



# Advanced Issues in HIPAA Privacy & Security Compliance Monitoring

- Planning
- Practicing
- Promoting

Connie Emery

VP Compliance, Information Privacy/Security Officer

Andrew Vezina

Manager Information Privacy/Security

Tenet Headquarters, Dallas Texas

April 7, 2005



TENET COMPLIANCE

# Planning



# Risk Assessment

- What is the objective?
- What are the risks?
- What is the population?
- What is the ranking criteria?



# What is the Objective?

- To verify that policies and procedures are being followed.
- To verify that controls are working.
- To identify opportunities for improvement and develop training to address identified issues.
- To ensure compliance with laws (federal and state) such as Sarbanes/Oxley (SOX), SB1386, HIPAA.



# Speaking of Laws

- SOX – Section 404: Management Assessment of Internal Controls.
- SB1386 – Section 1798.2 CA Civil Code
- HIPAA – Privacy 45 CFR 164.500-534; Security 45 CFR 164.302-318
- Others – ???



# What are the Risks?

The possibility that an event will occur that will Adversely affect the achievement of objectives.

Privacy/Security Risks (very broad categories):

- Inappropriate use/disclosure of Protected Health Information
- Inappropriate use/disclosure of Company Information
- Issues related to Information Confidentiality
- Issues related to Information Availability
- Issues related to Information Integrity



# What is the Population?

Different for each organization:

- One hospital organization – departments
- Small hospital organization – hospital entities, non-hospital entities, corporate entities
- Large hospital organization – hospital entities, non-hospital entities, corporate entities, division entities, region entities, business offices, health plans



# How do you rank the risk?

Steps to setting up the risk ranking tool:

- Complete an Inventory
- Identify ranking categories
- Identify scoring criteria





# Complete an Inventory

## 1. Covered entities

- Hospitals
- Non-hospital entities
- Health plans

## 2. Supporting business units

- Business and billing offices
- Corporate and regional offices
- Collection offices
- Call centers



# Identify Ranking Categories

- # Non-Hospital Entities (NHEs)
- # Beds
- Date Prior Visit
- # HIPAA Incidents
- Outsourced IS
- Mgmt Change
- System Change
- Regional Compliance Input
- Regional HIM Input
- POC Input
- Prior Scan Score



# Identify Scoring Criteria

## (Objective/Subjective)

|                      |  |
|----------------------|--|
| # NHEs:              | +10 = 3; 9-5 = 2; 4-0 = 1  |
| # Beds:              | +400 = 3; 399-200 = 2; 199-0 = 1                                   |
| Date Prior Visit:    | Pre 04/03 = 3; Post 04/03 = 2; '04 = 1                             |
| # HIPAA Incidents:   | < 20 = 3; 21-60 = 2; +61 = 1                                       |
| Outsourced IS:       | Yes = 2; No = 1  |
| Mgmt Change:         | Yes = 2; No = 1  |
| System Change:       | Yes = 2; No = 1  |
| Regional Comp Input: | 10-7 = 3; 6-4 = 2; 3-0 = 1   |
| Regional HIM Input:  | 10-7 = 3; 6-4 = 2; 3-0 = 1   |
| POC Input:           | 10-7 = 3; 6-4 = 2; 3-0 = 1   |
| Prior Scan Score:    | No Controls = 3; Controls not Followed = 2; Controls Effective = 1 |



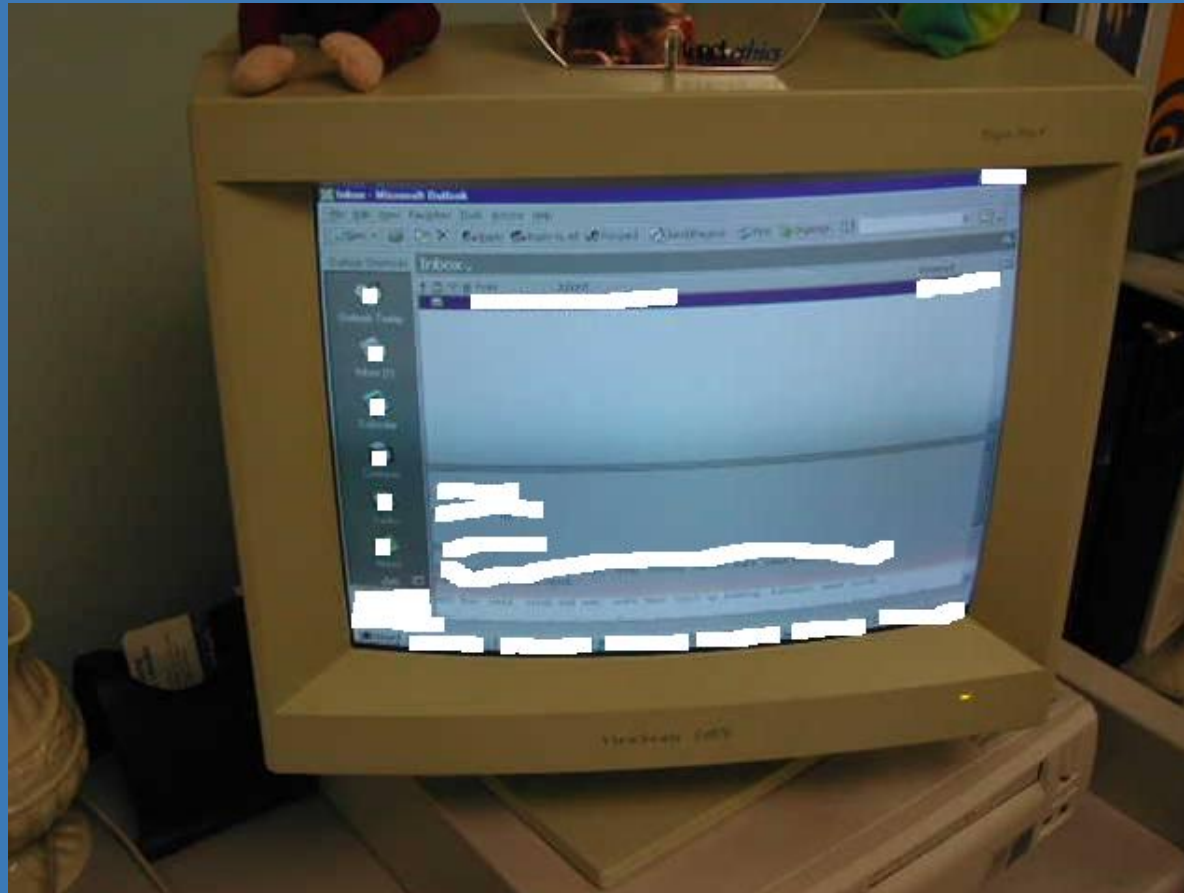
TENET COMPLIANCE

# Where is the Cut Line?

- Highest Score Possible = 30
- Number of Major Locations = 120
- Number of Locations Scoring  $> 25 = 36$
- Staff Size = 4
- Review Alternatives: Remote Scans;  
Assistance from HCOs and HIM Personnel



# Practicing



# Privacy/Security Team – What We Do

- Collect, monitor, and assist in responding to privacy/security incidents.
- Maintain privacy/security policies and procedures.
- Maintain privacy/security training content and monitor compliance with training initiatives.
- Perform on-site privacy/security vulnerability assessments at Tenet's covered entities and business units (+450).
- Perform remote monitoring of network security at Tenet's covered entities and business units.
- Work with Corporate IS to identify privacy/security risks associated with new applications and operating systems.



TENET COMPLIANCE

# The Review Process

- Technical

- Vulnerability Scan of Network Connectivity.
- War Dialing of Phone System.
- User Access Review of Systems/Applications.
- Password Auditing
- Wireless Scanning

- Administrative

- After-hours Walkthrough
- Random Staff Interviews



TENET COMPLIANCE

# Recurring Issues – Technical

- User Access Issues.
- Password Control Issues.
- Enabled Network Services (FTP, Telnet, HTTP, SNMP, etc.).
- Open Ports, Virus/Trojan Vulnerabilities.
- Audit logging – not enabled/reviewed.
- Unsecured Modem Connectivity.





# Recurring Issues – Administrative

- Unlocked Doors.
- PCs Left Logged On.
- Posted Passwords.
- “Dumpster Diving”.
- Access to PHI.
- Other Privacy/Security Risks.
- Does Anyone Ask What We’re Doing?



# PROMOTING

Privacy / Security - Default - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://secure.etenet.com/Departments/Compliance/PrivacySecurity/> Go Links

eTenet Hospital More Tenet Sites Connie's Page

Tenet Compliance

Search New Search Engine! Go

More Search Options

HR & Benefits | Departments | Policies & Procedures | Tools & Applications | Education & Training | Tenet Initiatives | News

Welcome, **Connie Emery** [Log Out](#) (If this is not you, please log out.)

[Dept Home](#)

[Who We Are](#)


[What We Do](#)

[Org Chart](#)

[Policies & Procedures](#)

[Compliance](#)

[Guidelines](#)



**CONNIE EMERY**  
Privacy/Security Officer

### What's New

- ▶ [Revised 2003-04 Site Visit Schedule](#)
- ▶ [HIPAA Training Forms](#)
- ▶ [Translated NPPs and Acknowledgement Forms](#)
- ▶ [Non-Hospital NPPs and Acknowledgment Form](#)

### Privacy & Security Compliance Topics

- ▶ [HIPAA Training](#)
- ▶ [HIPAA FAQ Corner](#)
- ▶ [Privacy](#)
  - ▶ [Privacy Policies and Procedures](#)
- ▶ [Security](#)
  - ▶ [Security Policies and Procedures](#)
- ▶ [Privacy Officer List](#)
- ▶ [Privacy/Security Vulnerability Review](#)
- ▶ [HIPAA Heroes](#)
- ▶ [HIPAA Home Page](#) (maintained by Information Systems)
- ▶ [Records Management Policy](#) (maintained by Administration)
- ▶ [Privacy-Security Presentation](#) (14,442 kb PPT)\*\*

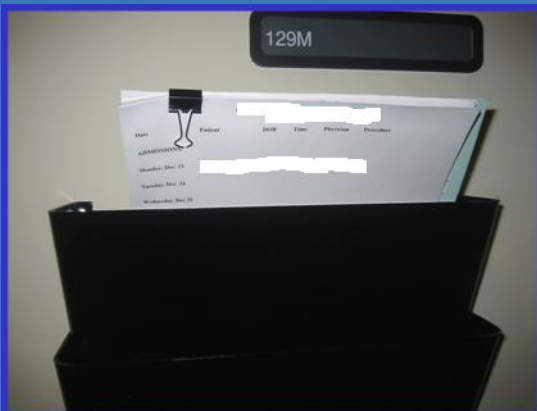
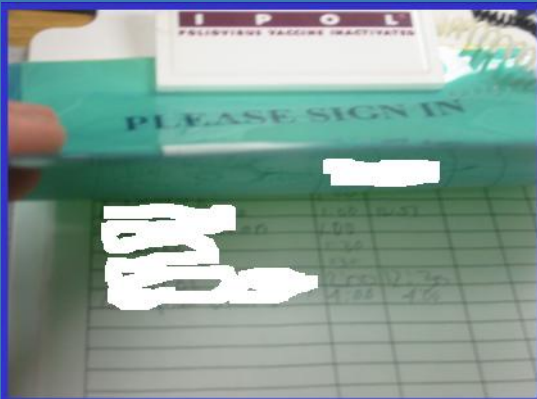
\*\* If you have problems opening this presentation in your browser, please right click on the link, click 'Save Target As' and save the file to your computer.

Internet

# A Picture's Worth..... Unlocked Doors



# A Picture's Worth..... Access to PHI



# A Picture's Worth..... Computers Left Logged On



# A Picture's Worth..... Passwords Posted



TENET COMPLIANCE

# A Picture's Worth..... Dumpster Diving



# A Picture's Worth..... Other Security Issues





# Incident Reporting

- Disposal/Display Issues
- Opt Out Issues
- Policy Issues
- Transmission Issues
- Extreme Issues
- NA Issues



# Questions?



**Connie R. Emery, CPA, CISA, CISSP, CIPP**  
Vice President and Privacy/Security Officer  
Compliance, Information Privacy & Security

**Tenet Healthcare Corporation**  
Headquarters Office  
13737 Noel Road, Suite 100  
Dallas, TX 75240  
Tel: 469.893.6709  
Cell: 214.280.6605  
Fax: 469.893.7709  
email: [connie.emery@tenethealth.com](mailto:connie.emery@tenethealth.com)  
[www.tenethealth.com](http://www.tenethealth.com)

Mailing Address: P.O. Box 809088 • Dallas, TX 75380-9088



**Andrew M. Vezina, CISSP, CISA**  
Manager, Information Privacy & Security  
Compliance, Information Privacy & Security

**Tenet Healthcare Corporation**  
Headquarters Office  
13737 Noel Road, Suite 100  
Dallas, TX 75240  
Tel: 469.893.2322  
Cell: 214.226.0352  
Fax: 469.893.3322  
email: [andrew.vezina@tenethealth.com](mailto:andrew.vezina@tenethealth.com)  
[www.tenethealth.com](http://www.tenethealth.com)

Mailing Address: P.O. Box 809088 • Dallas, TX 75380-9088



TENET COMPLIANCE



TENET COMPLIANCE