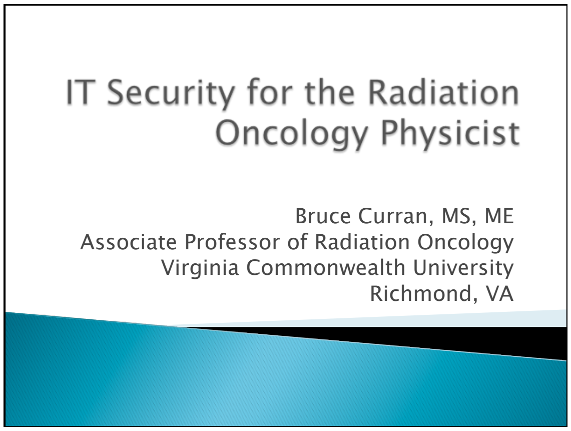
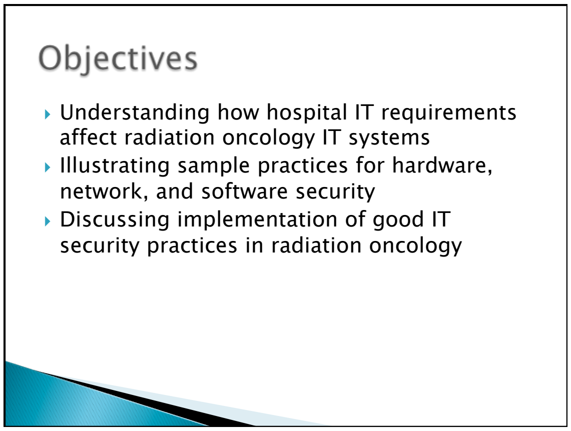


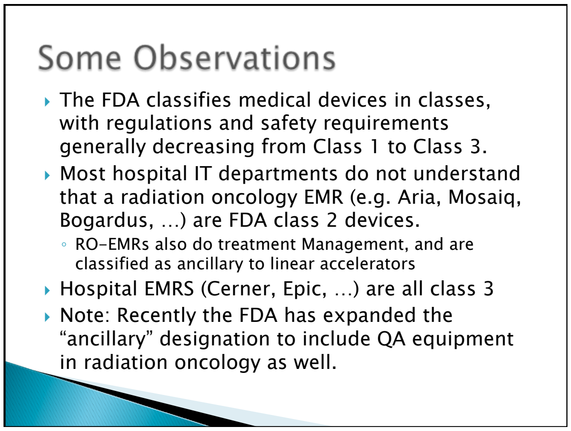
IT Security for the Radiation Oncology Physicist

Bruce Curran, MS, ME
Associate Professor of Radiation Oncology
Virginia Commonwealth University
Richmond, VA



Objectives

- Understanding how hospital IT requirements affect radiation oncology IT systems
- Illustrating sample practices for hardware, network, and software security
- Discussing implementation of good IT security practices in radiation oncology



Some Observations

- The FDA classifies medical devices in classes, with regulations and safety requirements generally decreasing from Class 1 to Class 3.
- Most hospital IT departments do not understand that a radiation oncology EMR (e.g. Aria, Mosaiq, Bogardus, …) are FDA class 2 devices.
  - RO-EMRs also do treatment Management, and are classified as ancillary to linear accelerators
- Hospital EMRS (Cerner, Epic, …) are all class 3
- Note: Recently the FDA has expanded the “ancillary” designation to include QA equipment in radiation oncology as well.

Medical Data Breaches

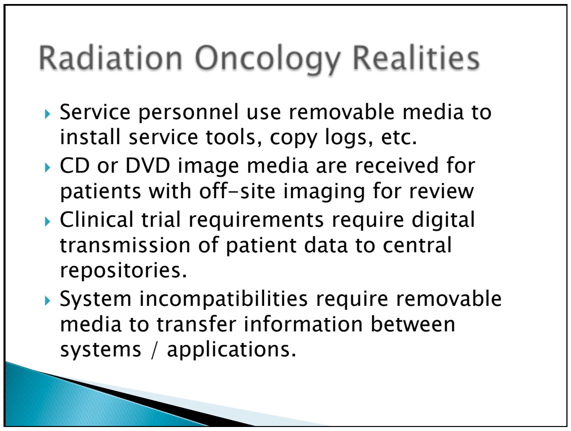
- While a stolen Social Security number might sell for 25 cents in the underground market, and a credit card number might fetch $1, "A comprehensive medical record for me to get free surgery might be $1,000," Halamka says. "It is a commodity that is hot on the black Internet [market].“
  - http://www.databreachtoday.com/hackers-are-targeting-health-data-a-7024

What HIPAA (and/or IT) wants

- Detection of unauthorized access or attempted access.
- Unique, individual logins for all users
- Strong, unique passwords, changed on a regular basis
- Password-protected screen savers, with timeouts of 2 - 10 minutes
- PHI data cannot be easily removed
  - No local PHI storage on computers that might be stolen
  - Removable devices cannot be used to copy PHI data and remove illicitly.
- Foreign/unknown applications cannot be run on local workstations
- Regular updating of anti-virus software and security patches for safeguarding workstations.

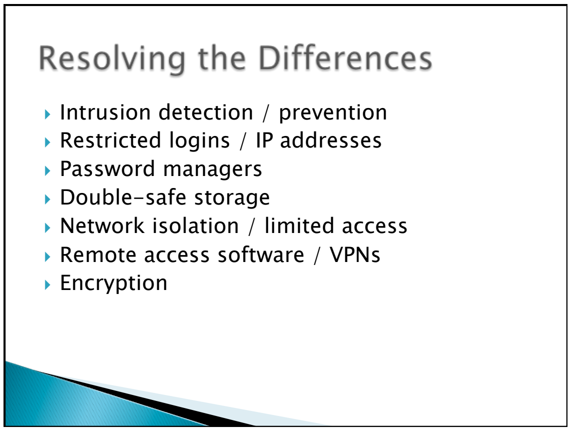
Radiation Oncology Realities

- Many systems are based on generic passwords for multiple users.
  - Permission and access structures do not allow necessary access/sharing for multiple logins.
- Systems have different requirements and legal character sets, not always in sync with institution password requirements.
  - Often systems do not allow non-alphanumeric characters.
- Time required, e.g. setting up a patient, is incompatible with short unprotected access intervals to a workstation.
- Multiple users access the same workstation and applications; logout / login process loses data and inserts significant delays in the radiation oncology process.



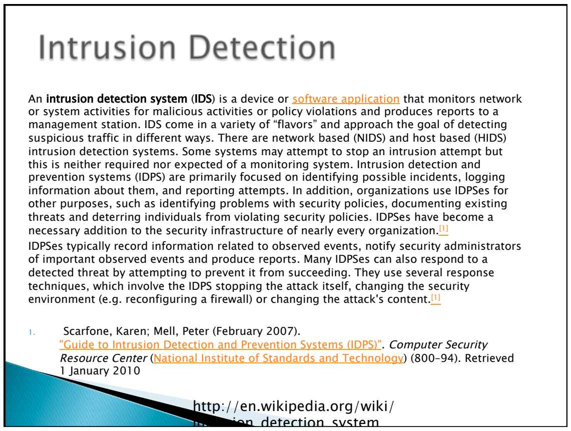
Radiation Oncology Realities

- Service personnel use removable media to install service tools, copy logs, etc.
- CD or DVD image media are received for patients with off-site imaging for review
- Clinical trial requirements require digital transmission of patient data to central repositories.
- System incompatibilities require removable media to transfer information between systems / applications.



Resolving the Differences

- Intrusion detection / prevention
- Restricted logins / IP addresses
- Password managers
- Double-safe storage
- Network isolation / limited access
- Remote access software / VPNs
- Encryption



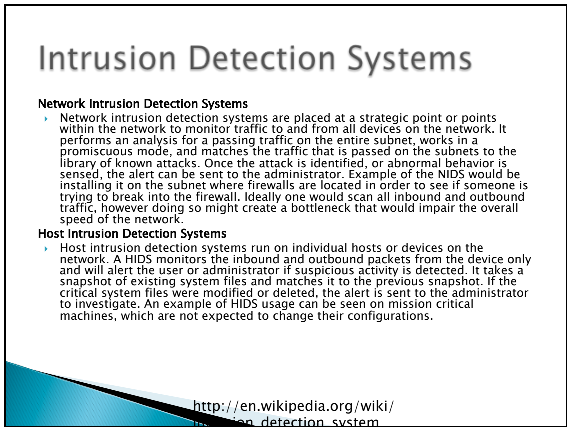
Intrusion Detection

An **intrusion detection system** (**IDS**) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.[1]

IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.[1]

1. Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)". *Computer Security Resource Center* (National Institute of Standards and Technology) (800-94). Retrieved 1 January 2010

http://en.wikipedia.org/wiki/
Intrusion_detection_system



Intrusion Detection Systems

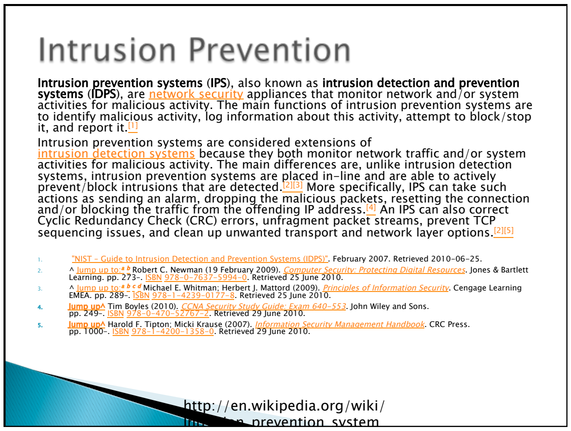
Network Intrusion Detection Systems

- Network intrusion detection systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis for a passing traffic on the entire subnet, works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of known attacks. Once the attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. Example of the NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.

Host Intrusion Detection Systems

- Host intrusion detection systems run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

http://en.wikipedia.org/wiki/Intrusion_detection_system



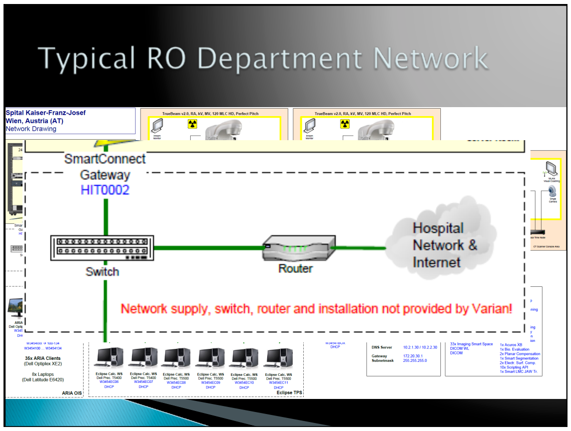
Intrusion Prevention

Intrusion prevention systems (**IPS**), also known as **intrusion detection and prevention systems** (**IDPS**), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.[1]

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected.[2][3] More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.[4] An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.[2][5]

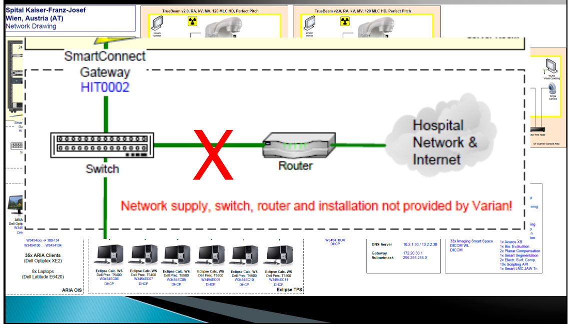
1. "NIST – Guide to Intrusion Detection and Prevention Systems (IDPS)". February 2007. Retrieved 2010-06-25.
2. ^ Jump up to:a b Robert C. Newman (19 February 2009). *Computer Security: Protecting Digital Resources*. Jones & Bartlett Learning. pp. 273–. ISBN 978-0-7637-5994-0. Retrieved 25 June 2010.
3. ^ Jump up to:a b c d Michael E. Whitman; Herbert J. Mattord (2009). *Principles of Information Security*. Cengage Learning EMEA. pp. 289–. ISBN 978-1-4239-0177-8. Retrieved 25 June 2010.
4. **Jump up^** Tim Boyles (2010). *CCNA Security Study Guide: Exam 640-553*. John Wiley and Sons. pp. 249–. ISBN 978-0-470-52767-2. Retrieved 29 June 2010.
5. **Jump up^** Harold F. Tipton; Micki Krause (2007). *Information Security Management Handbook*. CRC Press. pp. 1000–. ISBN 978-1-4200-1358-0. Retrieved 29 June 2010.

http://en.wikipedia.org/wiki/Intrusion_prevention_system



Typical RO Department Network

Typical RO Department Network (Isolated)



Network supply, switch, router and installation not provided by Varian!

User Accounts / Passwords

- Manufacturers are working to restructure their software to allow independent logins.
- It is possible to restrict a user account for use on a limited set of workstation(s).
  - For example, a "non-user specific" login that can only be used at workstations for a specific treatment machine or TPS workstation
- IP addressing can be used to isolate specific workstations from general access, including limited internet access
  - Remove DNS resolution and define all needed IP addresses in host tables

3.1 Active Directory Design Guidelines

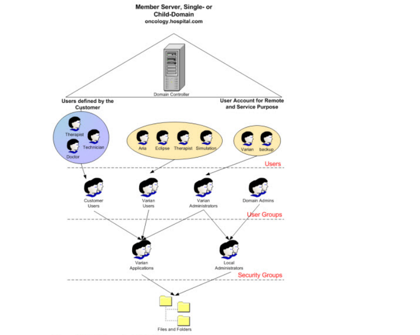
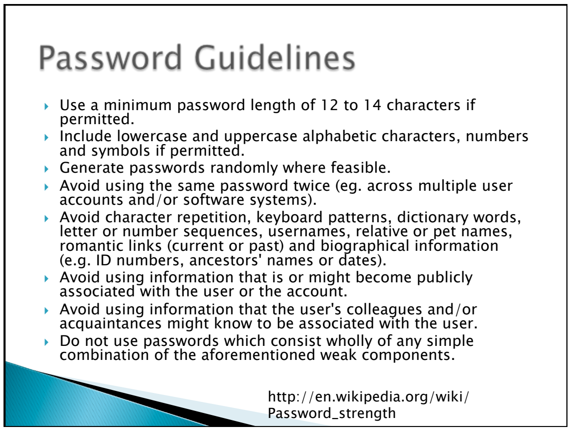


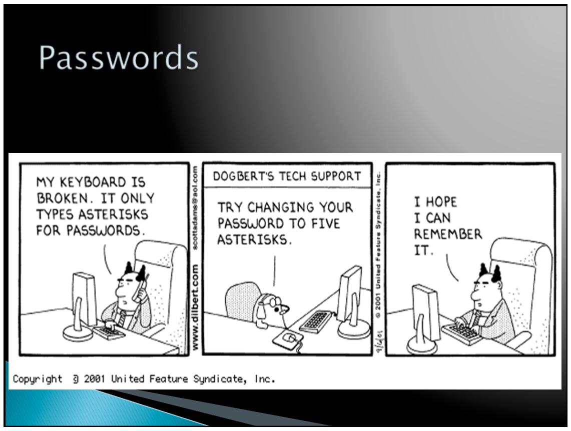
Figure 8: AD Security Guideline



Password Guidelines

- Use a minimum password length of 12 to 14 characters if permitted.
- Include lowercase and uppercase alphabetic characters, numbers and symbols if permitted.
- Generate passwords randomly where feasible.
- Avoid using the same password twice (eg. across multiple user accounts and/or software systems).
- Avoid character repetition, keyboard patterns, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past) and biographical information (e.g. ID numbers, ancestors' names or dates).
- Avoid using information that is or might become publicly associated with the user or the account.
- Avoid using information that the user's colleagues and/or acquaintances might know to be associated with the user.
- Do not use passwords which consist wholly of any simple combination of the aforementioned weak components.

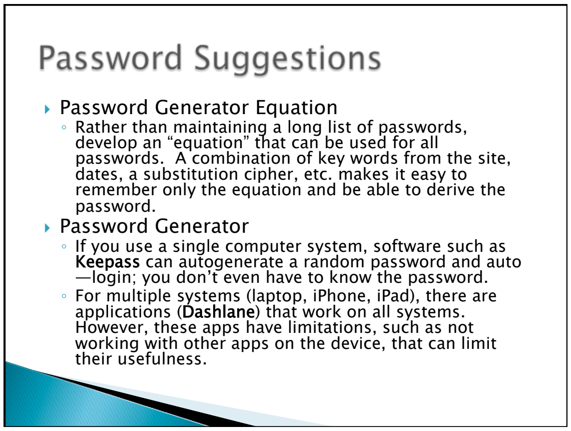
http://en.wikipedia.org/wiki/Password_strength



Passwords

MY KEYBOARD IS BROKEN. IT ONLY TYPES ASTERISKS FOR PASSWORDS.
scottadams@aol.com
www.dilbert.com
DOGBERT'S TECH SUPPORT
TRY CHANGING YOUR PASSWORD TO FIVE ASTERISKS.
© 2001 United Feature Syndicate, Inc.
I HOPE I CAN REMEMBER IT.

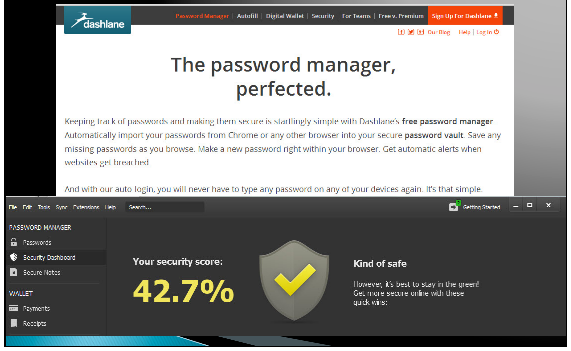
Copyright © 2001 United Feature Syndicate, Inc.



Password Suggestions

- Password Generator Equation
  - Rather than maintaining a long list of passwords, develop an “equation” that can be used for all passwords. A combination of key words from the site, dates, a substitution cipher, etc. makes it easy to remember only the equation and be able to derive the password.
- Password Generator
  - If you use a single computer system, software such as **Keepass** can autogenerate a random password and auto—login; you don’t even have to know the password.
  - For multiple systems (laptop, iPhone, iPad), there are applications (**Dashlane**) that work on all systems. However, these apps have limitations, such as not working with other apps on the device, that can limit their usefulness.

Password Managers



dashlane
Password Manager | Autofill | Digital Wallet | Security | For Teams | Free v. Premium
Sign Up For Dashlane
Our Blog
Help | Log In

The password manager, perfected.

Keeping track of passwords and making them secure is startlingly simple with Dashlane's **free password manager**. Automatically import your passwords from Chrome or any other browser into your secure **password vault**. Save any missing passwords as you browse. Make a new password right within your browser. Get automatic alerts when websites get breached.

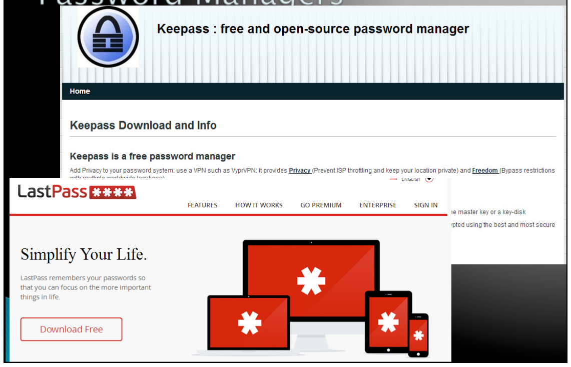
And with our auto-login, you will never have to type any password on any of your devices again. It's that simple.

Your security score: 42.7%

Kind of safe

However, it's best to stay in the green! Get more secure online with these quick wins:

Password Managers



Keepass : free and open-source password manager

Keepass Download and Info

Keepass is a free password manager

Add Privacy to your password system: use a VPN such as VyprVPN: it provides Privacy (Prevent ISP throttling and keep your location private) and Freedom (Bypass restrictions with multiple worldwide locations)

e master key or a key-disk

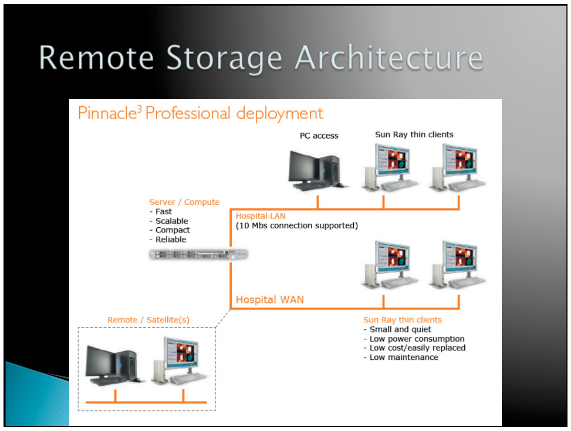
pted using the best and most secure

Simplify Your Life.

LastPass remembers your passwords so that you can focus on the more important things in life.

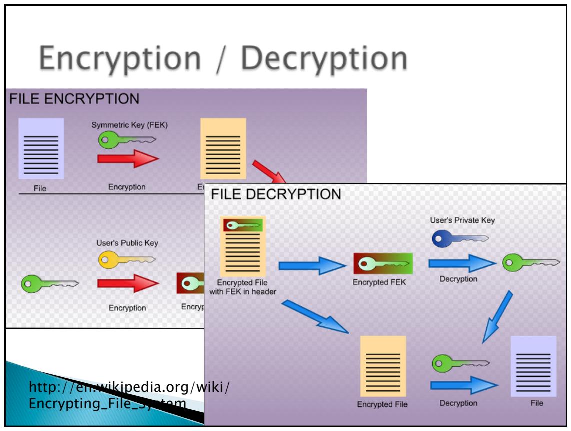
Current Practices

- Double-safe:
  - Similarly to NRC HDR regulations, most IT departments now require systems holding patient data to be behind two levels of security.
  - This is particularly true of patient databases, where large numbers of patients are stored in one system.
  - As a result, TPS storage is no longer allowed at the dosimetrist's desk; storage must be more secure.
  - Systems that have small amounts of patient data (local workstation cache, for example) are slowly being pushed to fully encrypted local storage.



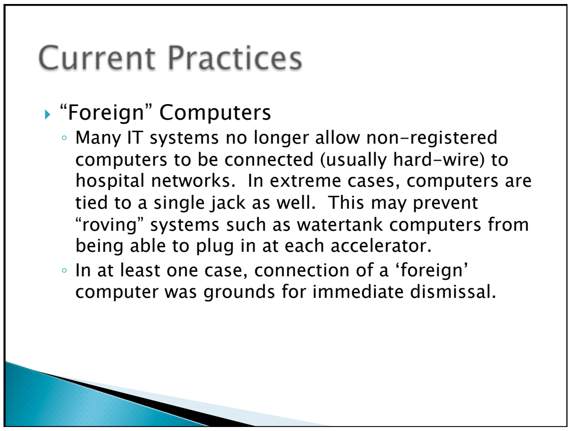
Remote Storage Architecture

Pinnacle³ Professional deployment



Encryption / Decryption

http://en.wikipedia.org/wiki/Encrypting_File_System



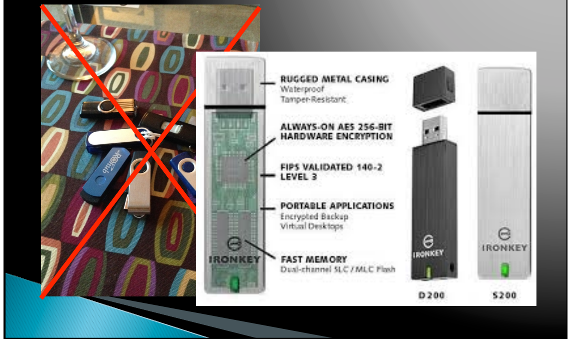
Current Practices

- “Foreign” Computers
  - Many IT systems no longer allow non-registered computers to be connected (usually hard-wire) to hospital networks. In extreme cases, computers are tied to a single jack as well. This may prevent “roving” systems such as watertank computers from being able to plug in at each accelerator.
  - In at least one case, connection of a ‘foreign’ computer was grounds for immediate dismissal.

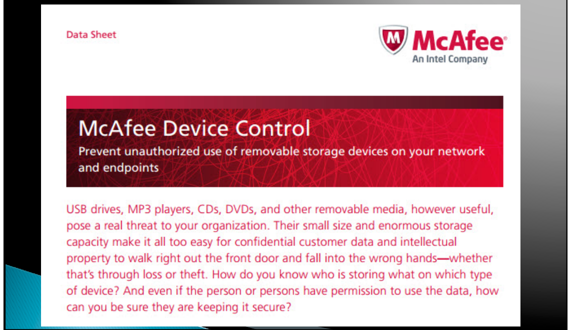
Current Practices

- Removable Devices
  - Non-encrypted (and possibly non-registered) USB devices are often not allowed to be mounted on computers within the IT network.
    - Some anti-virus+ software will check against hospital policy to only allow valid devices to be connected.
    - Cost of encrypted flash drives is much more than generic devices (~ $160 for an 8GB flash drive)
  - In some cases, USB ports are being locked up so that no devices can be plugged into them as well.

USB Devices



Device Control



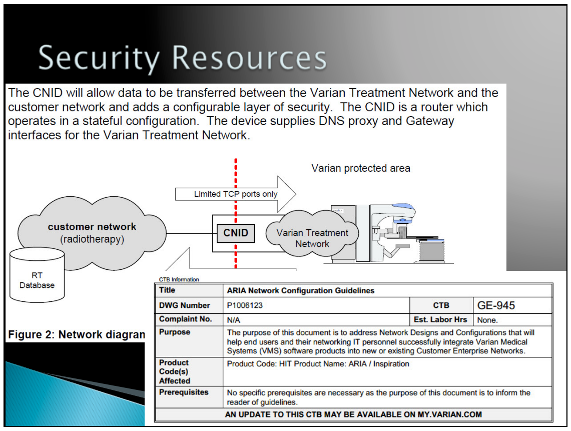
Data Sheet

McAfee
An Intel Company

McAfee Device Control

Prevent unauthorized use of removable storage devices on your network and endpoints

USB drives, MP3 players, CDs, DVDs, and other removable media, however useful, pose a real threat to your organization. Their small size and enormous storage capacity make it all too easy for confidential customer data and intellectual property to walk right out the front door and fall into the wrong hands—whether that's through loss or theft. How do you know who is storing what on which type of device? And even if the person or persons have permission to use the data, how can you be sure they are keeping it secure?



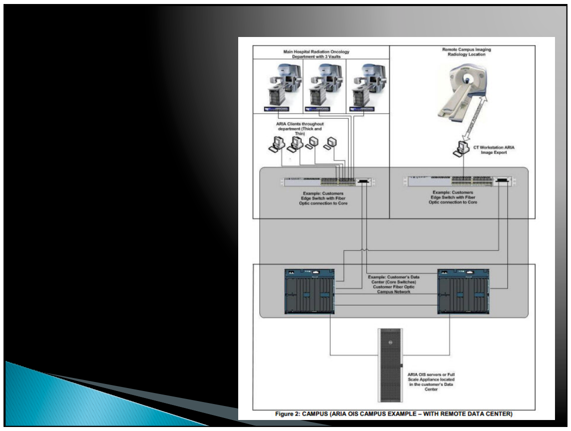
Security Resources

The CNID will allow data to be transferred between the Varian Treatment Network and the customer network and adds a configurable layer of security. The CNID is a router which operates in a stateful configuration. The device supplies DNS proxy and Gateway interfaces for the Varian Treatment Network.

Figure 2: Network diagran

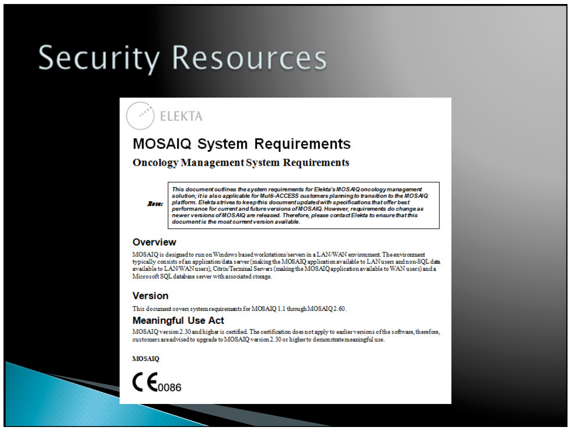
CTB Information

Title	**ARIA Network Configuration Guidelines**		
DWG Number	P1006123	**CTB**	GE-945
Complaint No.	N/A	**Est. Labor Hrs**	None.
Purpose	The purpose of this document is to address Network Designs and Configurations that will help end users and their networking IT personnel successfully integrate Varian Medical Systems (VMS) software products into new or existing Customer Enterprise Networks.		
Product Code(s) Affected	Product Code: HIT Product Name: ARIA / Inspiration		
Prerequisites	No specific prerequisites are necessary as the purpose of this document is to inform the reader of guidelines.		
AN UPDATE TO THIS CTB MAY BE AVAILABLE ON MY.VARIAN.COM			



Main Hospital Radiation Oncology Department with 3 Vaults
Remote Campus Imaging Radiology Location
ARIA Clients throughout department (Thick and Thin)
CT Workstation ARIA Image Export
Example: Customers Edge Switch with Fiber Optic connection to Core
Example: Customers Edge Switch with Fiber Optic connection to Core
Example: Customer's Data Center (Core Switches) Customer Fiber Optic Campus Network
ARIA OIS servers or Full Scale Appliance located in the customer's Data Center

Figure 2: CAMPUS (ARIA OIS CAMPUS EXAMPLE – WITH REMOTE DATA CENTER)



Security Resources

ELEKTA

MOSAIQ System Requirements

Oncology Management System Requirements

Note: *This document outlines the system requirements for Elekta's MOSAIQ oncology management solution; it is also applicable for Multi-ACCESS customers planning to transition to the MOSAIQ platform. Elekta strives to keep this document updated with specifications that offer best performance for current and future versions of MOSAIQ. However, requirements do change as newer versions of MOSAIQ are released. Therefore, please contact Elekta to ensure that this document is the most current version available.*

Overview

MOSAIQ is designed to run on Windows based workstations/servers in a LAN/WAN environment. The environment typically consists of an application/data server (making the MOSAIQ application available to LAN users and non-SQL data available to LAN/WAN users), Citrix/Terminal Servers (making the MOSAIQ application available to WAN users) and a Microsoft SQL database server with associated storage.

Version

This document covers system requirements for MOSAIQ 1.1 through MOSAIQ 2.60.

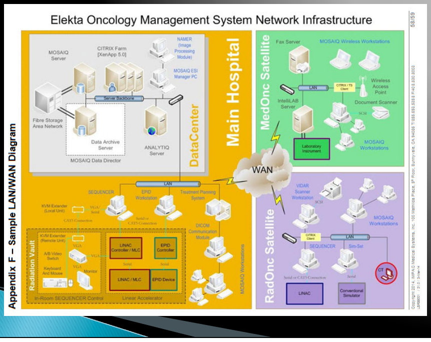
Meaningful Use Act

MOSAIQ version 2.30 and higher is certified. The certification does not apply to earlier versions of the software, therefore, customers are advised to upgrade to MOSAIQ version 2.30 or higher to demonstrate meaningful use.

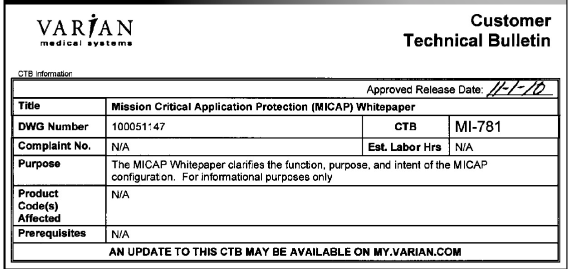
MOSAIQ

CE0086

Security Resources



Security Resources



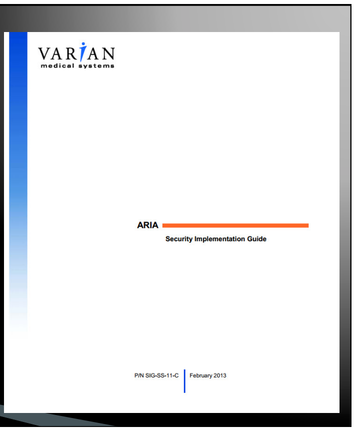
VARIAN medical systems

Customer Technical Bulletin

CTB information

		Approved Release Date: 11-1-10	
Title	**Mission Critical Application Protection (MICAP) Whitepaper**		
DWG Number	100051147	**CTB**	MI-781
Complaint No.	N/A	**Est. Labor Hrs**	N/A
Purpose	The MICAP Whitepaper clarifies the function, purpose, and intent of the MICAP configuration. For informational purposes only		
Product Code(s) Affected	N/A		
Prerequisites	N/A		
AN UPDATE TO THIS CTB MAY BE AVAILABLE ON MY.VARIAN.COM			

Security Resources



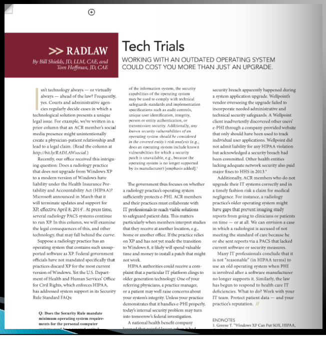
VARIAN medical systems

ARIA

Security Implementation Guide

P/N SIG-SS-11-C | February 2013

ACR Bulletin – June, 2014



>> RADLAW

By Bill Shields, JD, LLM, CAE, and Tom Hoffman, JD, CAE

Tech Trials

WORKING WITH AN OUTDATED OPERATING SYSTEM COULD COST YOU MORE THAN JUST AN UPGRADE.

Isn't technology always — or virtually always — ahead of the law? Frequently, yes. Courts and administrative agencies regularly decide cases in which a technological solution presents a unique legal issue. For example, we've written in a prior column that an ACR member's social media presence might unintentionally create a physician-patient relationship and lead to a legal claim. (Read the column at *http://bit.ly/RADLAWsocial*.)

Recently, our office received this intriguing question: Does a radiology practice that does not upgrade from Windows XP to a modern version of Windows have liability under the Health Insurance Portability and Accountability Act (HIPAA)? Microsoft announced in March that it will terminate updates and support for XP, effective April 8, 2014[1]. At press time, several radiology PACS systems continue to run XP. In this column, we will examine the legal consequences of this, and other technology, that may fall behind the curve.

Suppose a radiology practice has an operating system that contains such unsupported software as XP. Federal government officials have not mandated specifically that practices discard XP for the most current version of Windows. Yet the U.S. Department of Health and Human Services' Office for Civil Rights, which enforces HIPAA, has addressed system support in its Security Rule Standard FAQs:

> **Q: Does the Security Rule mandate minimum operating system requirements for the personal computer**
>
> of the information system, the security capabilities of the operating system may be used to comply with technical safeguards standards and implementation specifications such as audit controls, unique user identification, integrity, person or entity authentication, or transmission security. Additionally, *any known security vulnerabilities of an operating system should be considered in the covered entity's risk analysis* (e.g., does an operating system include known vulnerabilities for which a security patch is unavailable, e.g., because the operating system is no longer supported by its manufacturer) [emphasis added].[2]

The government thus focuses on whether a radiology practice's operating system sufficiently protects e-PHI. ACR members and their practices must collaborate with IT professionals to reach viable solutions to safeguard patient data. This matters particularly when members interpret studies that they receive at another location, e.g., home or another office. If the practice relies on XP and has not yet made the transition to Windows 8, it likely will spend valuable time and money to install a patch that might not work.

HIPAA authorities could receive a complaint that a particular IT platform clings to older generation technology. One of your referring physicians, a practice manager, or a patient may well raise concerns about your system's integrity. Unless your practice demonstrates that it handles e-PHI properly, today's internal security problem may turn into tomorrow's federal investigation.

A national health benefit company

security breach apparently happened during a system application upgrade. Wellpoint's vendor overseeing the upgrade failed to incorporate needed administrative and technical security safeguards. A Wellpoint client inadvertently discovered other users' e-PHI through a company-provided website that only should have been used to track individual user applications. Wellpoint did not admit liability for any HIPAA violation but acknowledged a security breach had been committed. Other health entities lacking adequate network security also paid major fines to HHS in 2013.[4]

Additionally, ACR members who do not upgrade their IT systems correctly and in a timely fashion risk a claim for medical negligence. For instance, a radiology practice's older operating system might have gaps that prevent imaging study reports from going to clinicians or patients on time — or at all. We can envision a case in which a radiologist is accused of not meeting the standard of care because he or she sent reports via a PACS that lacked current software or security measures.

Many IT professionals conclude that it is not "reasonable" (in HIPAA terms) to use an old operating system when PHI is involved after a software manufacturer no longer supports it. Similarly, the law has begun to respond to health care IT deficiencies. What to do? Work with your IT team. Protect patient data — and your practice's reputation. //

ENDNOTES

[1] Greene T. "Windows XP Can Put SOX, HIPAA,

Thank you

The image cannot be displayed. Y may not have enough memory to open the image, or th may have been corrupted. still in.