How to Prepare for an Audit

Judi Hofman CAP, CHP, CHSS

St Charles Health System

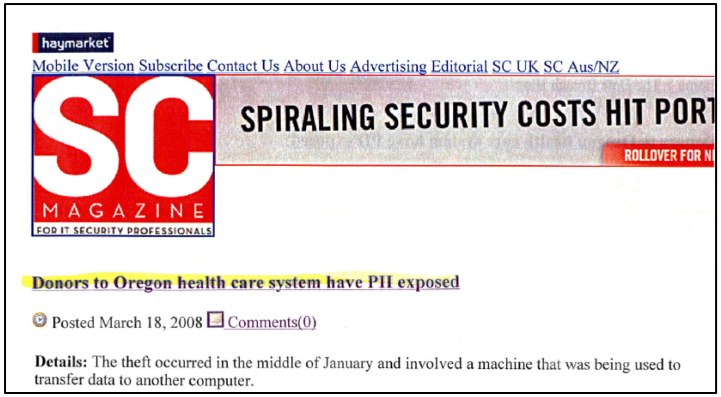
Bend, Oregon

St. Charles Health System

St. Charles Medical Center - Bend

St. Charles Medical Center - Redmond

Pioneer Memorial Hospital - Prineville



haymarket

Mobile Version Subscribe Contact Us About Us Advertising Editorial SC UK SC Aus/NZ

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

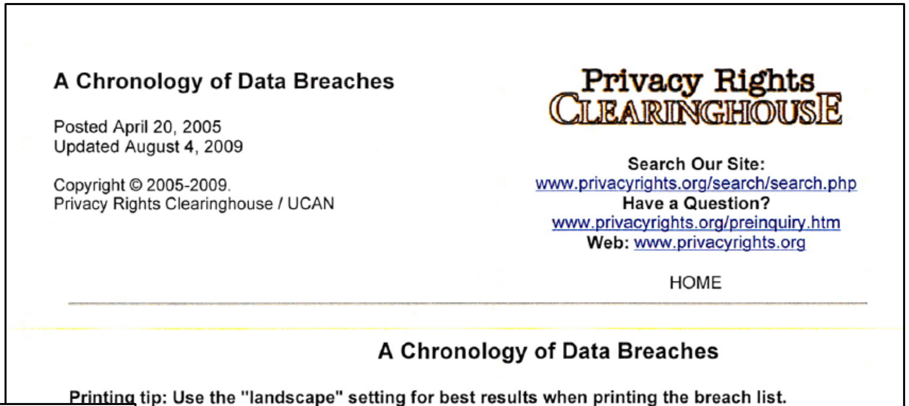
SPIRALING SECURITY COSTS HIT PORT

ROLLOVER FOR N

Donors to Oregon health care system have PII exposed

Posted March 18, 2008 Comments(0)

Details: The theft occurred in the middle of January and involved a machine that was being used to transfer data to another computer.



A Chronology of Data Breaches

Posted April 20, 2005
Updated August 4, 2009

Copyright © 2005-2009.
Privacy Rights Clearinghouse / UCAN

Privacy Rights CLEARINGHOUSE

Search Our Site:
www.privacyrights.org/search/search.php
Have a Question?
www.privacyrights.org/preinquiry.htm
Web: www.privacyrights.org

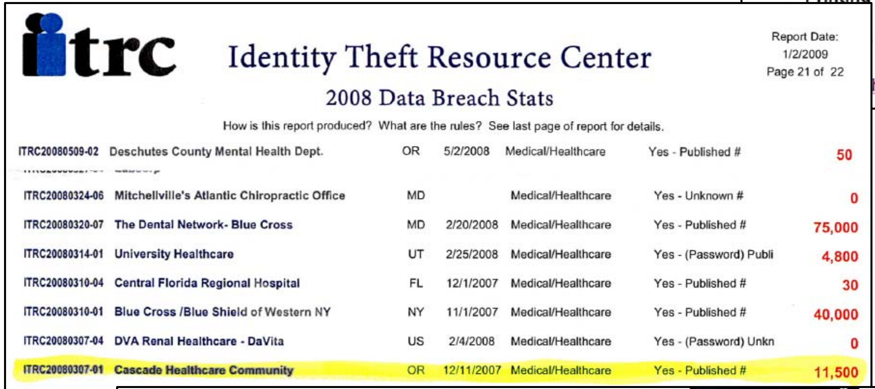
HOME

A Chronology of Data Breaches

Printing tip: Use the "landscape" setting for best results when printing the breach list.

introductory text and go directly to the listing of data breaches below.

hat does the Chronology of Data Breaches contain?



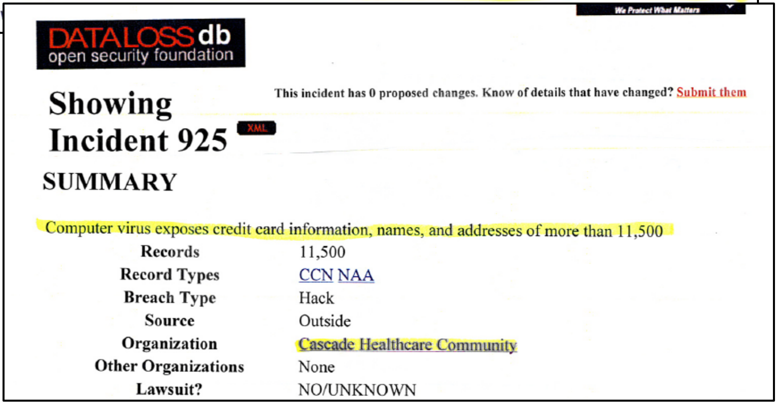
itrc Identity Theft Resource Center

Report Date: 1/2/2009
Page 21 of 22

2008 Data Breach Stats

How is this report produced? What are the rules? See last page of report for details.

ITRC20080509-02	Deschutes County Mental Health Dept.	OR	5/2/2008	Medical/Healthcare	Yes - Published #	50
ITRC20080324-06	Mitchellville's Atlantic Chiropractic Office	MD		Medical/Healthcare	Yes - Unknown #	0
ITRC20080320-07	The Dental Network- Blue Cross	MD	2/20/2008	Medical/Healthcare	Yes - Published #	75,000
ITRC20080314-01	University Healthcare	UT	2/25/2008	Medical/Healthcare	Yes - (Password) Publi	4,800
ITRC20080310-04	Central Florida Regional Hospital	FL	12/1/2007	Medical/Healthcare	Yes - Published #	30
ITRC20080310-01	Blue Cross /Blue Shield of Western NY	NY	11/1/2007	Medical/Healthcare	Yes - Published #	40,000
ITRC20080307-04	DVA Renal Healthcare - DaVita	US	2/4/2008	Medical/Healthcare	Yes - (Password) Unkn	0
ITRC20080307-01	Cascade Healthcare Community	OR	12/11/2007	Medical/Healthcare	Yes - Published #	11,500
ITRC20080229-02						



DATALOSS db open security foundation

We Protect What Matters

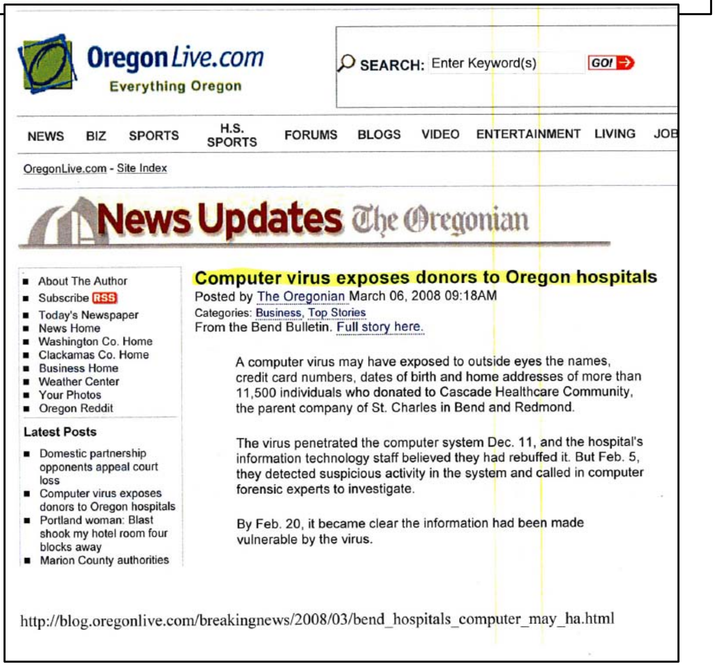
This incident has 0 proposed changes. Know of details that have changed? Submit them

Showing Incident 925 XML

SUMMARY

Computer virus exposes credit card information, names, and addresses of more than 11,500

Records	11,500
Record Types	CCN NAA
Breach Type	Hack
Source	Outside
Organization	Cascade Healthcare Community
Other Organizations	None
Lawsuit?	NO/UNKNOWN



OregonLive.com Everything Oregon

SEARCH: Enter Keyword(s) GO!

NEWS BIZ SPORTS H.S. SPORTS FORUMS BLOGS VIDEO ENTERTAINMENT LIVING JOB

OregonLive.com - Site Index

News Updates The Oregonian

- About The Author
- Subscribe RSS
- Today's Newspaper
- News Home
- Washington Co. Home
- Clackamas Co. Home
- Business Home
- Weather Center
- Your Photos
- Oregon Reddit

Latest Posts

- Domestic partnership opponents appeal court loss
- Computer virus exposes donors to Oregon hospitals
- Portland woman: Blast shook my hotel room four blocks away
- Marion County authorities

Computer virus exposes donors to Oregon hospitals

Posted by The Oregonian March 06, 2008 09:18AM
Categories: Business, Top Stories
From the Bend Bulletin. Full story here.

A computer virus may have exposed to outside eyes the names, credit card numbers, dates of birth and home addresses of more than 11,500 individuals who donated to Cascade Healthcare Community, the parent company of St. Charles in Bend and Redmond.

The virus penetrated the computer system Dec. 11, and the hospital's information technology staff believed they had rebuffed it. But Feb. 5, they detected suspicious activity in the system and called in computer forensic experts to investigate.

By Feb. 20, it became clear the information had been made vulnerable by the virus.

http://blog.oregonlive.com/breakingnews/2008/03/bend_hospitals_computer_may_ha.html

2011 OIG Audit Findings

7 hospitals

- □ 151 vulnerabilities
  - 124 to be high impact
  - 24 to be medium impact
  - 3 to be low impact

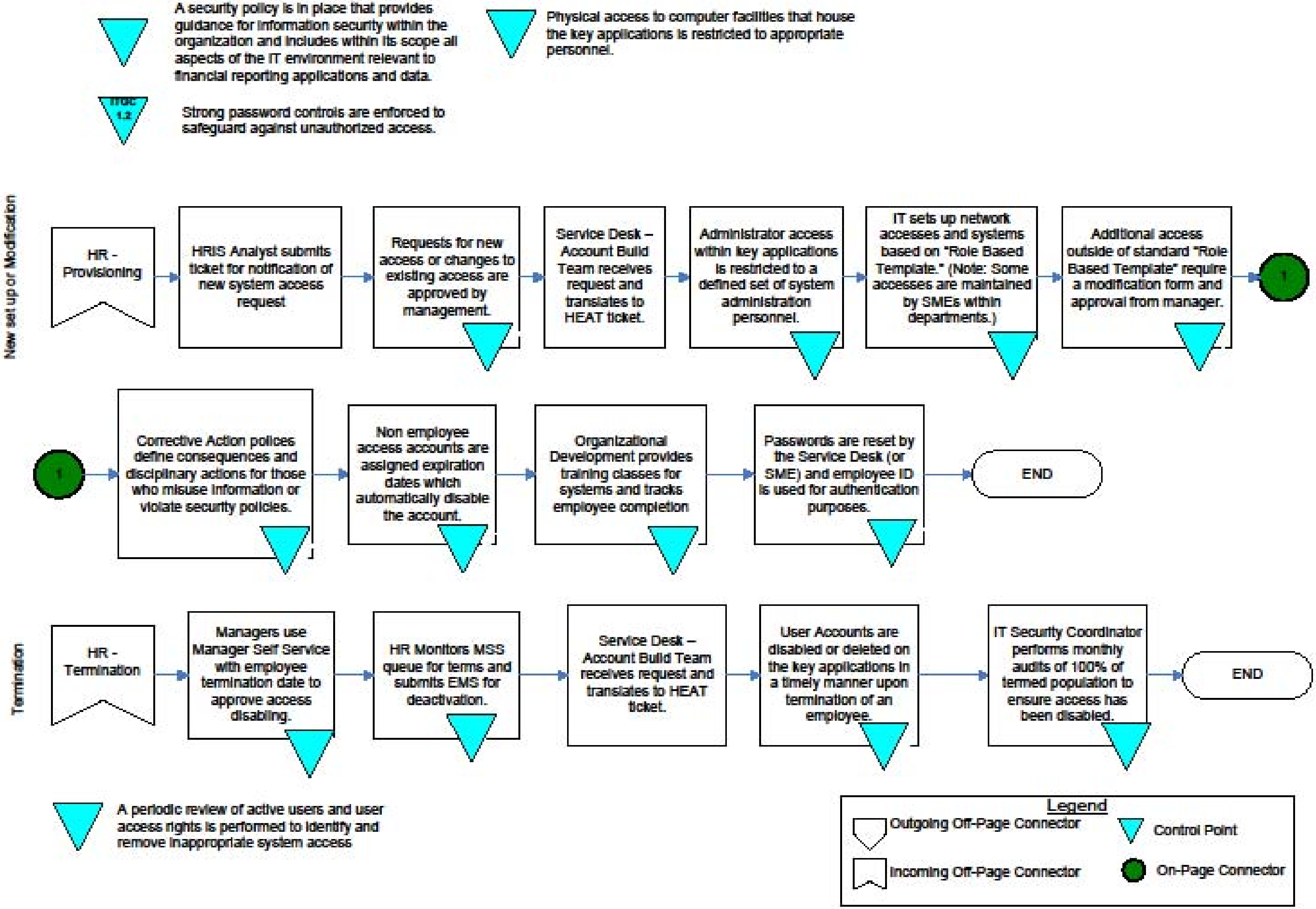
High Vulnerability – may result in highly costly loss of major tangible assts or resources; may significantly violate, hard or impede an organization mission reputation or interests; may result in human death or serious injury

HHS national rollup review of the Centers for Medicare & Medicaid Services HIPAA Oversight
http://healthcarecompliance101.com/2011/05/20/oig-audit-report-of-hipaa-security-of-hospitals/

How to Prepare for an Audit

- Centralized documentation
  - Policies and Procedures
  - Current Risk Analysis
  - Disaster recovery/emergency mode of operations plan
  - Incident response investigation documentation
  - Control testing and documentations
    - Application Layer
    - Infrastructure Layer
    - Enterprise Controls

Logical Access – 2012



A security policy is in place that provides guidance for information security within the organization and includes within its scope all aspects of the IT environment relevant to financial reporting applications and data.

Physical access to computer facilities that house the key applications is restricted to appropriate personnel.

Strong password controls are enforced to safeguard against unauthorized access.

New set up or Modification

HR - Provisioning

HRIS Analyst submits ticket for notification of new system access request

Requests for new access or changes to existing access are approved by management.

Service Desk – Account Build Team receives request and translates to HEAT ticket.

Administrator access within key applications is restricted to a defined set of system administration personnel.

IT sets up network accesses and systems based on "Role Based Template." (Note: Some accesses are maintained by SMEs within departments.)

Additional access outside of standard "Role Based Template" require a modification form and approval from manager.

Corrective Action polices define consequences and disciplinary actions for those who misuse information or violate security policies.

Non employee access accounts are assigned expiration dates which automatically disable the account.

Organizational Development provides training classes for systems and tracks employee completion

Passwords are reset by the Service Desk (or SME) and employee ID is used for authentication purposes.

END

Termination

HR - Termination

Managers use Manager Self Service with employee termination date to approve access disabling.

HR Monitors MSS queue for terms and submits EMS for deactivation.

Service Desk – Account Build Team receives request and translates to HEAT ticket.

User Accounts are disabled or deleted on the key applications in a timely manner upon termination of an employee.

IT Security Coordinator performs monthly audits of 100% of termed population to ensure access has been disabled.

END

A periodic review of active users and user access rights is performed to identify and remove inappropriate system access

Legend

Outgoing Off-Page Connector

Control Point

Incoming Off-Page Connector

On-Page Connector

TESTING RESULT / FINDINGS

Steps Performed: Test Script Review:

1) Obtain the entity's Password Policy (if any)
2) From the corresponding control contact, obtain screen shots (or other documentary evidence) of password configurations for each layer of the in-scope application (application, database, server).
3) For each layer per application, ensure passwords contain a) periodic expiration, b) complexity (num, letters, and/or symbols), and c) minimum length as stated in policy.
4) Note any exceptions

Round 1

Testing Sample:	Application	Layer	Step 3.a	Step 3.b	Step 3.c	Pass (Yes, No)?	Work Paper REF	Notes
1	Ap 1	Application	✓	✓	✓	Yes	ITGC.1.1.a	b
2	Ap 1	Database	✓	✓	✓	Yes	ITGC.1.1.b	b
3	Ap 1	Server	✓		✓	No	ITGC.1.1.c	a, b
4	Ap 2	Application	✓	✓	✓	Yes	ITGC.1.2.a	b
5	Ap 2	Database	✓	✓	✓	Yes	ITGC.1.2.b	b
6	Ap 2	Server	✓	✓	✓	Yes	ITGC.1.2.c	b
7	Ap 3	Application	✓	✓	✓	Yes	ITGC.1.3.a	b
8	Ap 3	Database	✓	✓	✓	Yes	ITGC.1.3.b	b
9	Ap 3	Server	✓	✓	✓	Yes	ITGC.1.3.c	b

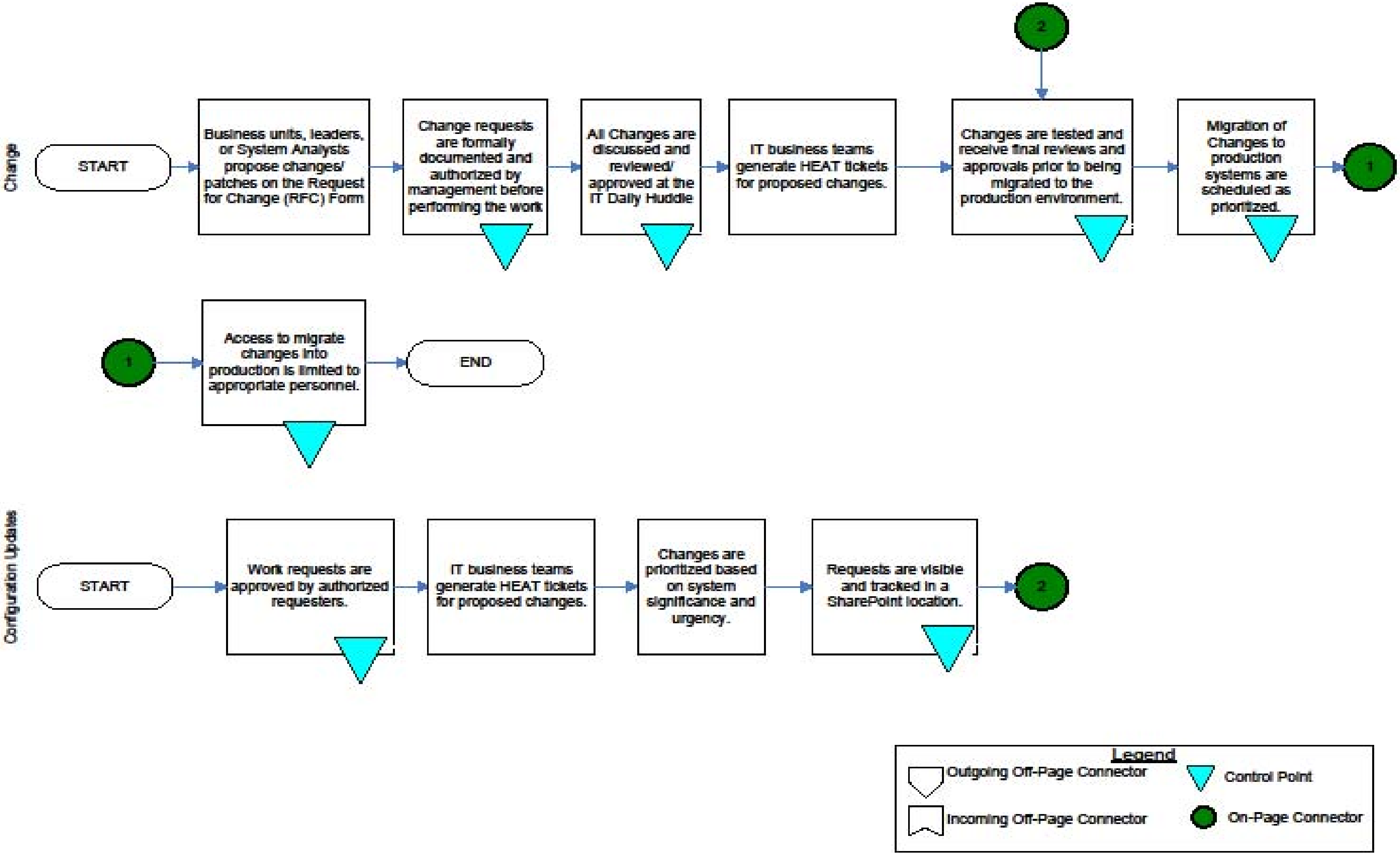
Notes: Notes Review:

a)	Passwords have no complexity at the server level for Ap 1
b)	Entity Policy on Passwords is in DRAFT only

Observations/Conclusions: Observation / Conclusions Review:

ID	Control Description	Ap 1	Ap 2	Ap 3	Ap 4
HIPAA 1	Strong password controls are enforced to safeguard against unauthorized access.	FAIL	PASS	PASS	PASS
HIPAA 2	User Accounts are disabled or deleted on the key applications upon termination of an employee.				
HIPAA 3	Administrator access within key applications is restricted to a defined set of system administration personnel.				
HIPAA 4	A review of user accounts and their associated access levels is performed and adequately documented to ensure appropriate access to the system.				
HIPAA 5	Change requests are formally documented and authorized by management before performing the work.				
HIPAA 6	Monitoring procedures are designed to provide reasonable assurance around completeness and timeliness of system and data processing.				
HIPAA 7	Backups are scheduled and monitored for successful completion.				

Change Management – 2012



Change

START

Business units, leaders, or System Analysts propose changes/ patches on the Request for Change (RFC) Form

Change requests are formally documented and authorized by management before performing the work

All Changes are discussed and reviewed/ approved at the IT Daily Huddle

IT business teams generate HEAT tickets for proposed changes.

2

Changes are tested and receive final reviews and approvals prior to being migrated to the production environment.

Migration of Changes to production systems are scheduled as prioritized.

1

1

Access to migrate changes into production is limited to appropriate personnel.

END

Configuration Updates

START

Work requests are approved by authorized requesters.

IT business teams generate HEAT tickets for proposed changes.

Changes are prioritized based on system significance and urgency.

Requests are visible and tracked in a SharePoint location.

2

Legend

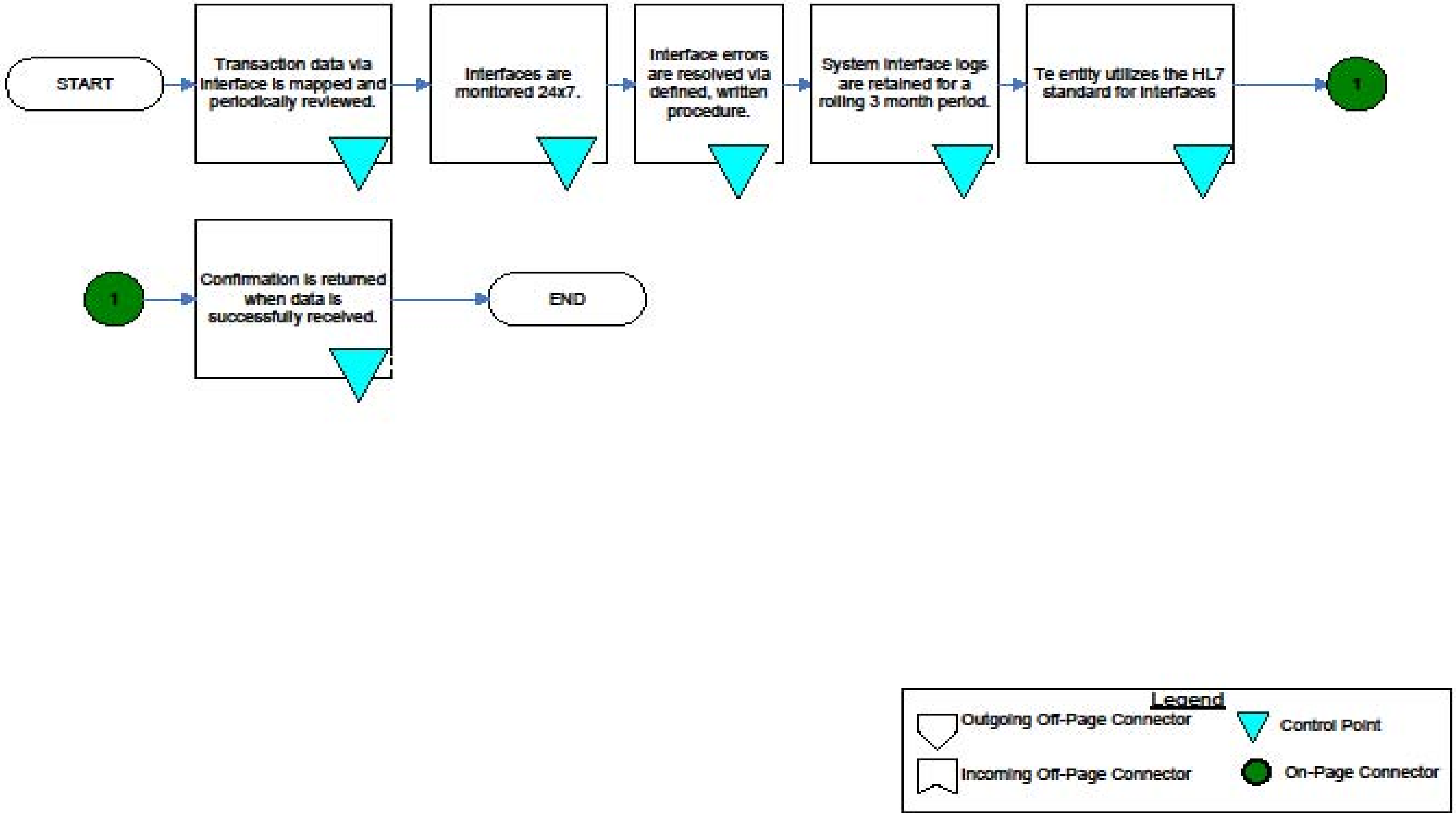
Outgoing Off-Page Connector

Incoming Off-Page Connector

Control Point

On-Page Connector

System Interfaces – 2012



START

Transaction data via interface is mapped and periodically reviewed.

Interfaces are monitored 24x7.

Interface errors are resolved via defined, written procedure.

System interface logs are retained for a rolling 3 month period.

Te entity utilizes the HL7 standard for interfaces

1

1

Confirmation is returned when data is successfully received.

END

Legend

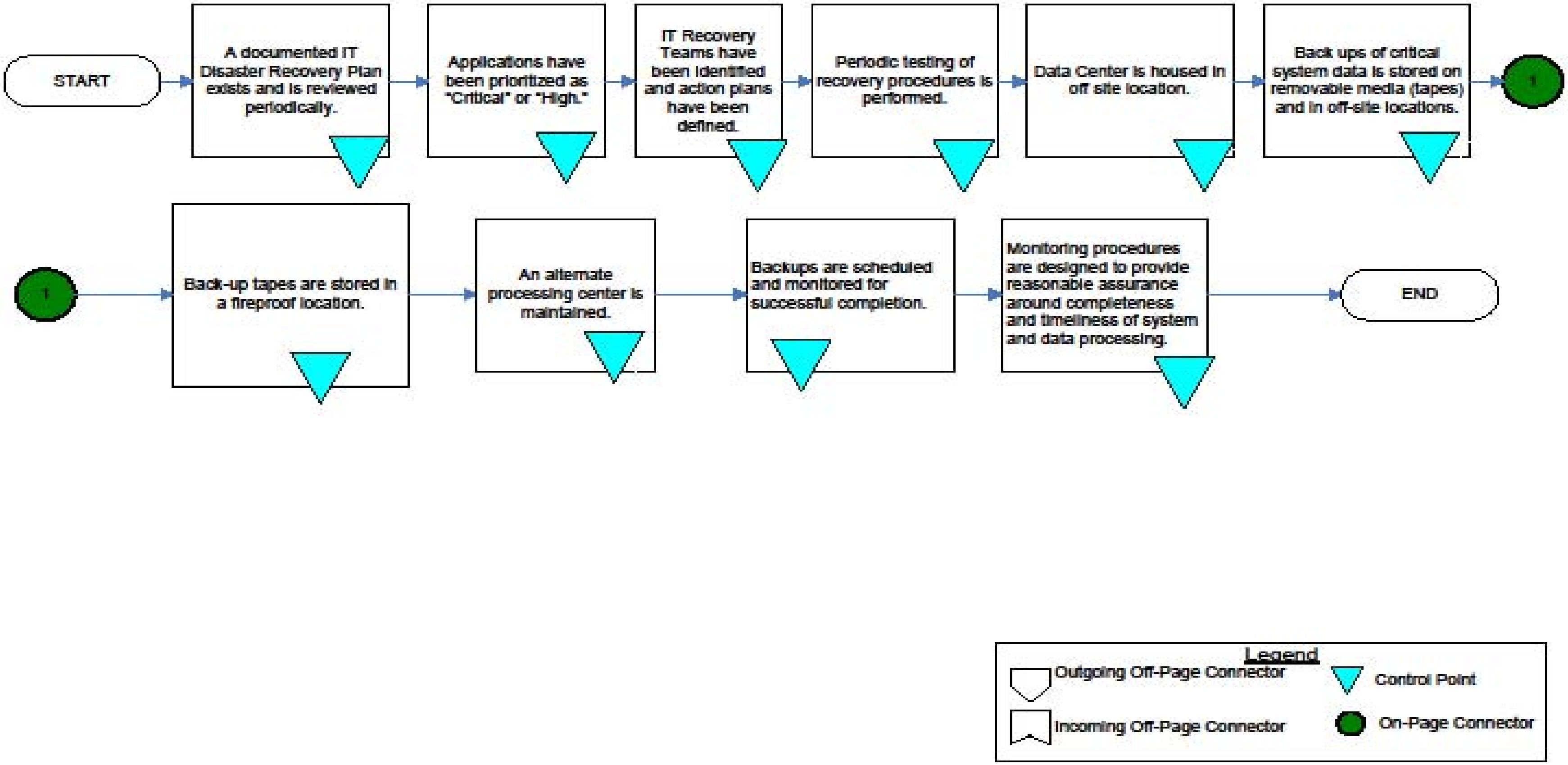
Outgoing Off-Page Connector

Incoming Off-Page Connector

▽ Control Point

● On-Page Connector

Disaster Recovery - 2012



START

A documented IT Disaster Recovery Plan exists and is reviewed periodically.

Applications have been prioritized as "Critical" or "High."

IT Recovery Teams have been identified and action plans have been defined.

Periodic testing of recovery procedures is performed.

Data Center is housed in off site location.

Back ups of critical system data is stored on removable media (tapes) and in off-site locations.

1

1

Back-up tapes are stored in a fireproof location.

An alternate processing center is maintained.

Backups are scheduled and monitored for successful completion.

Monitoring procedures are designed to provide reasonable assurance around completeness and timeliness of system and data processing.

END

Legend

Outgoing Off-Page Connector

Incoming Off-Page Connector

▼ Control Point

● On-Page Connector

How to Prepare for an Audit

- Develop a compliance plan
  - Engage impacted departments

    *IT *HR *Business *Internal Audit
  - Combine other compliance assessment activities

    *PCI *Financial *HR
- Evidence of Compliance
  - Design effectiveness
  - Operational effectiveness

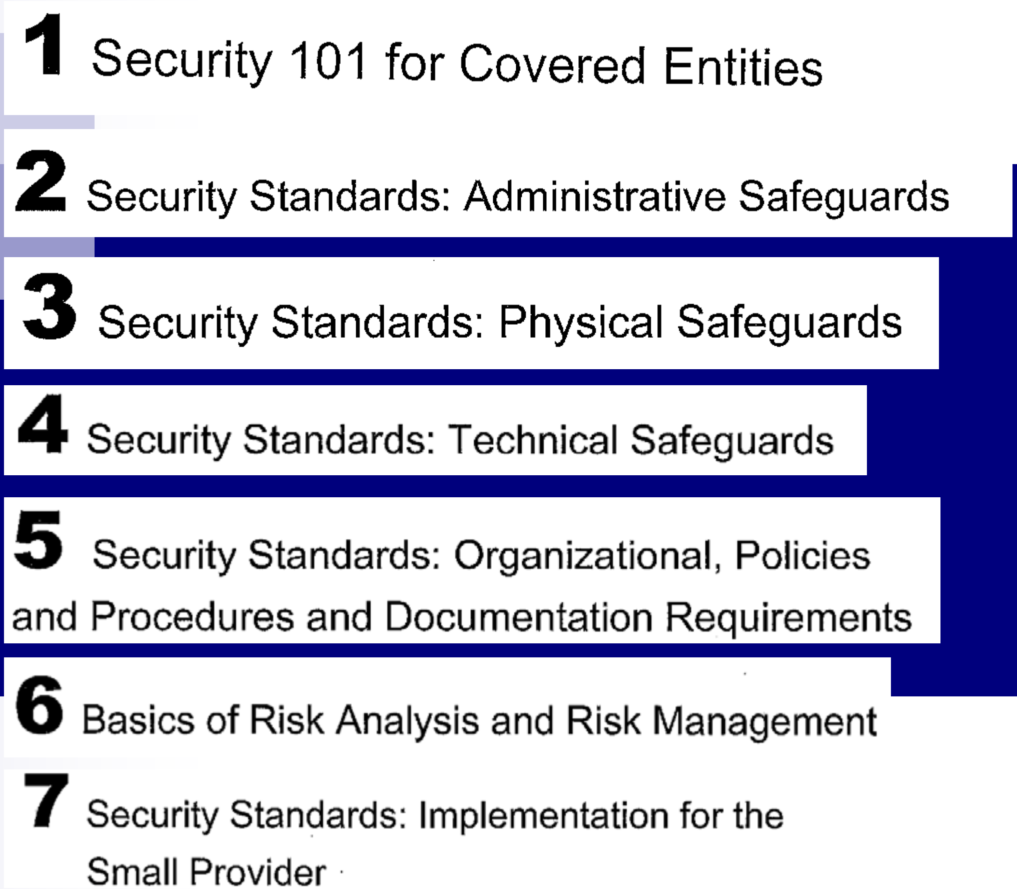
How to Prepare for an Audit

- Top of the list compliance focus includes:
  - Policies and Procedures
  - Workforce training (new an on-going)
  - Audit program (periodic & annual)
  - Incident response (including breach response)
  - Risk analysis & risk mitigation

How to Prepare for an Audit

- High risk areas include lack of:
  - On-going risk management
  - Current disaster recovery and emergency mode of operations plan
  - Encryption of any transmitted or transported electronic PHI
  - Access control
  - Risk assessment

HIPAA Security Series



1 Security 101 for Covered Entities

2 Security Standards: Administrative Safeguards

3 Security Standards: Physical Safeguards

4 Security Standards: Technical Safeguards

5 Security Standards: Organizational, Policies and Procedures and Documentation Requirements

6 Basics of Risk Analysis and Risk Management

7 Security Standards: Implementation for the Small Provider

http://www.hhs.gov/ocr/privacy/hipaa/administrative
/securityrule/securityruleguidance.html

Guidance of Risk Analysis Required under the HIPAA Security Rule

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

How to Prepare for an Audit

- High risk areas include lack of (continued):
  - Compliant data backup and recovery
  - Remote access management
  - Wireless access
  - Audit control
  - Person or entity authentications
  - Documentation plan to address OCR or state investigation and audits

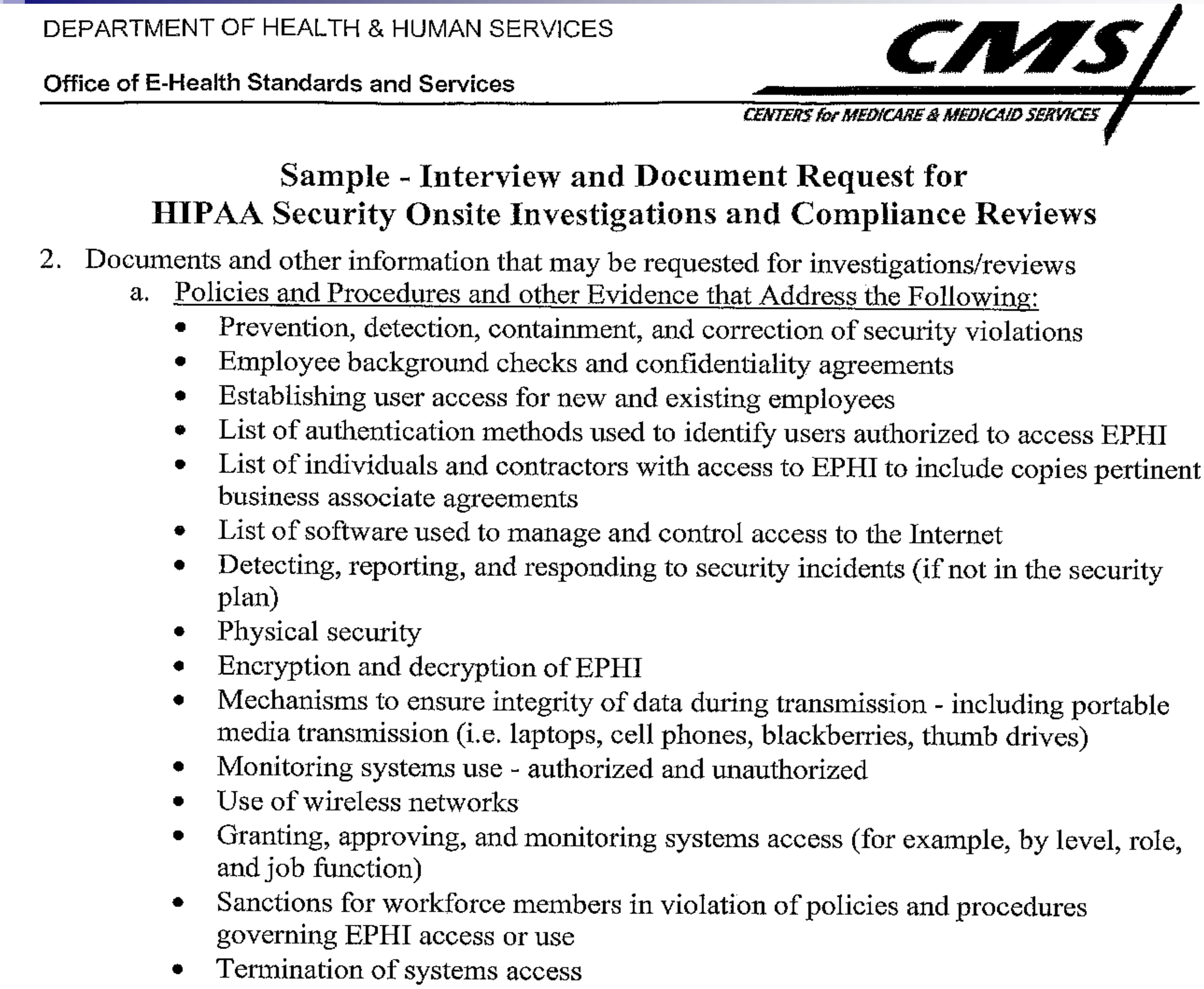
DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of E-Health Standards and Services

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Sample - Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews

1. Personnel that may be interviewed
   - President, CEO or Director
   - HIPAA Compliance Officer
   - Lead Systems Manager or Director
   - Systems Security Officer
   - Lead Network Engineer and/or individuals responsible for:
     - administration of systems which store, transmit, or access Electronic Protected Health Information (EPHI)
     - administration systems networks (wired and wireless)
     - monitoring of systems which store, transmit, or access EPHI
     - monitoring systems networks (if different from above)
   - Computer Hardware Specialist
   - Disaster Recovery Specialist or person in charge of data backup
   - Facility Access Control Coordinator (physical security)
   - Human Resources Representative
   - Director of Training
   - Incident Response Team Leader
   - Others as identified….



DEPARTMENT OF HEALTH & HUMAN SERVICES

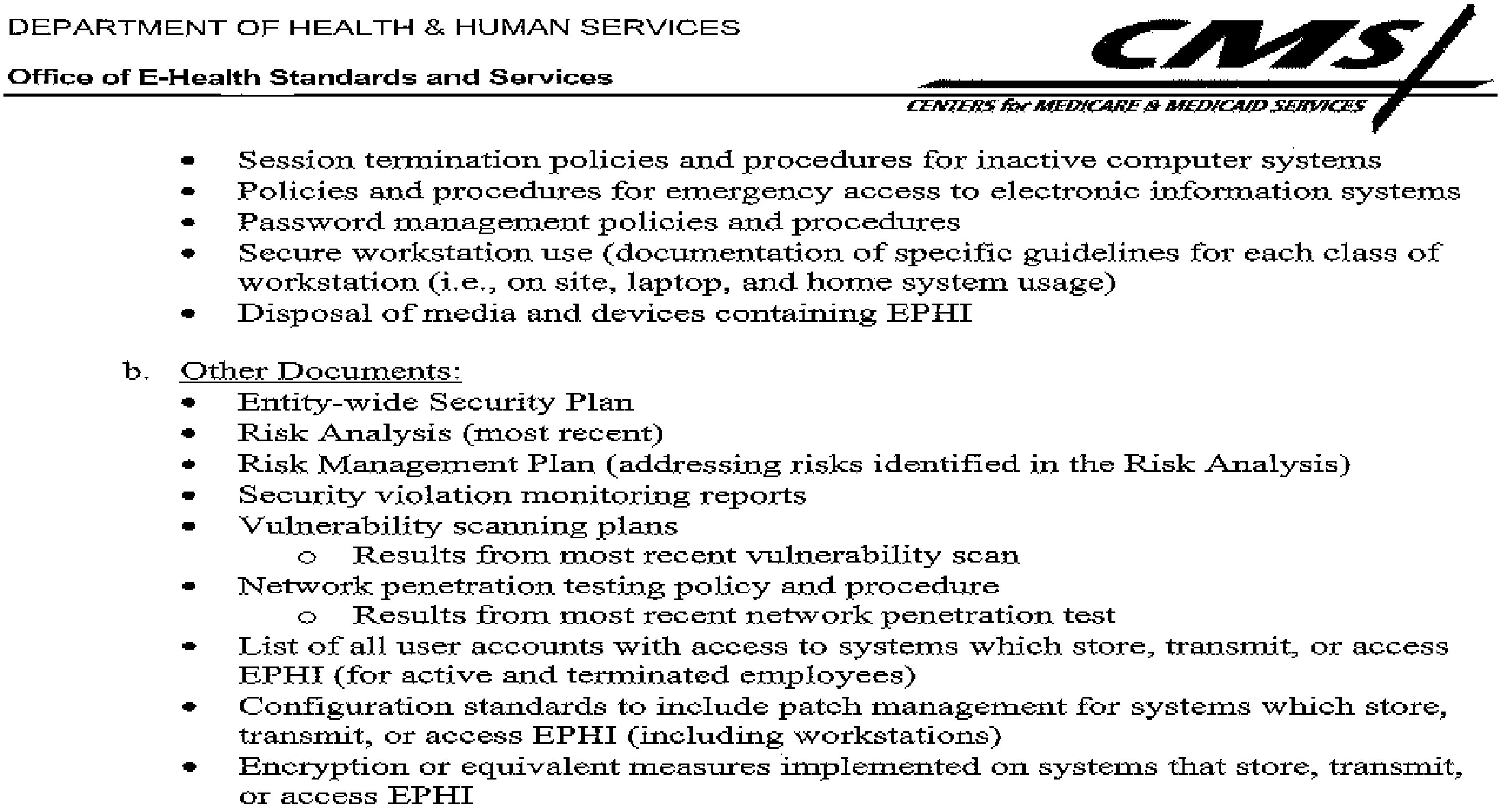
Office of E-Health Standards and Services

CMS

CENTERS for MEDICARE & MEDICAID SERVICES

Sample - Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews

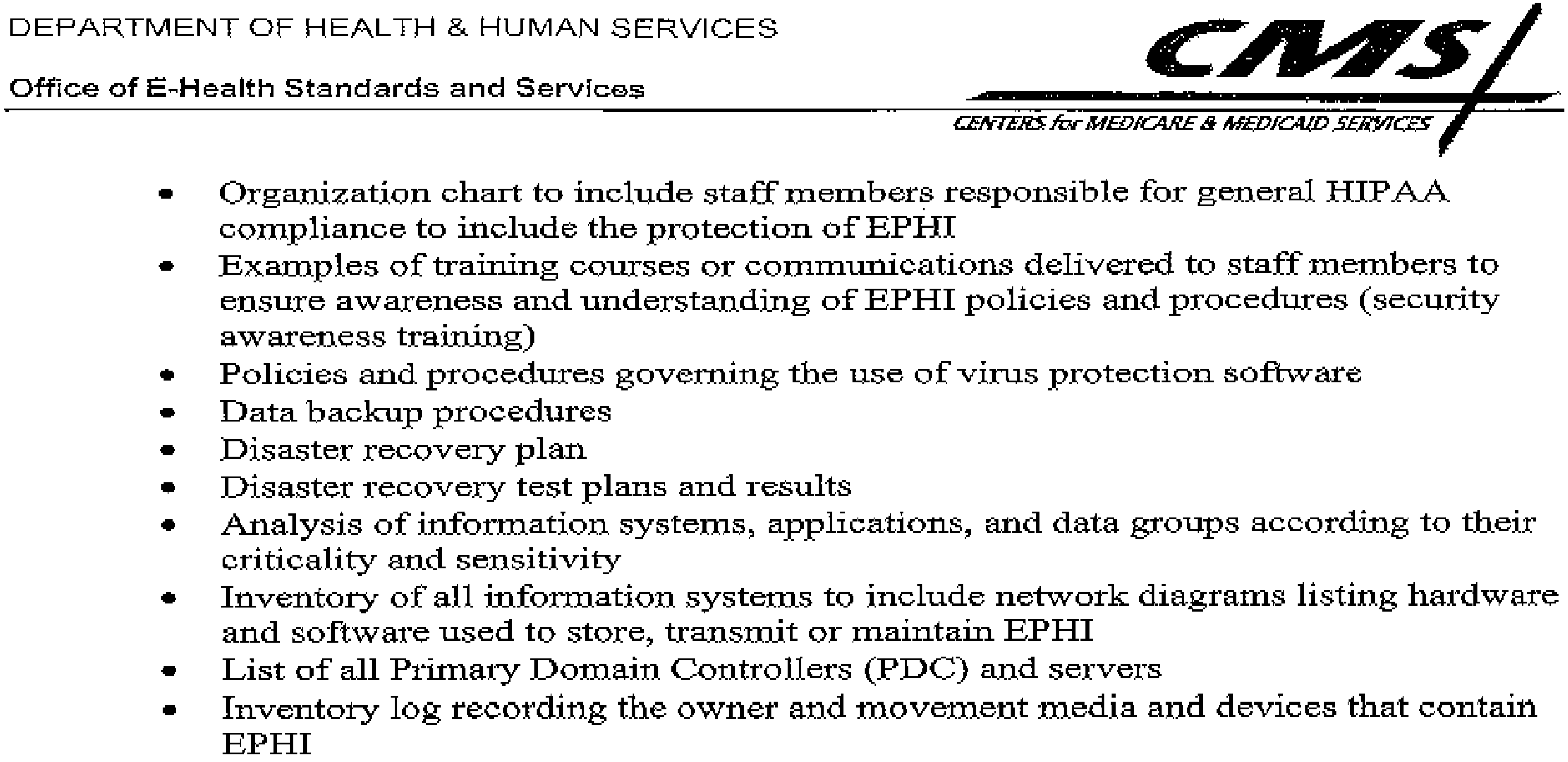
2. Documents and other information that may be requested for investigations/reviews
   a. Policies and Procedures and other Evidence that Address the Following:
      - Prevention, detection, containment, and correction of security violations
      - Employee background checks and confidentiality agreements
      - Establishing user access for new and existing employees
      - List of authentication methods used to identify users authorized to access EPHI
      - List of individuals and contractors with access to EPHI to include copies pertinent business associate agreements
      - List of software used to manage and control access to the Internet
      - Detecting, reporting, and responding to security incidents (if not in the security plan)
      - Physical security
      - Encryption and decryption of EPHI
      - Mechanisms to ensure integrity of data during transmission - including portable media transmission (i.e. laptops, cell phones, blackberries, thumb drives)
      - Monitoring systems use - authorized and unauthorized
      - Use of wireless networks
      - Granting, approving, and monitoring systems access (for example, by level, role, and job function)
      - Sanctions for workforce members in violation of policies and procedures governing EPHI access or use
      - Termination of systems access



- Session termination policies and procedures for inactive computer systems
- Policies and procedures for emergency access to electronic information systems
- Password management policies and procedures
- Secure workstation use (documentation of specific guidelines for each class of workstation (i.e., on site, laptop, and home system usage)
- Disposal of media and devices containing EPHI

b. Other Documents:

- Entity-wide Security Plan
- Risk Analysis (most recent)
- Risk Management Plan (addressing risks identified in the Risk Analysis)
- Security violation monitoring reports
- Vulnerability scanning plans
    - Results from most recent vulnerability scan
- Network penetration testing policy and procedure
    - Results from most recent network penetration test
- List of all user accounts with access to systems which store, transmit, or access EPHI (for active and terminated employees)
- Configuration standards to include patch management for systems which store, transmit, or access EPHI (including workstations)
- Encryption or equivalent measures implemented on systems that store, transmit, or access EPHI



DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of E-Health Standards and Services

CENTERS for MEDICARE & MEDICAID SERVICES

- Organization chart to include staff members responsible for general HIPAA compliance to include the protection of EPHI
- Examples of training courses or communications delivered to staff members to ensure awareness and understanding of EPHI policies and procedures (security awareness training)
- Policies and procedures governing the use of virus protection software
- Data backup procedures
- Disaster recovery plan
- Disaster recovery test plans and results
- Analysis of information systems, applications, and data groups according to their criticality and sensitivity
- Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit or maintain EPHI
- List of all Primary Domain Controllers (PDC) and servers
- Inventory log recording the owner and movement media and devices that contain EPHI

How to Prepare for an Audit

- Current Risk Assessment
- Prioritize high to low risk compliance gaps
- Assign resources to eliminate privacy and security compliance gaps
- Track and document compliance project status
- Document mitigation activity
- Store all centrally

How to Prepare for an Audit

- Have the right staff identified; staff that know how to talk to an auditor; know their processes; know the detail of the evidence
- This amounts to more than adopting required policies and procedures – compliance is an on-going process
- Need to demonstrate continued compliance activities (not a “one time” event)

How to Prepare for an Audit

- Key to surviving an audit unscathed
  - current and accurate documentation that is easily accessible
- CE bear the burden of demonstrating compliance
- The time is now to address compliance gaps
- Periodically review OCR website for new and changing information

- Questions