The Physicist's Role in IS

A. Baillie[1], G. Gibbs[2]
[1]BC Cancer Agency Centre for the Southern Interior, Kelowna, BC, Canada
[2]Colorado Associates in Medical Physics

Introduction

Medical physics has historically been involved with the most technical areas of medicine. This has led to a dependence on computer technology, so that now essentially any equipment involved with medical physics will be based on a computer.

Information Systems has historically been involved with financial and patient information systems. With the introduction of ubiquitous network infrastructure these previously separate worlds are now brought into intimate contact.

Information Systems is often seen by the organization as a corporate resource, whereas medical physics tends to be less apparent to the management. It is therefore common that IS will be given a broad mandate to be responsible for computer systems, or for information management.

On the other hand, the medical physicist is charged with ensuring that the medical equipment can be operated safely. Thus in radiation therapy the physicist is responsible for the quality of the radiation therapy equipment and for its safe use, and for the appropriate use of equipment such as treatment planning systems.

There is therefore a clear potential for conflict given that two groups can interpret that they are charged with a particular responsibility.

In a large organization this can lead to problems which are best dealt with by trying to develop an agreement which identifies where the responsibility lies. For example, one of the authors (Baillie) found it useful to develop a written understanding[1] between the

---

[1] BCCA Physics – IT Understanding

Information Technology is responsible for the provision and maintenance of a network environment and for desktop systems running Agency core applications. Physics is responsible for technical operations in radiation therapy. Often these responsibilities lead to areas of overlap where it could be unclear who should perform particular tasks. The purpose of this document is to provide guidelines that will avoid future misunderstandings.

The overriding principle in these matters is a mutual recognition that activities by one group can impact the ability of the other group to meet assigned responsibilities and therefore there is a need to restrict work to experienced individuals and to share information.

The levels of involvement of the two groups lie on a continuum depending on the type of systems involved. For example treatment planning systems, CT scanners, linacs, Unix systems tend to be primarily managed by Physics personnel, who tend to control access to these systems. Network equipment, desktop PCs, Windows NT systems tend to be primarily managed by IT and they tend to control access to them. Some

physics group and the IS group. Although there are still substantial areas where good collaboration is required, this kind of statement of understanding helps to avoid areas of conflict.

In a small organization, there may be no real IS infrastructure, and then a different issue arises. The physicist is then likely to be recognized as the *de facto* resource for all IS issues, and will run the risk of being asked to take on IS work, which will take time away from the real duties of the physicist. In this environment it is worth establishing boundaries on the areas where you give advice and intercede in problem issues. However, in order to effectively interact with IS representatives, the physicist must have a general understanding of their IS network architecture, protocols and security issues as well as understanding of the IS jargon. A basic review of these topics can be found at the end of this handout.

Specific Topics

The course organisers asked that we review various issues which may arise in setting up or managing networking and computer systems for medical physics activities.

Specifications for Servers and PCs

It is almost impossible to give specific advice in this area, because the performance of computer equipment tends to follow Moore's Law, with a doubling of performance per unit cost every 1.5 to 2 years. Therefore any equipment which is purchased is going to be outclassed very soon after purchase. However it is important to purchase systems with sufficiently high specification, because of the tongue-in-cheek Gates Law, which states that "the speed of software halves every 18 months". Thus an underpowered system will probably have trouble with future versions of the software.

---

primarily physics oriented systems, such as Varis, have an Agency-wide manifestation and these are managed by a collaborative team, with access being controlled by IT.

On physics managed systems, it is expected that changes will be made with the approval of the local physics leader (or a delegate if the leader wishes to assign this task). In general, information about the work carried out will be recorded locally only, however the physics leader is responsible for making sure that any changes which could impact the network are reported to IT.

On IT managed systems, changes will be generally made by IT staff except where:
1. No IT person is available
2. The work needs to be completed in a timeframe faster than IT can provide
3. The physics staff member has expert knowledge of the software involved.

Software installation requiring Administrative privileges can occur through an Installer account. Requests to use this account should be made to help desk and will be approved by the IT manager who in approving the request will consider the expertise of the individual and if necessary will consult the local physics leader.

An economic consequence of Moore's Law is that the latest technology can sell at a premium, while older technology is discounted, and a graph of performance against price tends to have an exponential shape. It is worth considering whether you can meet your needs by buying a product at the 'break point' in the curve where the price per performance unit starts to rise rapidly. This allow for the maximum performance at a good price, while recognising that you will be able to buy the very expensive performance next year at a much lower price.

Servers are PCs that are configured to manage large amounts of data, either in database applications or as disk storage. The important parameters on servers relate to the ability to handle data access by multiple users and therefore fast disk access, computational speed and network access are most important. For desktop PCs, computational speed, memory and good video graphics are likely to be the most important factors.

For imaging applications, the simplest and cheapest way to improve performance is to ensure that sufficient memory is installed. For example at BCCA, we routinely put 256KB of Ram into desktop PCs and 512KB of RAM into PCs that are used for imaging applications. On servers like those used for the Eclipse treatment planning database we will use 1 to 2 GB of memory.

Disk storage is now very cheap and any system should be equipped with lots of disk space. Any imaging systems will require large disk storage. For example at BCCA we find that our SomaVision systems require 16.7 MB per patient, 106 GB per year.

However take some time to consider the issues of data backup and archival as you select disks. If you decide to minimise your need for off-line backup by implementing fault tolerant disk storage the cost will increase considerably. Alternatively if you implement off-line backup the time required might become a problem as the disk size increases. You should develop a plan for off-line archival of your data. At the BCCA the official IS position is that disk space is so cheap that it will never be necessary to archive data off-line. However most software is not designed to handle large volumes of data well, and it becomes likely that users will be presented with increasingly long patient lists, etc, which will lead to operational inefficiencies.

If you are buying a software package from a manufacturer they will generally provide a recommended specification. There is little choice but to buy a system at least meeting that specification. However be aware that many manufacturers base these specifications on what is available rather than on what is needed to run their system.

Licensing

As the amount of software we use and the connectivity between applications grows, one become confronted with licensing issues more than ever. This issue can be frustrating and time consuming. It is safe to say that all vendors will expect to receive reimbursement for applications and or interfaces on a site, server or facility basis. It is extremely important during the process of acquiring new or upgrades to

hardware/software platforms that all necessary licenses be determined. Expect license fees for not only applications, but interfaces that import export media. Examples include DICOM and DICOM-RT transfer, DICOM print, DICOM storage just to name a few. Determine if the licenses are based on seats (total or active only) and if they are transferable between clients. Image transfer between your department and other departments is becoming a requirement. One can expect a license issue with different vendors at both ends of this transfer. Even attempts to perform backups can produce licensure concerns. Single client versus enterprise licenses have caused problems when attempting to perform backups of multiple PC hard drives from one workstation or server.. In summary, although it is frustrating and unpleasant, one must always research and confirm appropriate licensing for all software applications and functions.

DICOM

DICOM is an industry standard method for the exchange of data. It grew from an initiative to define standards for image transfer, but now includes modules for the transfer of other data such as radiation therapy structure data (e.g. organ contours), RT treatment beams and RT dose data. The standards are developed by the industry organisation NEMA and can be accessed at http://medical.nema.org

Data exchange using DICOM is generally better than via a proprietary mechanism, although this cannot be guaranteed since it depends on the degree to which the manufacturers have implemented the standards. DICOM defines ways to transfer all relevant data, but for much of the data it is up to the manufacturer whether a particular parameter is transferred.

The manufacturer is required to provide a conformance statement which defines what data is transferred by their DICOM interface, and what messages will be provided in the event that invalid data is sent or received. Generally the conformance statement for a piece of equipment will be available from the manufacturer, or more likely publicly available on their web-site (e.g. http://www.elekta.com/ContentInternational.nsf/pga_Frameset?openpage&url=dicom_conformance_statements) By examining the conformance statements of any 2 pieces of equipment, you will be able to determine whether the required data will be transferred.

In practice this is a very complex task and for most combinations the respective manufacturers should be able to give you a direct answer.

DICOM is an extremely complicated standard, and if you want to really understand what is going on you must expect to spend a long time studying the documentation. There are conceptual issues to be overcome, as the user must be familiar with an object-based model of information processes, and the language used in the standards can be difficult to understand initially. However there are many resources on the internet, such as http://www.rsna.org/practice/dicom/index.html, http://www.dclunie.com/medical-image-faq/html/index.html, or www.mrc-cbu.cam.ac.uk/~chris.rorden/dicom.html (there is no intent to suggest that these are particularly appropriate sites, search for DICOM to browse others).

DICOM defines both the format for the data to be transferred and the way that the transfer will occur. The DICOM implementation in a software package will determine what type of service the software can provide, e.g. it may be able to store the image sent to it, or it may be able to send data upon receiving a query requesting the data. DICOM sets up a process for the two programs which want to communicate to negotiate whether they are able to define a mutually understandable format for the data exchange. Once this has been agreed then the data is formatted as a stream of tagged data, which is sent to the receiving program, and which can be stored on disk as a DICOM file.

There are also many free or inexpensive DICOM software tools available on the internet. We have used Medical Connections DicomObjects (http://www.medicalconnections.co.uk/) to program a DICOM interface for some in-house software, and have found the Agfa DICOM Validation Tool (http://medical.agfa.com/dicom/advt.html) useful for debugging connections. (Again we do not imply any particular endorsement of these products – they just happen to be ones that we have used).

Once the software components are installed on your network, connection is generally simple. For each piece of DICOM software residing on a particular computer, you must define a name for the DICOM entity (known as the Application Entity Title, or AE Title). You must also define the port to be used (a number which is usually recommended by the manufacturer and often defaulted to 104). Then, to set up the connection, on the sending end of the connection you define the target of the transfer by specifying the IP address of the target, its defined AE Title, and the port number. Usually that will establish the connection, although some devices will also require that the receiving end specify which devices data can be transferred from.

Security

Data security must address both deliberate and accidental modification of data and system configuration. In areas which are the physicist's responsibility there is a potential for significant adverse outcomes following a breach of security requirements.

In a large organisation, the control of access from the outside world is the responsibility of the IS department. You should not compromise the firewall provisions by, e.g. connecting modem lines to PCs on the network.

The primary control of access to software is through passwords. Your organisation should have a strict policy on passwords. There must be a mechanism to ensure that passwords are regularly changed so that only the authorised users may use the systems. Users should also be encouraged to use 'strong' passwords - a good discussion of password strength for various types can be found at http://geodsoft.com/howto/password and links therein (particularly /human_passwords.htm).

Equally important is the control of access to shared disk storage. You should take responsibility to monitor the access permissions for folders which contain data which is used for patient care. In many large organizations there are shared storage areas which

are good places to store required data as it can then be widely accessed for use throughout your department. It is possible to configure the permissions and user groups to protect the data from modification by unauthorized users. (It is also wise to have a special 'physics administrator' user for this purpose to protect yourself from making changes inadvertently.) However generally the IS administrators will still have an override access to these folders, and many operating systems, are set up so that it is relatively easy for these administrators to accidentally change these permissions. You should set up a QA process to review these periodically.

Often the IS department will only allow its system administrators to have the administrator privileges which allow software installation on PCs. Software installation has the potential to introduce security breaches on the network and it is reasonable that IS should have control of this function. However your agreement between physics and IS should address whether this is appropriate and set out procedures that will allow the IS department to be able to trust that if these privileges are granted they will not lead to security problems.

Backup of all stored data is essential. In a large organization, you should be able to rely on the IS department to provide this service. However in a small organization you will likely have to set up a backup methodology. Often users set up a backup system and only discover that it doesn't work properly when they have a disk failure. Make sure that you confirm that your backup system is really working.

Perhaps the simplest yet important security issue is physical access to servers. By limiting access the obvious concerns of theft of computers or hot swappable drives can be avoided.

"Red Book"
Having a central repository within the Radiation Oncology department for all network related information has been found to be helpful. Benefits include:

- When you need help, there is often not time to collect data
- Remembering tidbits of software/hardware configuration from one event to another is hard, particularly as the physicist advances in age.
- Installers of hardware often leave town with the knowledge you need to fix problems.
- There are lots of interconnected pieces; no one vendor will accept responsibility for another's software or hardware.

We keep this information in electronic as well as paper forms, the electronic form is most current, the paper form is more portable.
Elements to include in the "Red Book":

- IP addresses
- Subnet Masks
- Gateway Address
- DNS server Address
- AET/Port numbers for DICOM devices

- Configuration instructions for different pieces of hardware (How do I set all of these parameters once I know them?)

HL7

Health Level 7 (HL7) is a file format for health related information. It is growing rapidly and is destined to be the primary format for health data transfer. A very good web site for information and standards for this format including the latest HL7 Version 3.0 is http://www.hl7.org/ . Information systems are beginning to trigger billing events when tests or procedures are performed. It is most likely that this billing event will find its way to an HL7 format. It is very possible that at some point, particularly in radiation oncology, a physicist may be involved in the mapping of patient information from a particular application to an integration engine. A basic understanding of HL7 format and standards will be beneficial.

System Manager/Administrator

It is very possible that a physicist may become the system manager/administrator for a domain or application package associated with imaging or radiation oncology. The core tasks of a system manager/administrator may include:

- Create new user accounts; make changes in current accounts
- Maintain system hardware
- Train end users
- Perform tasks that keep the system running smoothly, (maintenance, etc.)
- Document the system
- Define policies and procedures related to how systems are administered at your organization
- Recover from emergencies
- Plan the system and future upgrades
- Inform/educate management of potential technical needs for upgrades
- Watch for security threats and implement remedies

As mentioned earlier, a physicist's acceptance of the role of system administrator may be just enough job security to produce early permanent retirement! We are frequently the clinical expert while the IS staff is the business expert. It is most likely that combined efforts with one or more IS representatives to function as a synergetic systems administrator team will produce the best results. Keep this in mind when making your decision about your role as the system guru.

HIPPA

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the

security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

The Health Insurance Portability and Accountability Act has three important features of which any physicist working in the United States must be aware.

1.Transaction – Any electronic transfer of patient data must be in an appropriate file format.

2. Privacy – Privacy of all electronic, verbal or written information must be maintained

3. Security – Information should only be used/shared on a need to know basis.

Basic Terms, Descriptions and Overview of Networks

Network consists of a cabling or wireless scheme used to connect computers and a common protocol, or language, that computers use to communicate with each other.
The two basic types of network:
Peer-to-peer – Each PC on the network is a workstation and shares its resources, such as files on its hard drive or the printer

Client/server: A computer configuration where one computer (the client) runs the user application and communicates with another computer (the server) where the data is stored. The server often services multiple clients. Most modern applications are configured using client/server networks.

There are three basic types of servers:
File Server- Used to share files and printers
Print Server – Dedicated to receiving print jobs into a queue and spooling them to a printer
Application Server – Shares applications, a web server is an example of this

The connection of the computers is called a Local Area Network (LAN). Connecting two or more LANS forms a Wide Area Network (WAN).

The network architecture, how things connect or access the network, has two major players, Ethernet and Token Ring. These are the fundamental ways data packets are moved on a network.

Ethernet is prevalent, because it's cheap and easy to install and therefore more common. It is contention based and therefore prone to collisions (data packets access the LAN at the same time and in effect become garbled with each other along the line). When a machine attempts to send a message and it has a collision with another message, it will try again and again. This access method is called Carrier Sense, Multiple Access, Collision Detection (CSMA/CD).

Token Ring is completely different. It is deterministic, using an electronic "token" to decide which machine can transmit when. In general, a Token Ring network is more efficient, more expensive and unlike Ethernet, it may slow down when there is a lot of network activity but it will not stop.

The Network Interface Card (NIC) is a card installed on the PC that takes information being sent from a PC, puts the info into a data packet then transmits the packet into the LAN. The data packet will have a certain format such as source address, destination address and data.

Cabling of the networks are usually done with 10BaseT or 100BaseT (10Mbps vs 100Mbps). Fibre optic cabling is becoming more common, It is faster but more expensive.

Hubs, Bridges, Switches used in Ethernet networks to segment devices on the LAN. A segment is a physical division of the network and is one way to reduce the size of the collisional domain and help speed things up. A Router is similar to a switch except it is used connect LANs on a WAN.

Now that we have the basics to understand the hardware architecture of a network, we will quickly review protocols used by the network. The protocol is the language that PCs will use to communicate. Examples of Protocols are:

NetBEUI – (NetBios Extended User Interface) Used on small independent LANs, and in general is not routable unless it is encapsulated.

IPX/SPX - (Internetwork Protocol Exchange/Sequence Packet Exchange). IPX supports the transport and network layers of the OSI network model. It can be used between multiple networks and connected with a router. SPX operates at the transport layer providing connection-oriented communication on top of IPX.

TCP/IP (Transmission Control Protocol/Internet Protocol) IP is a network-level protocol like IPX and TCP is a transport-level protocol like SPX which rides on top of IP and is used for reliability.

Here are some examples of the network types and the protocols used on them:

Network Type	Protocols Used
Direct cable connection	NetBEUI, TCP/IP, IPX/SPX
Dial Up Networking (DUN)	NetBEUI, TCP/IP, IPX/SPX
Microsoft (NT, 98, etc.)	NetBEUI, TCP/IP, IPX/SPX
Internet	TCP/IP
Network 4 and below	IPX/SPX
Network 5 and above	IPX/SPX

IP Address - Is used to identify a device. Each IP address on the network must be unique. IPX handles this requirement for you automatically by using a combination of the IPX network address plus the burned-in address of the NIC. This burned-in address of the NIC is also called the Media Access Control (MAC). When using IP, you must assign the addresses. This can be done automatically through a DHCP (Dynamic Host Configuration Protocol) or it can be done manually.

An IP address is 32 bits or four octets and broken into five classes. Classes D and E are reserved.

IP Address Classes

Address Class	First Octet Range	Number of Networks	Number of Hosts/ Network	Default of Subnet Mask
Class A	1-126	126	16,777,214	255.0.0.0
Class B	128-191	16,384	65,534	255.255.0.0
Class C	192-223	2,097,152	254	255.255.255.0

Domains - Like a workgroup, a domain is a logical grouping of machines for the purpose of administration and resource sharing.
Primary Domain Controller (PDC) is a server where the master copy of database of users on the domain. It is used to authenticate you to the domain at login time.

Security, Proxy Servers and Firewalls

Security was discussed earlier in this handout. In summary, there are three important issues for Server Security:

1. Control physical access to the servers
2. Maintain a password policy
3. Use permission for folders

Network Security – As the network grows, so does the point of "intrusion". If you are connected to the internet, your points of intrusion increase a million fold (at least). If your LAN is connected to the internet you will need a proxy server or a firewall.

Proxy Server – Also called "application level gateways" sits between the client applications and the web server. It intercepts all requests between the client and server and forwards or filters based on administrative criteria. All outgoing communications with a proxy server will have the proxy server IP address instead of the client's. This allows control of what sites your clients can access as well as prevents your internal IP addresses from being exported.

Firewall - A system designed to prevent unauthorised access to or from a private network. Firewalls, can be hardware, software or both, which is usually the case. A firewall examines each file/message and blocks those that don't meet specified criteria. There are several types of firewalls.

1. Simple routers with packet-filtering capabilities
2. Network Address Translator (NAT) which enables a LAN to use one set of IP addresses for internal traffic and a second set for external traffic.
3. "True" firewalls that use a multilevel approach including packet-filtering, application-level gateways and circuit level gateways.

Virus scanning should be done at desktops and servers if you LAN is connected to the internet or anyone is installing software from outside of your control. There are multiple desktop and server based anti-virus vendors, such as Symantec, Innoculan, etc..

For firewalls or an email or Simple Mail Transfer Protocol (SMTP) gateway, there are multiple vendors such as WebShield, Interscan, etc..