Security Audits: Is Your Organization Prepared and in Compliance?

Judi Hofman CAP, CHP, CHSS
Privacy and Information Security Officer
Cascade Healthcare Community
Bend, Oregon

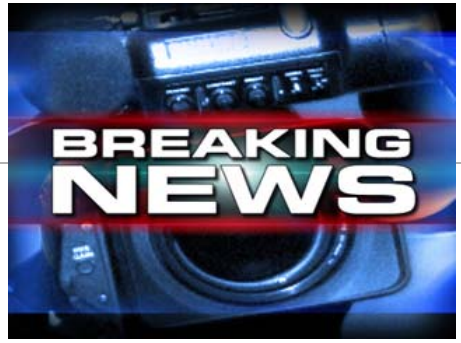
Cascade
HEALTHCARE COMMUNITY

St. Charles Medical Center - Bend

St. Charles Medical Center Redmond

Pioneer Memorial Hospital Prineville

Cascade
HEALTHCARE COMMUNITY



Hospital donor files compromised

Data breach at Cascade Healthcare may affect more than 11,500 people

By Markian Hawryluk and Betsy Q. Cliff / *The Bulletin*

Published: March 06. 2008 4:00AM PST

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.

On Wednesday, the hospital announced the data may have been exposed. The data breach is a concern due to the potential for identity theft.

Hospital officials say it is not clear whether any of the information was seen by individuals outside the hospital. There is no evidence that patient health information was compromised, officials said.

"Although the investigation provided no indication that information was misused, CHC is working quickly and diligently to provide all affected members of our community with leading credit monitoring service at no charge," Cascade Healthcare President and CEO Jim Diegel said in a prepared statement.

"We want to express our sincere apologies to those community members who have trusted us with their information for the inconvenience and worry this situation may have caused."

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 NI

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.

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

- What

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	Wellesley Health Dept.	MA	2/5/2008	Medical/Healthcare	Yes - Published #	500

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

Cascade
HEALTHCARE COMMUNITY

The Breach

Virus Occurrence - December 11, 2007

Notification by CMS of a “CMS” triggered HIPAA Security Audit to be conducted by their audit contractor – PriceWaterhouseCooper

- Original Notification from CMS
  July 1, 2008
- First Meeting
  July 25, 2008

Cascade
HEALTHCARE COMMUNITY

Requested Meetings by CMS - PwC

- Pre-entrance Teleconference 7/25
- Entrance Conference 8/4
- On-site at CHC 8/4/08 – 8/8/08
  - Three investigators

All together we had 15 meetings with senior executives and department directors/ managers in one week.

Cascade
HEALTHCARE COMMUNITY

Prepared by Client List of Requested Documents (PBC)

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Remote Access

Cascade
HEALTHCARE COMMUNITY

Prepared by Client (PBC) List of Requested Documents

- Set Up - electronic file folder
- Rule of thumb - give them the only what they ask for, if they need more documentation they will ask, you don't want them looking into things they did not come to audit in the first place.
- Clear your calendar!
- Notify you leadership group that they my have some high priority meetings coming out on their calendar
- Keep your friends close and your enemies closer

CMS Prepared By Client (PBC) list

Administrative Safeguards

- AS-1 Policies and procedures on creation, maintenance, and governance of risk assessments (RA) and system security plans (SSP)
- AS-2 Most current Risk Assessment (RA) for impacted applications and General Support Systems (GSS) including Certification/Approval Page. Please note if there are multiple RA/SSPs, please provide those for applications and GSSs that process or store PII/PHI.
- AS-3 Most current SSP for impacted applications and GSS including Certification/Approval Page

  Please note if there are multiple RA/SSPs, please provide those for applications and GSSs that process or store PII/PHI.
- AS-4 Policies and procedures on protection of PHI and ePHI; including sanctions for violation of policy.

  -Including procedures on the protection and use of blackberry devices, thumb drives, portable disk drives, etc.

  -Compliance with HIPAA Security Rule

Cascade
HEALTHCARE COMMUNITY

CMS Prepared By Client (PBC) list - continued

- AS-5 Listing of all PHI violations within the past year
- AS-6 Policies and procedures governing monitoring of access and violations; including follow up activities for suspicious activity. Policies and procedures that include information on:
  -records logging information system activity, including audit logs, access
- AS-7 IS Dept Organization Chart; including Privacy/HIPAA Official
- AS-8 Job Description for Privacy/HIPAA Official
- AS-9 Security Awareness, Privacy, Training Content (initial and annual)
- AS-10 Listing or organization chart of all Incident Response Team members; including job descriptions for team members
- AS-11 Listing of all current employees (including name, dept/cost center, job title, & direct supervisor/manager)
- AS-12 Listing of all employees hired within the past year (including name, dept/cost center, job title, & direct supervisor/manager)

CMS Prepared By Client (PBC) list - continued

- AS-13 Policies and procedures governing security awareness training (new hire and refresher)
- AS-14 Policies and procedures governing virus identification software including updating, detecting, and reporting malicious software and/or viruses.
- AS-15 Policies and procedures (baselines) governing passwords including:
  - -Password Standards/Configurations
  - -Creation, changing, and safeguarding
  - -Passwords on remote devices (laptops, PDA's, etc.)
- AS-16 Polices/procedures for Data and Resource Classification
- AS-17 Most recent internal audit/review of HIPAA compliance
- AS-18 Network Diagram

Physical Safeguards

- PS-1 Policies and procedures governing workstation security (for devices storing ePHI) including on-site, laptops, at home system usage, etc.
- PS-2 Inventory of laptops and desktops in your environment

CMS Prepared by client (PBC) list - continued

Technical Safeguards

- TS-1 Policies and procedures governing the use of generic, group or system IDs
- TS-2 Policies and procedures governing disabling vendor supplied defaults
- TS-3 Policies and procedures governing granting of dial up/remote access
- TS-4 Policies and procedures on the encryption/decryption of ePHI
  *During Transmission;*ePHI on remote devices;*ePHI on backup and archived data
- TS-5 Evidence of the implementation of password policies on platforms which store, transmit or process ePHI
- TS-6 Transmission Security procedure (formal requirements for transmission of ePHI; controls governing integrity of information transmitted on networks)
- TS-7 Configuration standards for platforms which store, transmit, or process ePHI (including workstations)
- TS-8 Policies and procedures governing the use of wireless networks in the environment
- TS-9 Wireless access points baseline configurations (if applicable)

Cascade
HEALTHCARE COMMUNITY

CMS Prepared by client (PBC) list - continued

Remote Access

- RA-1 Procedures/Baseline for Firewall protection on laptops
- RA-2 Listing of users provided with laptops & with remote access
- RA-3 Rules of Behavior/Personnel Security rules for laptop users
- RA-4 Entity wide Patch Management policy (including pushing updates to remote devices)
- RA-5 Entity wide Configuration management policy (including remote devices)

Cascade
HEALTHCARE COMMUNITY

HIPAA Compliance Review Analysis and Summary of Results

Center for Medicare & Medicaid Services
Office of E-health Standards and Services

2008

Cascade
HEALTHCARE COMMUNITY

Corrective Action Plan (CAP)

- **Risk Assessment 164.308(a)(1)(ii)(A)**
  - CEs did not perform a risk assessment
    - Note: "The Global State of Information Security 2008" only 57% of survey respondent organizations conducted enterprise risk assessment at least once a year
  - CEs did not have a formalized, documented risk assessment process
  - CEs had outdated risk assessments
  - CEs did not address all potential areas of risk

Corrective Action Plan (CAP) - Continued

- **Currency of Policies and Procedures 164.308(a)(8)**
  - CEs did not review and approve security policies and procedures within the time frame that their policy required
  - CEs did not document evidence of their review and approval of policies and procedures
  - CEs documented procedures were inconsistent with procedures followed by ED personnel
  - CEs did not have formally documented policies related to training
  - CEs did not track and retain evidence of training completion
  - CEs did not conduct security awareness training prior to granting user access
  - CEs did not conduct security refresher training on a regular basis

Corrective Action Plan (CAP) - Continued

- **Workforce Clearance 164.308(a)(iii)(B)**
  - CEs granted access to ePHI prior to completing background investigations
- **Workstation Security 164.310(b)**
  - CEs did not have a formalized, documented policy or process for verifying the security of workstations
  - CEs were not complying with their policies and procedures for securing workstations
  - CEs did not deploy the necessary tools to implement documented policies

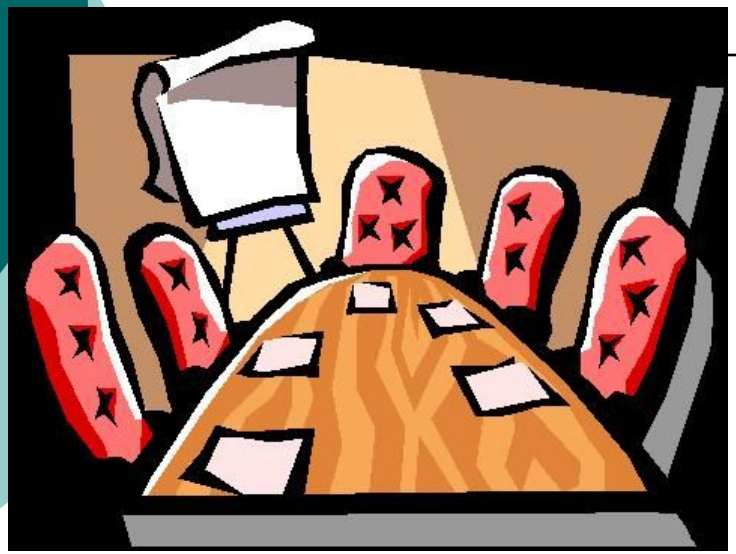
Corrective Action Plan (CAP) - Continued

- **Encryption**
  - Encryption was not implemented on all workstations and laptops
  - Encryption was not implemented on the transmission of data which contained ePHI
  - Strong encryption was not consistently implemented
- **Got your evidence**
  - Education
    - Pulled sample of employee
      - Requested documentation that each completed security train prior to access to e-PHI applications
  - Firewall
    - Pulled sample of systems and laptops
      - Viewed configuration for security

CMS Response to "Covered Entity" (CE)
Corrective Action Plan

Finding #	Finding	CE Response	CE Corrective Action Plan (CAP)	CMS Response
CE - 1	CE should conduct a formal, documented risk assessment for system corporate reporting tool and applications which house, process, or transmit EPHI. For each threat identified, the risk assessment should include: • likelihood of occurrence; • impact severity; • mitigating control(s); and, • risk level. The risk assessment should be conducted in accordance with CE's "HIPAA Risk Assessment and Risk Management" procedure. After an initial risk assessment has been conducted, CE should conduct an analysis to determine the appropriate interval for conducting these assessments, based on the current interval of 12-18 months. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, RA-4, "Risk Assessment Update" recommends that risk assessments be performed on a regular basis or whenever	I. mm/dd/yy - full HIPAA Security Audit. II. mm/dd/yy- A risk assessment was performed on a new critical EMR application. III. We have established a committee called the CE Data Security Governance Committee.	I. We will review the technical process for each individual application and our overall system security plan. II. We will identify a baseline of the inventory of information assets and responsible data stewards--our first step in identifying our assets so that we can do a risk assessment. **Note:** Our technical resources are severely limited in 2008 due to the planned go live of a major electronic medical record application. Target Dates for completion of CAP Steps: I. mm/dd/yy II. mm/dd/yy III. mm/dd/yy	.
	there are significant changes to the system. The maximum interval for conducting these assessments is identified as three years. Once the appropriate interval is identified, CE should update their procedure to state that this process should be performed at the identified interval or whenever there is a significant change to the environment.			

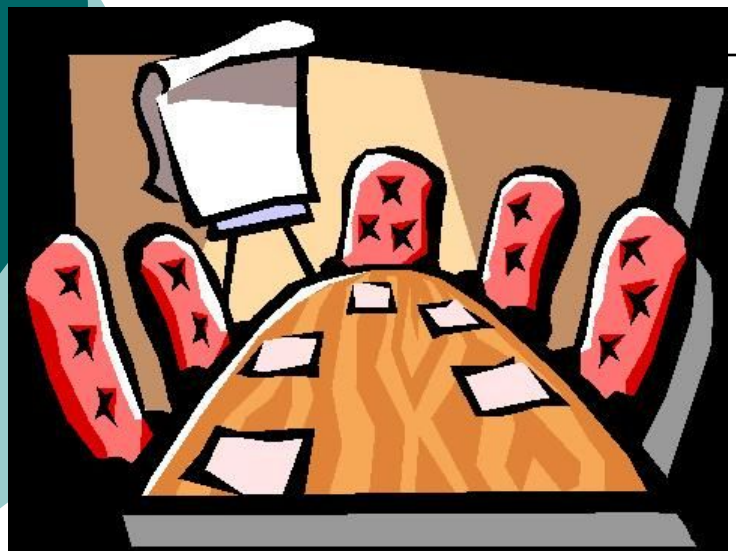
Cascade
HEALTHCARE COMMUNITY



Time Line

- Prepared by client (PBC) list items due 8/13
- First Draft report to Cascade and CMS 8/18
- Exit meeting and discussion on corrective actions with PwC 8/20
- Second draft report to Cascade and CMS containing corrective actions 8/22
- Final draft from CHC response to second draft due 8/29

Cascade
HEALTHCARE COMMUNITY



Time Line - Continued

- Corrective action – response to first due date
  - in November 1, 2008
- Response back from CMS
  - December 22, 2008
- Corrective action – due date
  - February 2009
- Response back from CMS
  - July 22, 2009
- Corrective action – due date
  - August 22, 2009
- Follow by OCR-HHS Division
  - January 4, 2009

Cascade
HEALTHCARE COMMUNITY

Summary of Results

- Final report from PwC – 45 pages
  - Background
  - Testing Performed Results of Testing
  - Recommendation of Corrective Action
  - Summary

- Procedural Report
  - Corrective Action Response from CHC
  - Corrective Action Plan (CAP) Steps
  - Target Date for Completion of CAP Steps

Cascade
HEALTHCARE COMMUNITY

New investigating authority - Office for Civil Rights

Cascade
HEALTHCARE COMMUNITY

Follow up by Quality Software Services, Inc. (QSSI)

CMS Response to "Covered Entity" (CE)
Corrective Action Plan
July 22, 2009

Finding #	Finding	CE Response	CE Corrective Action Plan (CAP)	CMS Response
CE - 1	CE should conduct a formal, documented risk assessment for system corporate reporting tool and applications which house, process, or transmit EPHI. For each threat identified, the risk assessment should include: • likelihood of occurrence; • impact severity; • mitigating control(s); and, • risk level. The risk assessment should be conducted in accordance with CE's "HIPAA Risk Assessment and Risk Management" procedure. After an initial risk assessment has been conducted, CE should conduct an analysis to determine the appropriate interval for conducting these assessments, based on the current interval of 12-18 months. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, RA-4, "Risk Assessment Update" recommends that risk assessments be performed on	I. mm/dd/yy - full HIPAA Security Audit. II. mm/dd/yy- A risk assessment was performed on a new critical EMR application. III. We have established a committee called the CE Data Security Governance Committee.	I. We will review the technical process for each individual application and our overall system security plan. II. We will identify a baseline of the inventory of information assets and responsible data stewards--our first step in identifying our assets so that we can do a risk assessment. **Note:** Our technical resources are severely limited in 2008 due to the planned go live of a major electronic medical record application. Target Dates for completion of CAP Steps: I. mm/dd/yy II. mm/dd/yy III. mm/dd/yy	**July22, 2009** – CMS acknowledges "Covered Entity" (CE) response to Finding # 1 identified by the requirement to conduct formal documented risk assessment and to determine through analysis the appropriate intervals for conducting risk assessments. We also acknowledge the CE planned corrective action plan (CAP) steps. CMS acknowledges that your CAP is incomplete. Please provide a status report not later than August 22, 2009 showing progress in the satisfaction of this finding and include the following: 1. Evidence that CE performed the HIPAA Security Audit; 2. Evidence that CE performed a HIPAA Security Risk Assessment on the new critical EMR application; 3. Evidence that CE Data Security Governance Committee (DCGC) identified all assets that contain ePHI; 4. Evidence that CE has defined a risk assessment schedule for all assets that contain ePHI; 5. Evidence that CE has conducted one or more risk assessments in accordance with the schedule prepared by the DSGC; 6. A copy of the CE Policy and Procedure specifying that risk assessments must be performed, the period and the procedure for conducting the risk assessments.

- Other Investigations
  - “piggy backing”on HIPAA/HITECH
    - National Labor Relations Board
      - Reviewing breach investigation of CE

Cascade
HEALTHCARE COMMUNITY

Final Tips

- Do your due diligence with each and every breach
  Especially with the new HITECH
  "harm threshold" provision
- Anticipate mini meltdowns
- Know your support team and the VP's that's "got your back"
- Work the plan
  - Stay on top of the CAP due dates even if your organization hasn't met full implementation of the CAP
  - Action plans take TIME! Set realist goals and time lines

Cascade
HEALTHCARE COMMUNITY

OCR Vows ‘Vigorous Enforcement’ of Security as well as Privacy

Cascade
HEALTHCARE COMMUNITY

Ironic

- Department of the Army/FBI
  - Thumb drive - data Lost

Cascade
HEALTHCARE COMMUNITY

Thomson Reuters 100 Top Hospitals: Health System Quality/Efficiency Benchmarks

CHC named one of top 50 hospital systems nationwide for quality and efficiency

In a recent study conducted by Thomson Reuters, a leading source of health research and information, Cascade Healthcare Community was named one of the top 50 health systems in the nation for quality and efficiency.

“Providing the safest care for our patients with the best possible outcomes is something we strive for every day at Cascade Healthcare Community,” said James A. Diegel, president and CEO of CHC. “To be recognized alongside 49 other top-performing health systems in the nation, including the Cleveland Clinic and the Mayo Clinic, by a respected research organization is a true achievement.”

According to Thomson Reuters, the study evaluated all U.S. health systems with two or more short-term, general, non-federal hospitals. Researchers looked at five metrics that gauge clinical quality and efficiency including mortality, medical complications, patient safety, average length of stay and adherence to clinical standards of care.

In total, the study evaluated quality measures for 252 health systems using information from the 2006 and 2007 Medicare Provider Analysis and Review data sets and the Centers for Medicare and Medicaid Services Hospital Compare data sets.

Cascade
HEALTHCARE COMMUNITY

Questions?