Healthcare institutions must take a proactive approach to securing medical images.

Increasingly, medical systems are becoming members of the network, and like desktops or notebooks, these systems have distinct security requirements. Security for a picture archiving and communication system (PACS) should never be taken for granted. Careful consideration must go into every element of each system that is implemented.

Four Major PACS Security Issues

The images stored in a PACS must be accurate, confidential and rapidly recoverable if lost. In addition, PACS-related medical equipment should only be accessed and administered by the appropriate personnel. There are four main areas of concern with PACSs:

- **Accurate medical information**: The purpose of a PACS is to warehouse and rapidly provide centralized medical images. Because patient care is the most important issue, PACS data must be extremely accurate. If the accuracy of medical images is compromised, patients may not be properly diagnosed and/or treated.
• Inappropriate virus scanning: Michael Fairbanks, radiology application analyst for Seattle Cancer Care Alliance, points out: “One of the biggest things that we’re concerned about is HIPAA (Health Insurance Portability and Accountability Act) compliance, specifically the privacy issues.” HIPAA requires that patient information be kept confidential, and putting medical images on a computer network automatically increases the number of security considerations organizations must address. For example, as Neil Buckley, network security manager for Partners HealthCare System in Boston, states: “We have policies restricting the use of e-mail for patient identifiable information.”

• Separate access and administration: Only specific personnel in a healthcare institution require access to particular medical images. Computed tomography (CT) and magnetic resonance imaging (MRI) service engineers should only have access to their own specific equipment. In addition, administrative tasks must be separated. For example, a radiologist and the receptionist may have computers on the same network, but only the radiologist should be able to access PACS data.

• Rapidly recover lost data: No system can be made 100 percent secure, and it is possible for any system to fail. In the event of a successful intrusion and/or system failure, medical images must be recovered rapidly.

Seven Steps to a Secure PACS

• Use approved virus scanning: Inappropriate virus scanning applications can detect viruses signatures in medical images and automatically “correct” them, altering the images. Medical images could be quarantined, slowed or arbitrarily changed without anyone’s knowledge. Under very rare circumstances, these changes could lead to inaccurate data that may conceivably cause patients to receive an incorrect diagnosis.

Virus scanning packages that can be used with PACS include McAfee Active Virus Defense Suite, Symantec AntiVirus Enterprise Edition and Trend Micro OfficeScan Client/Server Edition. Make sure that the PACS vendor provides information about what virus scanners are appropriate and information about how to correctly configure the virus scanner so it does not negatively impact a PACS.

• Use virtual local area networks (VLANs) to separate systems: A VLAN can be used to group equipment that exists in different local area networks (LANs) into one virtual network. Steven Hughes, an engineer with the U.S. Department of Veterans Affairs Medical Center, in Boston, explains that “PACS equipment must be isolated within a VLAN. ‘The VLAN can be centrally administered, so equipment can be moved but still stay on the same VLAN. A VLAN can be used to ensure that network users’ computers cannot access unnecessary equipment. A good solution to help create and manage VLANs for your entire enterprise is the Cisco IOS Enterprise product.”

• Place PACSs behind a firewall: Most healthcare institutions use firewalls to separate their internal network from the Internet. As Seattle Cancer Care Alliance’s Fairbanks states, “We have so many firewalls, sometimes it’s hard just to get some of our pieces of equipment connected.” Perceived challenges such as this may be the reason that few institutions use firewalls to separate a PACS from the rest of the network, but they should. Firewalls can be used to isolate PACS equipment from the rest of the equipment and users on the network. Using the Cisco IOS Enterprise product line, you can create and centrally manage firewalls for your VLANs.

• Require a virtual private network (VPN) for remote users: Users who access PACS data and equipment remotely should be required to log into a secure VPN. A VPN can ensure that users are only allowed to access data they are authorized to view, and that technicians are only able to administer their own medical equipment. Microsoft Internet Security and Acceleration (ISA) Server is a software solution that can help you create and administer VPNs.

• Encrypt data with Internet Protocol Security or Secure Sockets Layer: SSL can be used to encrypt data provided through a Web site. IPSec can be used to encrypt data accessed by remote users from the Internet or intranet. Data encryption stops unauthorized network access to the data as it is transferred across the wire. The use of IPSec is supported by the Cisco IOS product line.

• Use an Intrusion Detection System (IDS) and network monitoring: An intrusion detection system and network monitoring software can detect network problems and security threats before they compromise PACS data. A software solution to help identify these issues is Symantec Host Intrusion Detection System. For a hardware solution, Cisco Systems provides an IDS Network Module. GFI Network Server Monitor and Orion Network Performance Monitor are solid network monitoring solutions.

• Plan for data backup and recovery: Unfortunately, today’s rapidly evolving technologies mean a determined party may, given enough time and resources, find methods of compromising a PACS. Even the most secure systems can sometimes fail. CA’s BrightStor ARCserve Backup and Symantec Backup Exec are both high-quality enterprise backup and restore utilities. The Adaptite File Saver ESA1500 is also a network appliance that provides a hardware solution for backup and recovery and supports mobile devices. Also, look into offsite storage and hot sites for disaster recovery.

Accuracy and Confidentiality Through PACS Security

PACS must securely integrate with your existing network to ensure that PACS medical images are accurate and rapidly available. As per HIPAA, patient information must remain confidential. Following these best practices will help you achieve these goals.

Steps to Securing a PACS

Is a PACS secure against intrusion?

- Virus protection supported by PACS
- VLAN used to separate systems
- PACS is behind a firewall
- VPN required for remote access
- IPSec tunneling or SSL encryption
- IDS and network monitoring
- Data backup for rapid recovery