



Out of Sight, Out of Control:
Uncovering the Hidden Data Security
Risks of Connected Medical Devices

January 20, 2011

THE HEALTH SHIRT

IT'S FORMFITTING,
HANDWASHABLE
AND HAS SIX
PHYSIOLOGIC SENSORS
AND ELECTROCARDIOGRAPHIC
ELECTRODES

SHAME
IT
DOESN'T
GO WITH
THOSE
PANTS



NIK
SCOTT

Device #1

- ◆ Operating System: Windows NT (1996)
- ◆ Patches/Updates: Periodically
- ◆ Anti-virus: No
- ◆ Application Software: one off

Device #2

- ◆ Operating System: UNIX 5 (1999)
- ◆ Patches/Updates: No
- ◆ Anti-virus: No
- ◆ Application Software: one off

Device #3

- ◆ Operating System: Windows 2000
- ◆ Patches/Updates: Yes (from manufacturer)
- ◆ Anti-virus: No
- ◆ Application Software: one off

Device #4

- ◆ Operating System: Windows NT (1996)
- ◆ Patches/Updates: At owners risk
- ◆ Anti-virus: At owners risk
- ◆ Application Software: one off

Device #5

- ◆ Operating System: Windows 2000
- ◆ Patches/Updates: No
- ◆ Anti-virus: No
- ◆ Application Software: one off

Device #6

- ◆ Operating System: Solaris 8 (2000)
- ◆ Patches/Updates: No
- ◆ Anti-virus: No
- ◆ Application Software: one off

Device #7

- ◆ Operating System: Redhat Linux (2001)
- ◆ Patches/Updates: No
- ◆ Anti-virus: No
- ◆ Application Software: one off

Device #8

- ◆ Operating System: MS DOS 3.3 (1986)
- ◆ Patches/Updates: No
- ◆ Anti-virus: No
- ◆ Application Software: one off

Device #9

- ◆ Operating System: Unix (1999)
- ◆ Patches/Updates: Yes
- ◆ Anti-virus: No
- ◆ Application Software: one off

Operating System: Windows NT (1996)
Patches/Updates: Periodically
Anti-virus: No
Application Software: one off
Year Introduced: 2001

Device #1



**GE CIC Pro
Patient Monitoring
System**

Operating System: UNIX 5 (1999)
Patches/Updates: No
Anti-virus: No
Application Software: one off
Year Introduced: 2004

Device #2

**BioMerieux - Vitek
Microbial Identification
and Antibiotic
Susceptibility
Testing System**



Operating System: Windows 2000 (2000)
Patches/Updates: Yes (from manufacturer)
Anti-virus: No
Application Software: one off
Year Introduced: 2003

Device #3



**Kodak – DirectView CR
Radiology Plate Reading
Device**

Operating System: Windows NT (1996)
Patches/Updates: At owners risk
Anti-virus: At owners risk
Application Software: one off
Year Introduced: 2004

Device #4

Sysmex X-Series Automated Hematology Analyzer



Operating System: Windows NT (1996)

Patches/Updates: No

Anti-virus: No

Application Software: one off

Year Introduced: 1996

Device #5

**Siemens - Sireskop
Fluoroscopy Machine**



Operating System: Solaris 8 (2000)
Patches/Updates: No
Anti-virus: No
Application Software: one off
Year Introduced: 2003

Device #6

**Phillips Digital Diagnost
Traditional x-ray
machine**



Operating System: Redhat Linux (2001)
Patches/Updates: No
Anti-virus: No
Application Software: one off
Year Introduced: 2005

Device #7



**Phillips - HD3
Ultrasound Machine**

Operating System: MS DOS 3.3 (1986)
Patches/Updates: No
Anti-virus: No
Application Software: one off
Year Introduced: unknown

Device #8



GE 9600 C-Arm
Radiology/Flouroscopy
Mobile C-Arm

Operating System: Unix
Patches/Updates: Yes
Anti-virus: No
Application Software: one off
Year Introduced: 2003

Device #9



**GE 1.5T Signa Excite
HD MRI System**

So what?



“You caught a virus from your computer and we had to erase your brain. I hope you’ve got a back-up copy!”

Background: the need

- Virus infected medical devices
- Known gap between IT and CE
- Healthcare audits – a pattern of failures
- Increased funding = increased scrutiny
- Economic environment demands reduced risk of downtime/patient diversion

Background: the need

- Vast Variety of Operating Systems
- No built in way to detect "attacks"
- Easier target for hackers?
- Casual treatment of medical devices as general platforms
- Mandatory breach reporting
- Increased and sometimes mandatory penalties with fines as high as \$1.5M/standard/year
- Federal criminal and state civil enforcement

Background: the need

- Healthcare cyber attacks up 85% in 2007
(Healthcare organizations feeling cyber attacks growing, NetworkWorld.com, 27 February 2008) Cyber Attacks on Healthcare Organizations Double in 4Q
(Secureworks, 27 February 2010)
- 6,325,393 Breaches reported since September 2009
(<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>)
- Misdirected spyware infects Ohio hospital (IDG News Service, 18 September 2009)

Background: the need

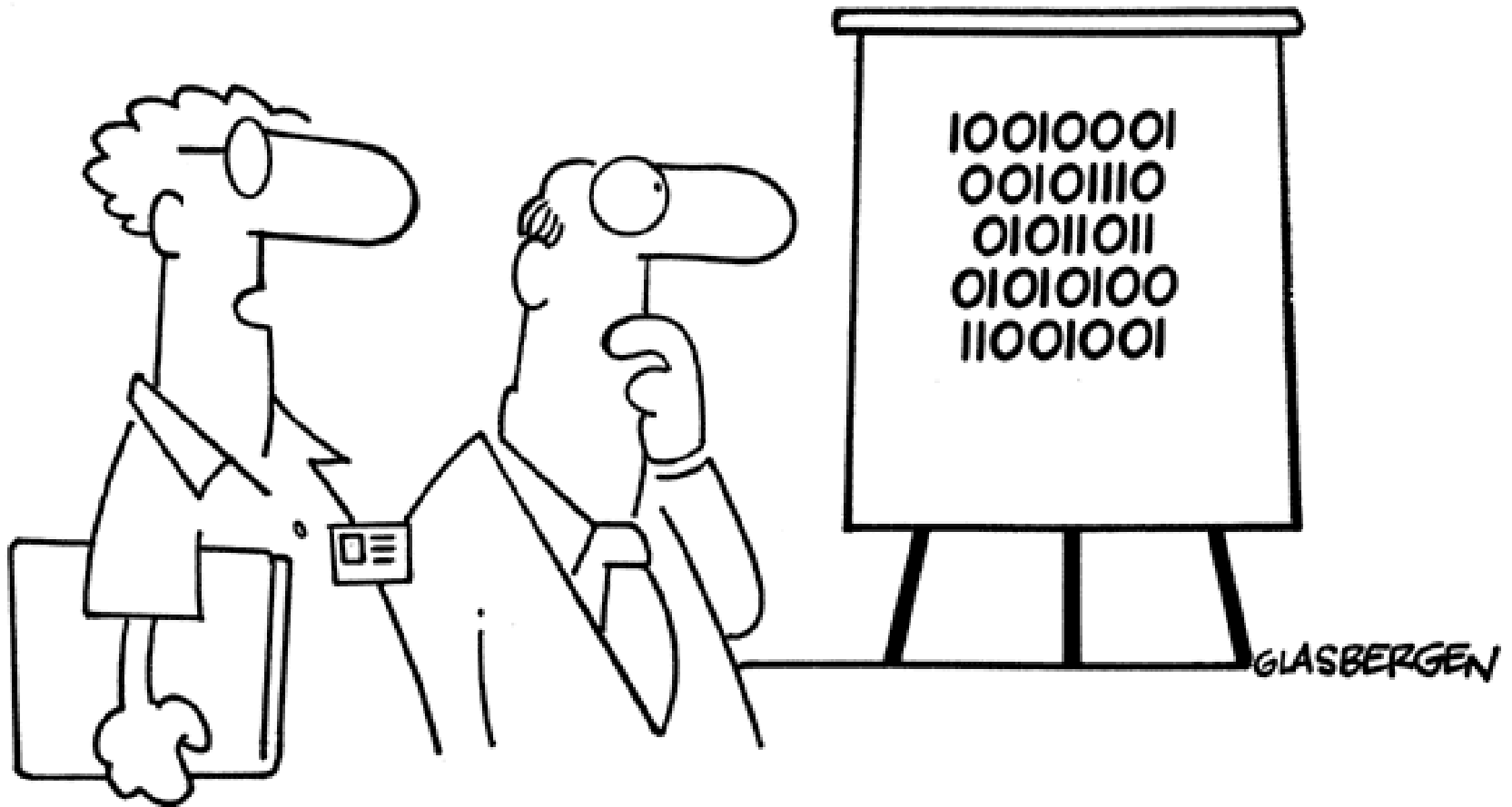
- 90% of all respondents have had a breach in the past 24 months (Are You Ready for HITECH?, Ponemon, November 2009)
- Hackers May Prey on Medical Devices (MD&DI, March 2009)
- Hospital privacy leak could harm patients (Las Vegas Sun, 23 November 2009)
- Patient ID Theft Rises (WSJ, 29 November 2009)

Background: the need

- Jailed – Former UCLA Healthcare System surgeon illegally accessed medical records (4 months and \$2,000 fine)
- Palmetto General Hospital employee and accomplice sentenced for stealing patient records (www.databreaches.net/?p=8054)
- State Attorney General – CT files first HIPAA-related lawsuit (USDC CT CIV. NO. 3:10-CV-57 (PCD))
- CVS & RiteAid each settled for \$1M or more in fines

Okay, what now?

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



**“We’ve devised a new security encryption code.
Each digit is printed upside down.”**

Issues to Address

- Policy & procedure alignment
- Comprehensive networked medical device inventory
- Network information for connected medical devices
- Centralized MDS² database
- Risk assessment
- Comprehensive list of recommended actions
- Action Plan in the event of a breach
- Device Security

Issues to Address

- Policy & procedure alignment
 - Do they address all Security Issues?
 - Do they reflect actual practice?
 - How often are they reviewed?
 - Who reviews them?

Issues to Address

- Comprehensive networked medical device inventory
 - Does it contain every device that generates, stores or transmits ePHI? (mobile, intermittent connections)
 - Do you maintain a record of the OS version, application version, updates and patches?
 - Who owns the device?
 - Who is responsible for repairs or upgrades?
 - Who reviews what logs?

Issues to Address

- Network information for connected medical devices
 - Does the device connect to the network?
 - How does it connect? (can be more than one way)
 - Is the connection continuous or intermittent?
 - Do you know the IP Address, MAC Address?
 - Who is the device permitted to communicate with?
 - Who decides what patches or updates get applied?

Issues to Address

- Centralized MDS² database
 - Do you maintain such a database?
 - Who is responsible for obtaining the MDS²'s? (supply chain, device owner, CE, IT)
 - Is the database centralized or located at each department?
 - Who updates it as patches or updates are applied?

Issues to Address

- Risk assessment
 - Has one been done that includes networked medical devices?
 - Does it include devices that are not connected but generate or store ePHI?
 - Who participates in its development?
 - Who is responsible for reducing risks discovered?
 - Is it updated regularly (at least as often as changes are implemented)?

Issues to Address

- Comprehensive list of recommended actions
 - Has such a list been generated from the risk assessment?
 - Who updates it?
 - Who is responsible for reducing risk?
 - Who are they responsible to?

Issues to Address

- Action Plan in the event of a breach
 - What is the plan?
 - Who gets contacted/notified?
 - Who is responsible for remediation?
 - Who are they responsible to?
 - Who pays for it?
 - Who determines the device's usability?
 - Who regularly reviews the plan?

Issues to Address

- Device Security
 - When do you start asking these questions?
 - Does the device have internet access? Why?
 - What is it used for when not “testing”?
 - Is it in a “secure” area?
 - Does it require a unique logon?
 - Does it automatically log off after a predetermined period of time?
 - Who is it allowed to communicate with?

Issues to Address

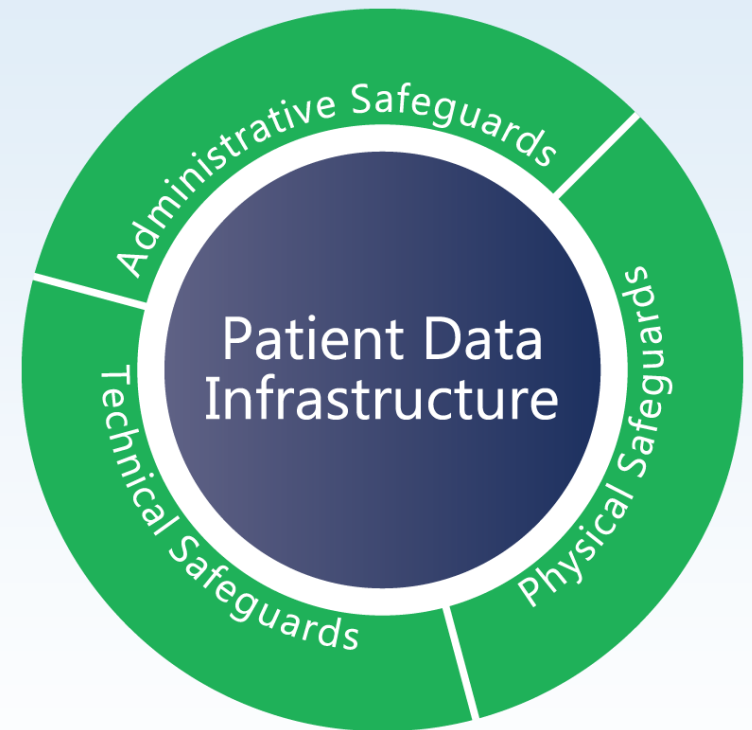
- Device Security
 - Can you add anti-virus software?
 - Does the device display ePHI?
 - If so, can it be viewed by a casual observer?
 - Does it transmit or receive ePHI?
 - If so, how?
 - Are login attempts monitored?
 - Are passwords required to be changed?
 - Is there a data discovery procedure for the device?
 - Is the storage media reused?
 - Lifecycle Management
 - End of life data removal (verified, documented, etc.)

Issues to Address

- Device Security
 - VLAN?
 - NIDS/NIPS?
 - Security Research Vendor?
 - Vulnerability Analysis Vendor?
 - Encryption?

Change Management

- ◆ Equipment Owner
- ◆ Clinical Engineering
- ◆ Risk Management
- ◆ Supply Chain
- ◆ Information Technology
- ◆ Facilities/Infrastructure
- ◆ Clinicians
- ◆ Device Operators





"THE COMPUTER LINKS ME TO OTHER DOCTORS, SO I CAN SEE WHAT THEY CHARGE."

Additional Resources

- HIPAA: 45 CFR 160, 162 and 164
- Security Rule: 45 CFR 160
 - Subparts of 164 A and 164 C
 - www.hhs.gov/ocr/privacy/index.html
- HIPAA Security Series (7 parts)
 - [/www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf)
- NIST (www.nist.gov)

Thank you.
Questions?

Earl.Reber@eProtex.com

www.eProtex.com

(317) 275-1506