

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

February, 2013

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---

# Computer Viruses Are "Rampant" on Medical Devices in Hospitals

A meeting of government officials reveals that medical equipment is becoming riddled with malware.

By David S. Gelles and Lawrence H. White



PHOTO COURTESY OF GE HEALTHCARE; GRAPHIC COURTESY OF GE HEALTHCARE

---

---

---

---

---

---

---

---

---

---

## How is this "Compliance" related?

- HIPAA
  - First "Implementation Specification"
    - 45 CFR § 164.308(a)(1)(ii)(A)
    - Risk Analysis (risk of what?)
  - Often mistakenly thought of as an IT compliance issue
- Meaningful Use
  - Stage 1 - Core Objective and Measure 15
  - Conduct or review a HIPAA security risk analysis
  - Positive reinforcement but what are the penalties for falsely attesting?



---

---

---

---

---

---

---

---

---

---

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

## Device #2



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 #3



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 #4



Siemens - Sireskop  
Fluoroscopy Machine



---

---

---

---

---

---

---

---

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

## Device #5



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



---

---

---

---

---

---

---

---

## Really?

- Pyxis Medstation 3000
  - Siemens MagicView 1000
  - Hologic Fluoroscan C-Arm
  - Philips Sonos 5500 US
  - FocalSim Radiology System
  - Fuji Smart CR FCR XG-1
  - GE Multi C MPI Vasc Lab
  - SHIMADZU YSF-300 Flouro
- Windows 2000  
Windows XP  
Windows XP Prof  
Windows XP Embed  
Windows Server 2003  
Windows XP SP1  
Windows 2000  
Windows 2000



---

---

---

---

---

---

---

---

So what?

---

---

---

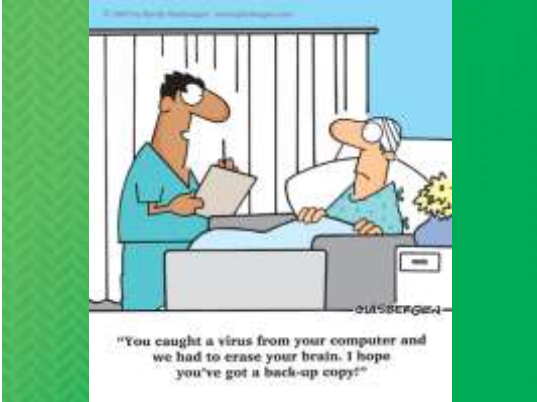
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

## Background: the need ▶

- **CMS starts Meaningful Use attestation audits**
  - "The Centers for Medicare & Medicaid Services (CMS) has quietly begun to audit providers who have received payments under the EHR incentive program . . ." (FierceEMR, 23 July 2012)
- **OCR's Leon Rodriguez: HIPAA enforcement more critical with transition to EHR's**
  - "One issue with the security rule in the audits is electronic protected health information," Rodriguez said. "With EHR's, there's a wide variety of places where ePHI is stored. So you need a real analysis of where it exists . . ." (FierceEMR, 12 October 2012)
- **Energy Department Is the Latest Victim of an Online Attack**
  - "It's a continuing story of negligence. . . the agency continued to have security issues despite the fact that *it manages the most sophisticated military and intelligence technology the country owns.*" (The New York Times, 04 February 2013)




---

---

---

---

---

---

---

---

---

---

## 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)
- **Cyber attacks up 400% since 2011** ([infosecurity-magazine.com/view/27876/cyberattacks-up-400-since-2011/](http://infosecurity-magazine.com/view/27876/cyberattacks-up-400-since-2011/), 05 February 2013)
- **Main Sources of Data Breaches: Lost or Stolen Computing Device (46%); Employee Mistakes or Unintentional Actions (42%) and Third Party Snafus (42%)** (Third Annual Benchmark Study on Patient Privacy & Data Security, Ponemon)
- **Criminal Attacks: Increased from 20% in 2010 to 33%** (ibid.)




---

---

---

---

---

---

---

---

---

---

## Background: the need

- Over 21,471,000 Breached records reported since September 2009 (<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>)
- Over 500 Breaches of >500 records
  - Nearly half due to theft
  - Nearly 1/3 involve laptops/portable devices
  - Nearly ¼ involve business associates
- 34,000+ reports of breaches <500 records
- Privacy & Security Rule related complaints total over 70,000 (almost 2/3 have corrective action)



---

---

---

---

---

---

---

---

## Background: the need

- Misdirected spyware infects Ohio hospital (IDG News Service, 18 September 2009)
- 94% of all respondents have had a breach in the past 24 months (Third Annual Benchmark Study on Patient Privacy & Data Security, Ponemon, December 2012)
- Security "All e-PHI created, received, maintained, or transmitted by an organization is subject to the HIPAA Security Rule" (10 IT initiatives your hospital should undertake in 2012, Healthcare IT News)



---

---

---

---

---

---

---

---

## Background: the need



---

---

---

---

---

---

---

---

## Background: the need



eProtex

---

---

---

---

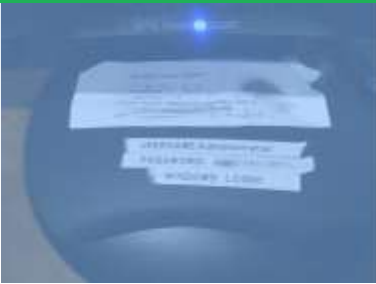
---

---

---

---

## Background: the need



eProtex

---

---

---

---

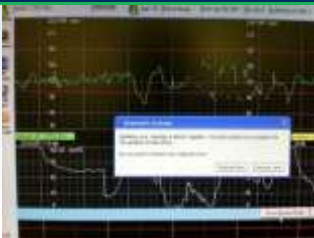
---

---

---

---

## Background: the need



<http://www.geek.com/articles/geek-cetera/birth-monitor-demands-windows-restart-as-mom-begins-to-push-20110415/>

eProtex

---

---

---

---

---

---

---

---

## Background: the need

- Jailed – Former UCLA Healthcare System surgeon illegally accessed medical records (4 months and \$2,000 fine)
- Unauthorized user accessed and encrypted ePHI for ransom (SEND2PRESS NEWSWIRE, 20 July 2012)
- State Attorney General – CT files first HIPAA-related lawsuit (USDC CT CIV. NO. 3:10-CV-57 (PCD))
- HHS imposes first CMP for HIPAA violations ([www.hhs.gov/news/press/2011pres/02/20110222a.html](http://www.hhs.gov/news/press/2011pres/02/20110222a.html))



---

---

---

---

---

---

---

---

## Background: the need

- Hospital Hack: As healthcare goes digital, infiltrators arrive over the internet (Divided we stand, 01 December 2012)
- Health-care sector vulnerable to hackers, researchers say (The Washington Post, 25 December 2012)
- Ransom, implant attack highlight need for healthcare security ([www.csoonline.com/article/725880](http://www.csoonline.com/article/725880), 08 January 2013)
- Vulnerable medical devices: A clear and present danger (TechRepublic 14 January 2013)
- Patient data revealed in medical device hack (SC Magazine, 17 January 2013)



---

---

---

---


---

---

---

---

## Background: the need

- Historic gap between IT and CE
- Increased funding = increased scrutiny
- Economic environment demands reduced risk of downtime/patient diversion
- Vast Variety of Operating Systems
- Easier target for hackers?
- Casual treatment of medical devices as general platforms
- No built in way to detect “attacks” 

---

---

---

---

---

---

---

---



# Okay, what now?

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---

## 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 MDS<sup>2</sup> database
  - Do you maintain such a database?
  - Who is responsible for obtaining the MDS<sup>2</sup>'s? (supply chain, device owner, CE, IT)
  - When are they obtained?
  - Is the database centralized or located at each department or at the individual device?
  - 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 your Privacy Officer? Security Officer?
  - 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 and to whom?
  - Are login attempts monitored?
  - Are passwords required to be changed?
  - Is there a data recovery 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?
  - MDDS Final Rule?
  - Mobile Medical Applications - Draft Guidance?
  - Business Associates?



---

---

---

---

---

---

---

---

## Change Management

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



eProtex

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---

## 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](http://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](http://www.nist.gov)

eProtex

---

---

---

---

---

---

---

---

