not treatment
- Notice of Privacy Practices/Designated Record Set
- Incidental use and disclosure if and only if…
- Verification of requestor
- Sanctions
- Business Associate Contracts

Security Requirement

- Access control
- Authentication
- Network Controls
- Training
- Reasonable safeguards
- Workstation controls: use; location (physical and technical)
- Authentication/ Authorization
- Audit trails
- Chain-of-Trust Agreements

Impacts & Benefits

HIPAA Security Framework

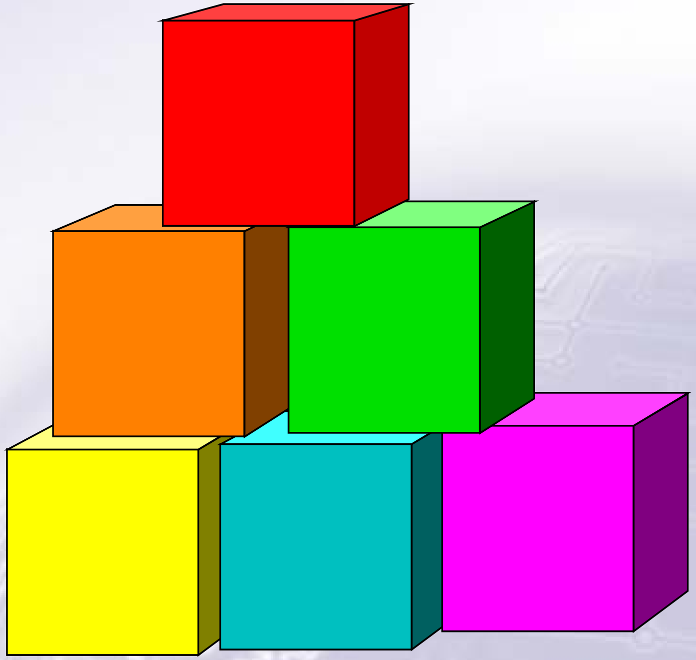
Flexible - Scalable - Technology Neutral

- Are based upon good business practices
- Tell you *What to do* not *How to do it*
- Each affected entity
  - Must assess own security needs and risks and
  - Devise, implement, and maintain appropriate security to address business requirements

Security Goals

- **Confidentiality**
- **Integrity**
- **Availability**

of protected health information



BS 7799/ISO 17799

- 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 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**

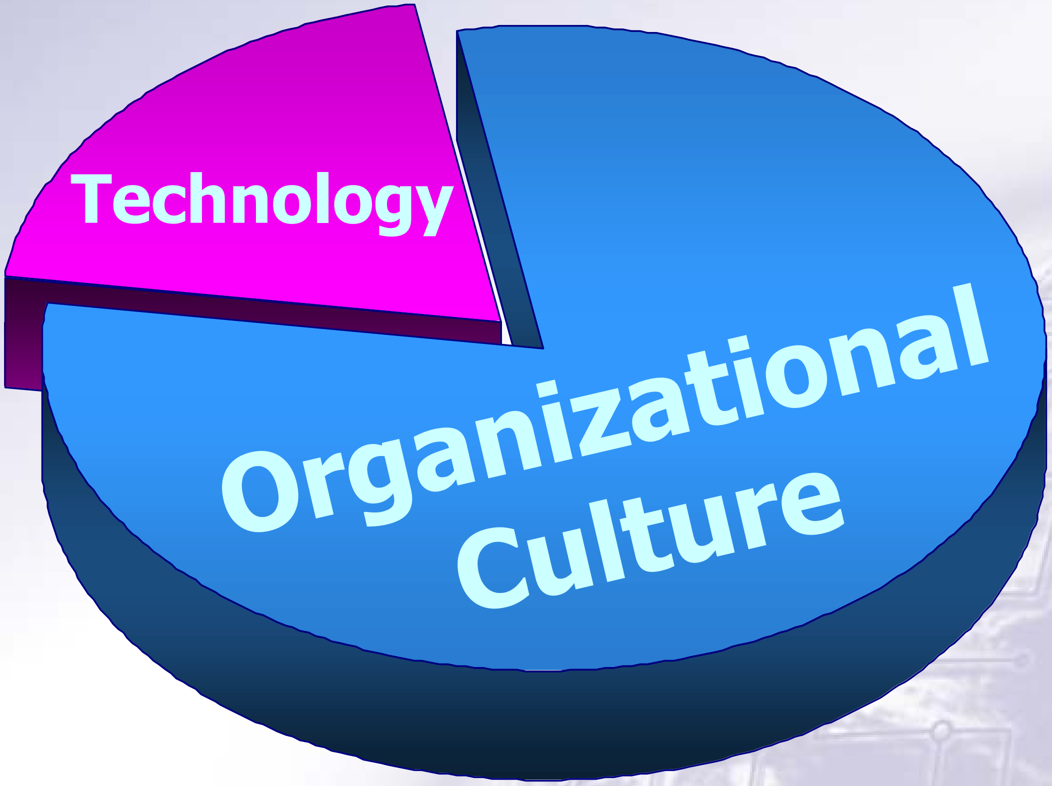
Security Standards

can be grouped into four categories:

- **Administrative safeguards** -comprehensive security policies and procedures; security training
- **Physical safeguards** -data integrity, backup, access, workstation location
- **Technical security services** -measures to protect patient information and control individual access to such information when it is at rest
- **Technical security mechanisms** -security measures to guard against unauthorized access to data when it is transit

HIPAA = Culture Change

Organizational culture will have a greater impact on security than technology.



Security Standards

- 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.

Consequences of Inadequate Security

ctg HealthCare Solutions

<u>Violation of patient privacy may result in</u>:

- **Civil Lawsuit**

  Financial loss

- **Criminal Penalties**

  Fines and prison time

- **Reputation**

  Lack of confidence and trust

Or Worse…

A breach in security could damage your organization’s reputation and continued viability.

“There is a news crew from *60 Minutes* in the lobby. They want to speak to to you about an incident that violated a patient’s privacy.”

Steps & Tools Toward Compliance

Steps Toward Compliance…

- Establish good security practices
- Train the workforce
- Update policies and procedures
- Make sure your business associates and vendors help enable your compliance efforts

Administrative Procedures Checklist

- Contracts with every business partner who processes PHI (Confidentiality)
- Contingency Plans (Availability/Integrity)
- Written Policies regarding routine and non-routine handling of PHI (Confidentiality)
- Audit logs and reports of system access (Confidentiality)
- Information Systems Security Officer

Administrative Procedures Checklist…

ctg HealthCare Solutions

- HR policies re security clearances, sanctions, terminations (Confidentiality)
- Security Training (Confidentiality)
- Security Plans for each system-all phases of SDLC; periodic recertification of requirements (Confidentiality/Integrity/Availability)
- Risk Management (*Risk Analysis*) Process (Confidentiality/Integrity/Availability)
- Security Incident reporting process (Confidentiality)

Physical Security Safeguards Checklist

- Policies and Procedures regarding data, software, hardware into and out of facilities (Integrity/Confidentiality/Availability)
- Physical access limitations- equipment, visitors, maintenance personnel (Confidentiality)
- Secure computer room/data center (Confidentiality)

Physical Security Safeguards Checklist…

- Workstation policies and procedures (Confidentiality)
- Workstation location to isolate PHI from unauthorized view/use (Confidentiality)

Technical Security Services (data @ rest) Checklist

CTG HealthCare Solutions

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

Technical Security Mechanisms (data in transit) Checklist

- VPN or Internet; Intranet/Extranet (Confidentiality/Integrity/Availability)
- Closed or Open System (Confidentiality/Integrity)
- Encryption Capabilities (Confidentiality/Integrity)
- Alarm features to signal abnormal activity or conditions- event reporting (Confidentiality/Integrity/Availability)

Technical Security Mechanisms (data in transit) Checklist…

- Audit trails (Confidentiality)
- Determine that the message is intact, authorized senders and recipients, went through unimpeded (Integrity)
- Messages that transmission signaling completion and/or operational irregularities (Integrity/Availability)

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

New Security Practices Required

- Media Controls
- Automatic Logoff
- Personnel Security Practices
  - Clearances
  - Terminations
- Technical Security Policies
  - Protection of Data at Rest
  - Data in Transmission

Existing Practices to Evaluate

- Trash/Recycle/Shred
- Unattended Computers
- Wireless Technology
- E-Mail

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

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

ctg HealthCare Solutions

- 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

Web - Hype Vs. Reality

- Sandra Bullock - “The Net”

- What is the *real* threat?

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

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

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?**

Steps Toward Compliance…

- Identify Business Associates
  - Query department directors
  - Compare against contracts file
  - Compare information against accounts payable files

- Develop Business Associate Contract (BAC) language, then negotiate BACs

Business & Technology Vendors

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

Vendor/Covered Entities Issues

- New risks for both sides
- Vendor cannot make a Covered Entity "HIPAA Compliant"
- Only Covered Entities and Business Associates can be HIPAA compliant
- HIPAA Security compliance is a combination of business process + human interaction + technology
- Vendors may ask for indemnification if covered entities do not implement systems completely to utilize all "features"

Vendor Questions

- 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?

Vendor Questions

- Virus checks each time a PDA is synchronized with a laptop or desktop to avoid transmitting garbled information, missed appointments, faulty diagnoses, erroneous prescriptions…; authenticating access; encryption to guard against intercepts
- Encryption software updates as the technology develops
- Smart card or biometrics to log on and access files and information on PDAs, desktops, and laptops

Vendor Questions

- Will any of these features have an adverse impact on system performance- response time, throughput, availability?

Vendor Questions

- 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?

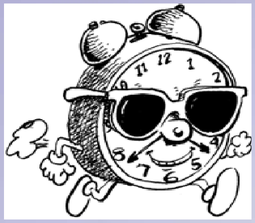
Vendor Questions

- 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?

Vendors

- Vendors cannot make you HIPAA-compliant- will "enable"
- You need to be an informed buyer
- Create a business associate contract that is favorable to you
- HIPAA will be continuously fine-tuned- build growth potential in your systems at no or minimal cost

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 Doc3.doc

Conclusions

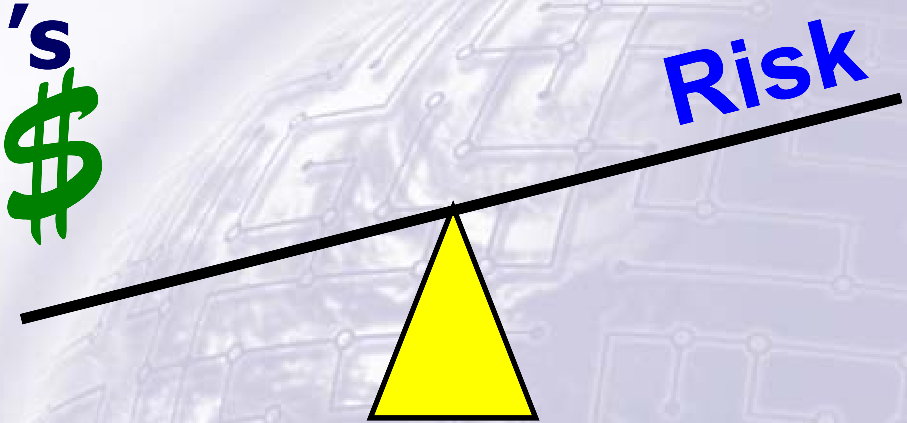
Reasonableness/Common Sense

ctg HealthCare Solutions

- 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

A Balanced Approach

- Cost of safeguards vs. the value of the information to protect
- Security should not impede care
- Security and Privacy are inextricably linked
- Your organization's risk aversion



Remember:

Due Diligence!

Thank You

ctg HealthCare Solutions

Questions?

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