Monitoring & Auditing HIPAA Compliance

Donald A. Sinko,
Chief Integrity Officer

Vicki R. Bokar,
Sr. Director Corporate Compliance
Cleveland Clinic

March 29, 2017

Agenda

- Overview of Cleveland Clinic Health System and Compliance structure
- Where HIPAA fit into our Compliance Program
- Where adjustments were needed
- Effectively auditing and monitoring for HIPAA compliance

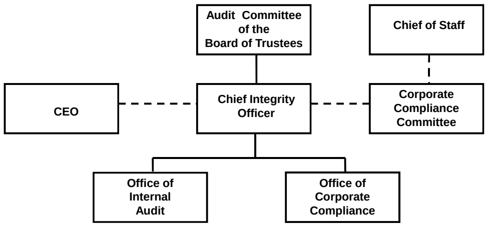
About Cleveland Clinic

- 7.1M Outpatient Visits
- 161,664 Acute Admissions
- 3,584 Physicians & Scientists
- 51,487 Employed Caregivers
- 28.5M sq. ft. Facility Space
- 10 Regional Hospitals
- 150+ Northern Ohio Outpatient Locations
- Staff physicians are salaried; on one year contracts

National & International Locations

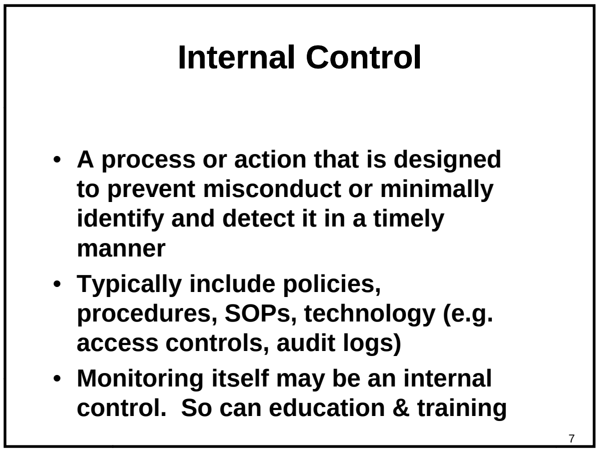
- Canada – Executive Health, Sports Health and Rehabilitation
- Nevada – Lou Ruvo Center for Brain Health, Glickman Urological & Kidney Institute
- Florida – Integrated Medical Campus in Weston; Outpatient Locations in West Palm Beach
- Abu Dhabi - Partnership with Mubadala Development Co.
- London – In Progress

Integrity Office Reporting Lines


Audit Committee of the Board of Trustees
Chief of Staff
CEO
Chief Integrity Officer
Corporate Compliance Committee
Office of Internal Audit
Office of Corporate Compliance

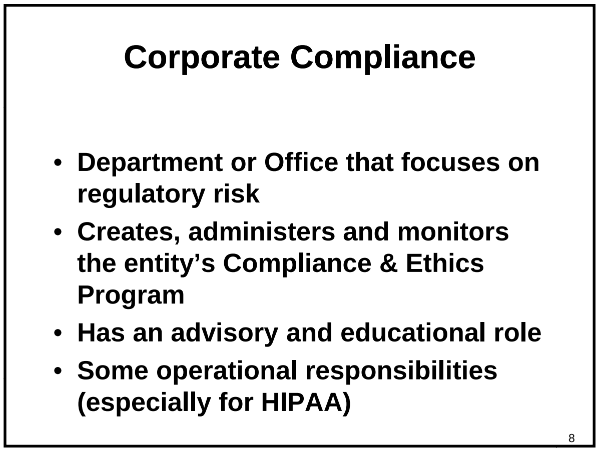
Internal Audit

- Focuses on all risks to the organization (not just regulatory risks)
- Tests effectiveness of new or existing internal controls, including those that affect the compliance program
- Audit work is formerly governed by professional audit standards
- Typically does not have operational responsibilities



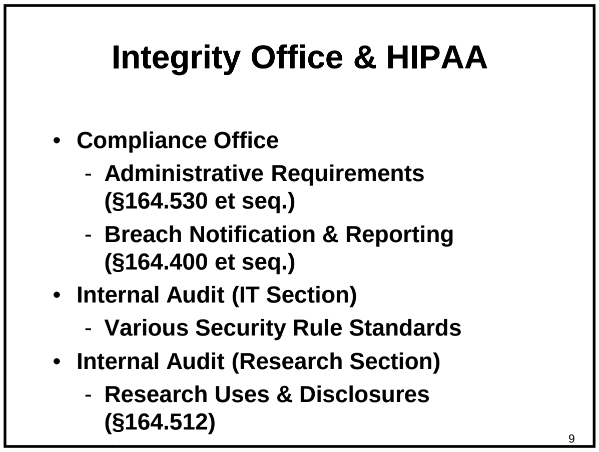
Internal Control

- A process or action that is designed to prevent misconduct or minimally identify and detect it in a timely manner
- Typically include policies, procedures, SOPs, technology (e.g. access controls, audit logs)
- Monitoring itself may be an internal control. So can education & training



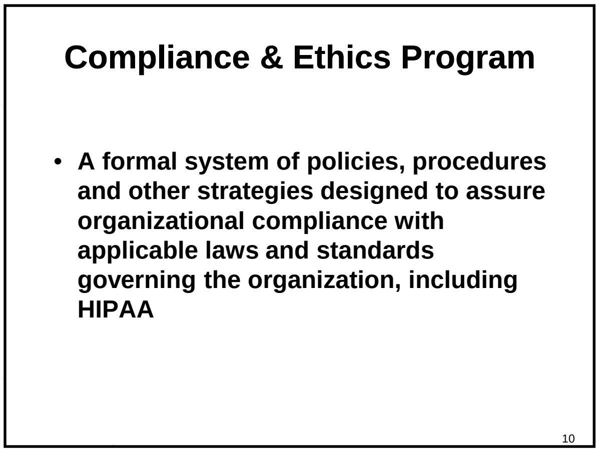
Corporate Compliance

- Department or Office that focuses on regulatory risk
- Creates, administers and monitors the entity’s Compliance & Ethics Program
- Has an advisory and educational role
- Some operational responsibilities (especially for HIPAA)



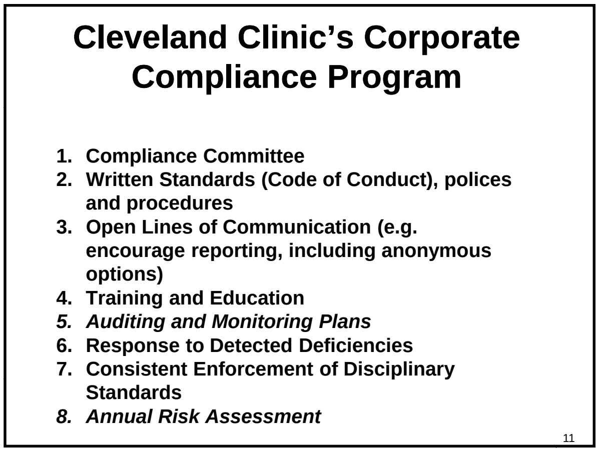
Integrity Office & HIPAA

- Compliance Office
  - Administrative Requirements (§164.530 et seq.)
  - Breach Notification & Reporting (§164.400 et seq.)
- Internal Audit (IT Section)
  - Various Security Rule Standards
- Internal Audit (Research Section)
  - Research Uses & Disclosures (§164.512)



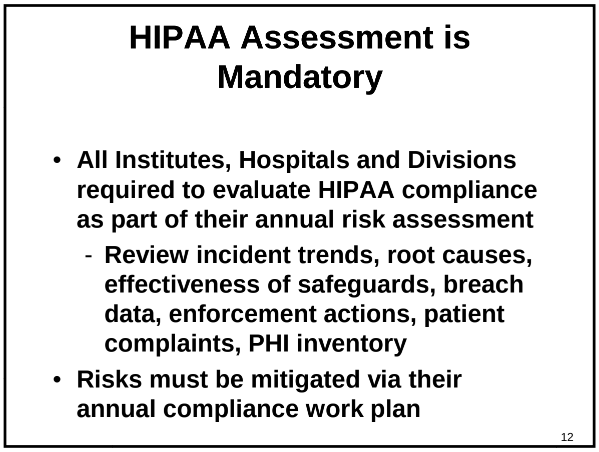
Compliance & Ethics Program

- A formal system of policies, procedures and other strategies designed to assure organizational compliance with applicable laws and standards governing the organization, including HIPAA



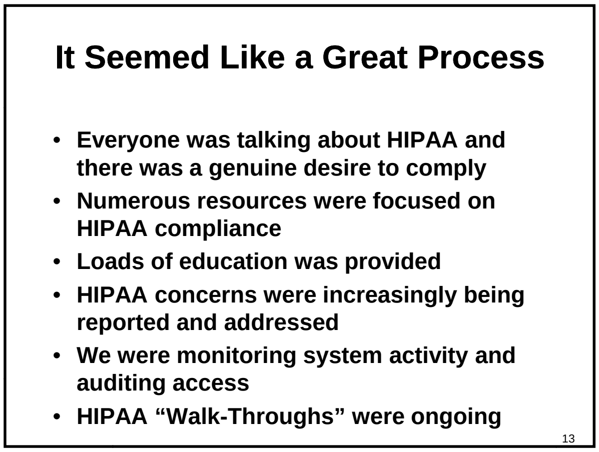
Cleveland Clinic’s Corporate Compliance Program

1. Compliance Committee
2. Written Standards (Code of Conduct), polices and procedures
3. Open Lines of Communication (e.g. encourage reporting, including anonymous options)
4. Training and Education
5. *Auditing and Monitoring Plans*
6. Response to Detected Deficiencies
7. Consistent Enforcement of Disciplinary Standards
8. *Annual Risk Assessment*



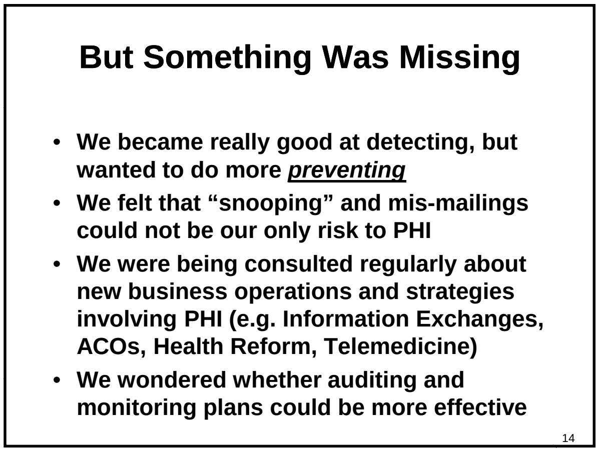
HIPAA Assessment is Mandatory

- All Institutes, Hospitals and Divisions required to evaluate HIPAA compliance as part of their annual risk assessment
  - Review incident trends, root causes, effectiveness of safeguards, breach data, enforcement actions, patient complaints, PHI inventory
- Risks must be mitigated via their annual compliance work plan



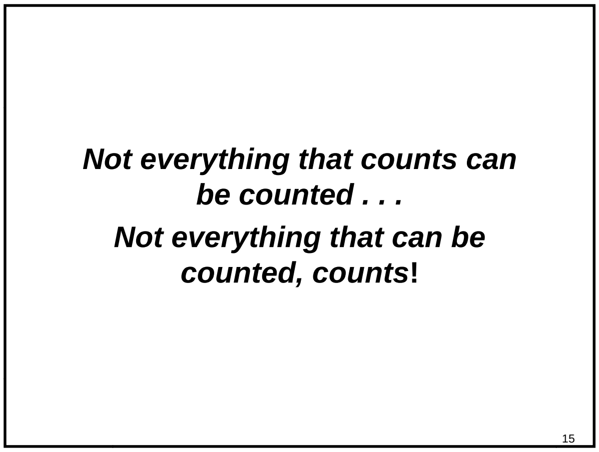
It Seemed Like a Great Process

- Everyone was talking about HIPAA and there was a genuine desire to comply
- Numerous resources were focused on HIPAA compliance
- Loads of education was provided
- HIPAA concerns were increasingly being reported and addressed
- We were monitoring system activity and auditing access
- HIPAA "Walk-Throughs" were ongoing



But Something Was Missing

- We became really good at detecting, but wanted to do more ***preventing***
- We felt that "snooping" and mis-mailings could not be our only risk to PHI
- We were being consulted regularly about new business operations and strategies involving PHI (e.g. Information Exchanges, ACOs, Health Reform, Telemedicine)
- We wondered whether auditing and monitoring plans could be more effective



Not everything that counts can be counted . . .

***Not everything that can be counted, counts*!**

An Important Clue

- “Compliance” & “Audit” have multiple meanings
- “Compliance” can also refer to the entity’s responsibility to comply with laws, regulations, an employee’s conduct or a patient’s adherence
- Audit is not just a department or office. “Audit” can refer to system activity logs, access reports, simple chart reviews, or a government audit
- We needed to educate our people

16

Auditing

- Usually retrospective and limited in time and scope
- Typically performed by independent party (internal or external auditors)
- Reviews compliance against a set of standards, such as statutes and regulations or internal policies, used as base measures
- Validates the effectiveness of policies, procedures and other controls in reducing risk

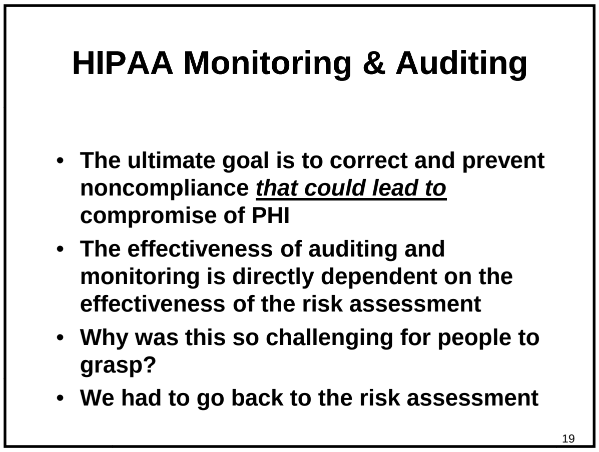
17

Monitoring

- Monitoring is an ongoing daily event which includes conducting analyses and tracking trends to correct issues in “real time” at the lowest level of detection
- It occurs during regular operations as a check to see if procedures are working

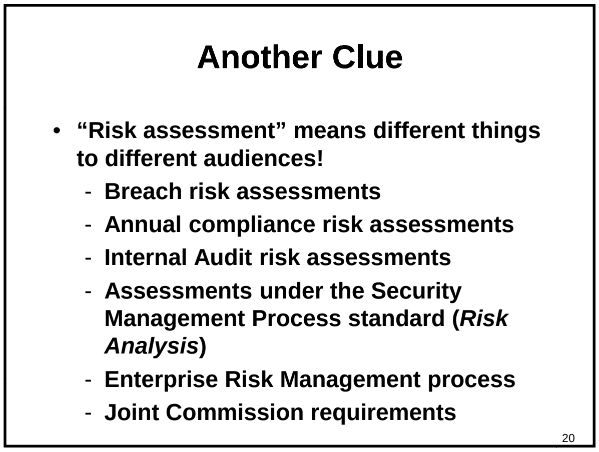
(Abridged CMS Definition)

18



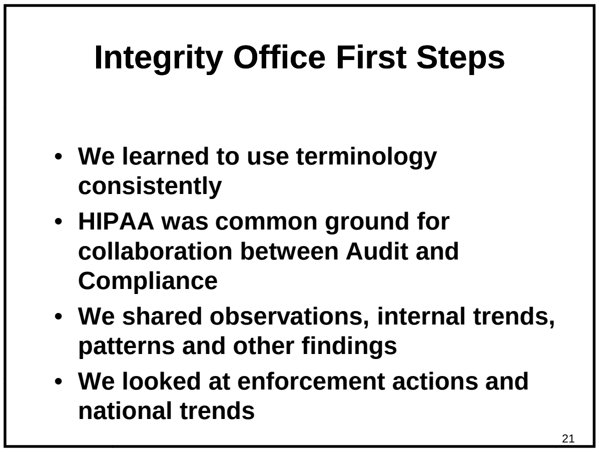
HIPAA Monitoring & Auditing

- The ultimate goal is to correct and prevent noncompliance ***<u>that could lead to</u>*** compromise of PHI
- The effectiveness of auditing and monitoring is directly dependent on the effectiveness of the risk assessment
- Why was this so challenging for people to grasp?
- We had to go back to the risk assessment



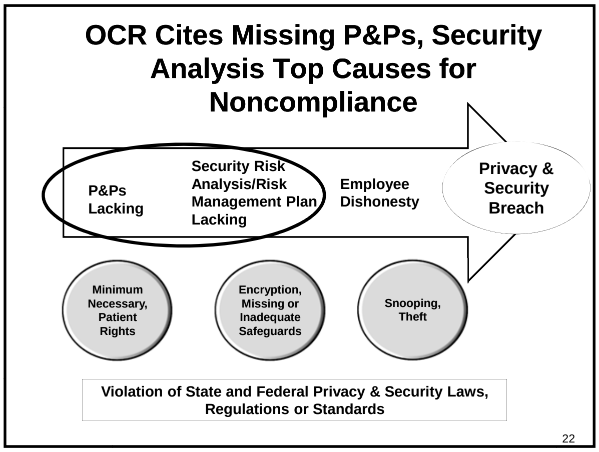
Another Clue

- "Risk assessment" means different things to different audiences!
  - Breach risk assessments
  - Annual compliance risk assessments
  - Internal Audit risk assessments
  - Assessments under the Security Management Process standard (*Risk Analysis*)
  - Enterprise Risk Management process
  - Joint Commission requirements



Integrity Office First Steps

- We learned to use terminology consistently
- HIPAA was common ground for collaboration between Audit and Compliance
- We shared observations, internal trends, patterns and other findings
- We looked at enforcement actions and national trends



OCR Cites Missing P&Ps, Security Analysis Top Causes for Noncompliance

P&Ps Lacking

Security Risk Analysis/Risk Management Plan Lacking

Employee Dishonesty

Privacy & Security Breach

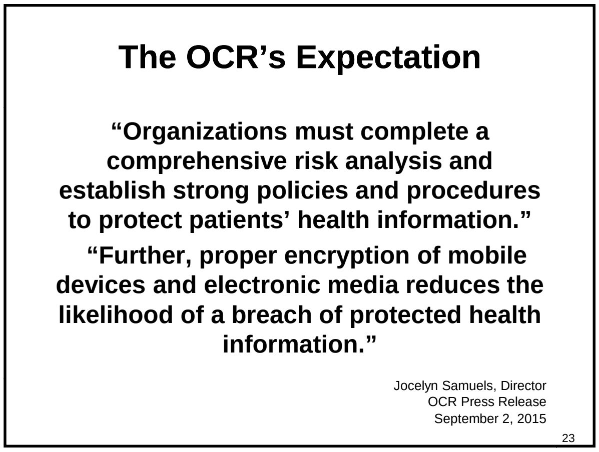
Minimum Necessary, Patient Rights

Encryption, Missing or Inadequate Safeguards

Snooping, Theft

Violation of State and Federal Privacy & Security Laws, Regulations or Standards

22



The OCR's Expectation

"Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients' health information."

"Further, proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information."

Jocelyn Samuels, Director
OCR Press Release
September 2, 2015

23

We Partnered with IT Security

- The Information Technology's Security Department was a trusted advisor to both Audit and Compliance on individual projects and investigations
- We relied on their constant vigilance and they relied on our support
- We looked at our own auditing and monitoring activities

24

We Focused on Existing Silos

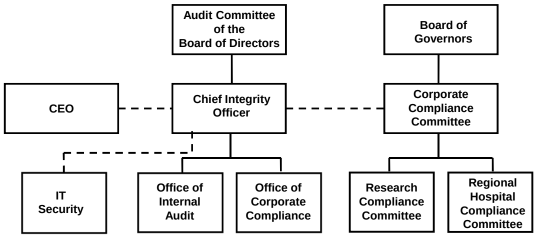
- Risk-driven (IA Risk Assessment)
- Event-driven

- Risk –driven (Compliance Risk Assessment)
- Complaint-driven
- Reported Events

- Based on Security Risk Analysis
- Policy-driven
- Event-driven

25

Removing Silos Improved Effectiveness



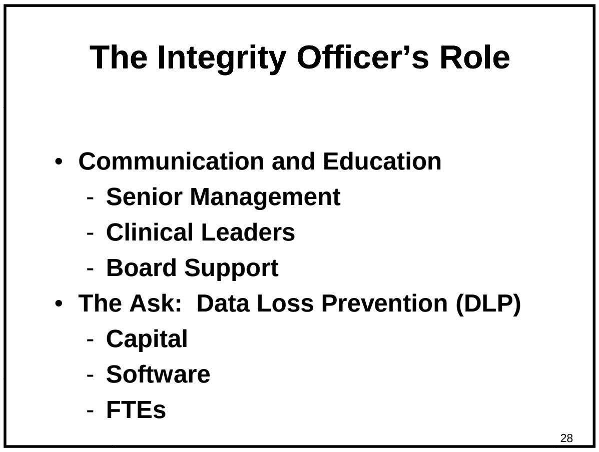
Audit Committee of the Board of Directors
Board of Governors
CEO
Chief Integrity Officer
Corporate Compliance Committee
IT Security
Office of Internal Audit
Office of Corporate Compliance
Research Compliance Committee
Regional Hospital Compliance Committee

26

We Did More Homework

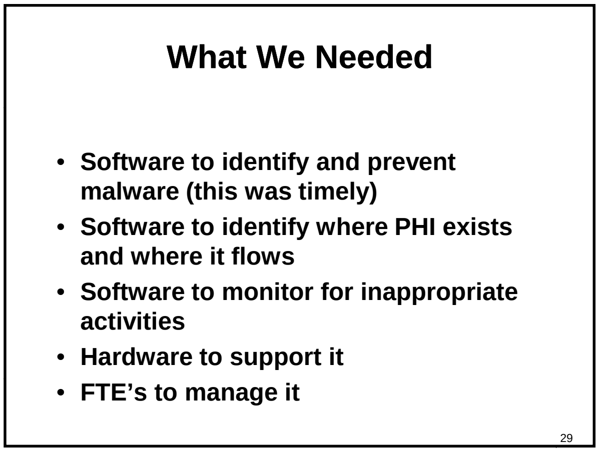
- We studied our own data (investigation trends, root causes, audit findings, security incidents etc.)
- We identified and prioritized our top risks
- We identified technological solutions that could facilitate more effective prevention and detection across the organization
- We came up with a compelling business case for the Senior Management

27



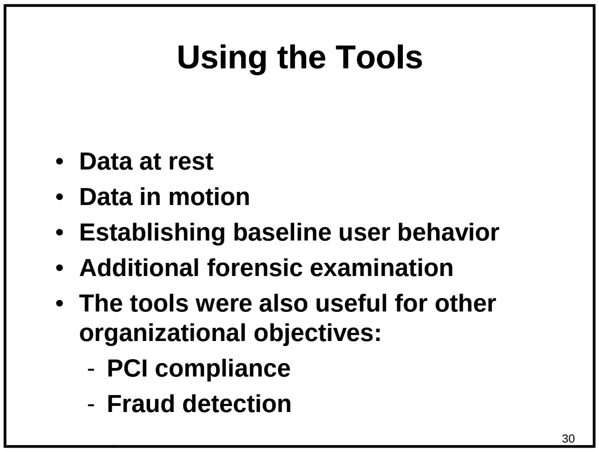
The Integrity Officer’s Role

- Communication and Education
  - Senior Management
  - Clinical Leaders
  - Board Support
- The Ask: Data Loss Prevention (DLP)
  - Capital
  - Software
  - FTEs



What We Needed

- Software to identify and prevent malware (this was timely)
- Software to identify where PHI exists and where it flows
- Software to monitor for inappropriate activities
- Hardware to support it
- FTE’s to manage it



Using the Tools

- Data at rest
- Data in motion
- Establishing baseline user behavior
- Additional forensic examination
- The tools were also useful for other organizational objectives:
  - PCI compliance
  - Fraud detection

Applying the Findings

- We identified specific departments that needed closer monitoring
- We found ePHI that was expired (per our retention policy) and could be sanitized
- We implemented technology to identify and automatically encrypt emails containing PHI and PII
- We developed a response plan for alerts that were triggered

31

You Don’t Need Sophisticated Technology

- Track & trend root causes of incidents and breaches
- Patient complaints r/t individual privacy rights, incidental disclosures etc.
- Do a policy & procedure “crosswalk”
- Track and trend disciplinary actions
- Monitor effectiveness of corrective actions (process redesign, SOPs, training). Are incidents decreasing?

32

Other Monitoring Ideas

- Inventory all medical devices that store PHI (networked or not)
- Medical Device “rounds” can confirm appropriate safeguards
- Review training completion rates and notify management if action required
- Survey or test random workforce members to assess comprehension and correct application of P&Ps

33

Other Ideas

- Audit a sample of Business Associate contracts
  - Are they compliant?
- “Secret shopper” site visits
  - Is verification of ID occurring?
  - Are safeguards in place to minimize incidental disclosures?
  - Are NPPs on display?
  - Do they know where to refer privacy complaints?

34

What About Your Ideas?

35

Cleveland Clinic

Every life deserves world class care