Charles Sonnex
A2 ICT, Task 3
St. Anthony's Hospital

## Introduction

The application that I have decided to report on is the system at St. Anthony's Private Hospital. .
St. Anthony's is situated on the A24, London Road, North Cheam, Surrey and is well served by road and public transport services. Close to the A3 and the M25, it is easily accessible and convenient for both Heathrow and Gatwick airports. The parking facilities at St. Anthony's are good with ample spaces.
The hospital can arrange for an ambulance service should it be needed.
St. Anthony's is a private catholic hospital, which provides private health care for over 200 patients.
The company has a huge plot of land, where many buildings stand, including offices, wards, an incinerator, conference centre, restaurant and others such as theatres, x ray rooms and treatment centres. Within the main building, a pharmacy, gift shop and a morgue are also present.
There are a number of departments within the organisation. Many perform few tasks using ICT therefore I will look only at the two main departments, which have the greatest use of the computer system at St. Anthony's. These being the Hotel Services Department and the Finance Department.
Both have very different roles within the organisation. The role and function of the hotel services department are as follows:

- To provide, safe, hygienic, high quality catering facilities throughout the hospital including the visitors restaurant, conference centre and to patients staying at the hospital.
- To host the conference centre and provide facilities within it for outside companies.
- To ensure housekeeping of patient rooms and of the whole hospital grounds.

Computers here are used for the ordering of produce and equipment, for standard word processing and database/spreadsheet creation.

The role of the finance department is as follows:

- Booking
- Patient Administration
- Patient Accounting
- Outpatients
- Payable/receivable accounts
- Stock control
- Budgeting

- Prepare all monthly, quarterly, and annual financial statements as required by the hospital chairman
- And payroll

The departmental functions involve a lot of communication between insurance companies, banks and other hospitals where they might instruct the transfer of funds or medical records etc.
The department is also responsible for making sure wages are paid and that expenses are accounted for. As well as making sure the company is making a profit and that all the money is logged, taxes are paid and legal procedures followed.

The two departments use both computers and manual paper filing in order to function. As St. Anthony's is a private hospital, it has a lot of dealing with insurance companies and with government agencies but also with the National Health Service (NHS).
All this administration and transfer of data brings about a number of issues for the system. Although the department personnel numbers are large in the Hotel Services Department, the number of staff that actually use the ICT system is limited. Five out of 150 staff was the number quoted to me in an interview with the Hotel Services Manager. This is because chefs, maids and cleaners have no general need to use such a system. Therefore management and other selective staff have the only access such as stock control or sectaries.  This is not true, however in the Finance Department, which employee wise is small but has the largest usage of the system at St. Anthony's because of the role and nature of their job. For both departments, computers are located in the offices of the department's employees.

## The System

The system itself is both expensive and large. All buildings using the system are hooked up under a Local Area Network (LAN)
Each PC on the network is considered a 'client'
The specification of the clients varies greatly according to their planned use.
These range from the lowest – 486SX/33 4MB memory, 124MB hard disk to the top specification of P3 800MHZ 128MB memory, 15GB hard disk. However the lower spec PC's are now being upgraded. All the clients are using Windows 98 and Windows NT.

Only a selected few computer have access to the Internet for both work and computer safety reasons, but this function is again being expanded to other 'clients' on the network. On the hospital network there are 88 printers, which are configured, to be used as a network printer accessible by all network users or it may be set-up as a local printer usable only by the PC of which it is attached.

The software that is used on the network mainly is Microsoft Word and Microsoft Excel (used from the Microsoft Office 2000 professional CD pack). Also on the network consists the program 'MEDAX2000 made by ACT Medisys Ltd.

"The MEDAX software package is a Private Hospital Patient Administration System. MEDAX2000 is a patient based system designed for easy use by healthcare professionals and administrators to capture and collate all patient events. The product's unique range and depth of information supplies hospitals with essential statistics, financial information and activity analysis for resource management. It also accommodates electronic data transfer for invoicing and remittances between hospitals and insurers. Comprehensive standard reporting facilities are embedded within the system, while Business Intelligence tools provide flexible and detailed reporting capability that allows data to be presented in both graphical and textual formats". (Sourced from the MEDAX2000 website)
MEDAX2000 is installed in 142 hospitals.
Central facilities include:

- Contract Management
- Financial Accounting
- Materials Management
- Medical Records
- Order Communications
- Outpatient Clinics
- Patient administration
- Pharmacy
- Radiology
- Standard Interfacing
- Theatre Management
- Waiting Lists and Bookings

St. Anthony's uses only a selective few of the above those mainly being accounting, contract management, patient administration and bookings.
The systems administrator tells me that ACT Medisys Ltd is very inefficient providing little customer service to their software users. Changes to the software would be most useful but because of copyright laws can't be done without the specific consent of ACT Medisys Ltd.
The software on the network brings about all sorts of legal aspects for licensing and security. These will be discussed later.

With such a large system, a 'systems administrator' is needed to ensure the system runs smoothly.
On the hospital site, a single building stands at the edge of the hospital. This converted residential house is home to the IT department.
The department consists of 3 administrators and a head systems administrator – a Mr. Emeritus. His job is to make sure that the computer system is always up and running and updated when required.

The administrator’s jobs are:

- Installing and Upgrading Software
- General Maintenance of the network
- Software training
- Network expansion
- Troubleshooting
- Backing up the server
- Monitoring performance of the computers, servers and the network
- Progress reports to employees of the fixing of the network
- Announces problems in the system to employees
- Ordering new Software/Hardware

Because of the large number of computers and peripherals on the system, many problems arise, therefore it is also his role to act as a ‘call out man’ when a ‘client’ has a problem. The administrator also has to carry out the day-to-day maintenance of equipment such as checks to the drives and the network.

Following an interview with Mr. Emeritus, the specification of the network was explained.

In the hospital department lies over 150 computers hooked up over a LAN ‘Compaq ProLiant 1600’ server which is rack mounted.

The rack also houses two other servers, and all three servers have identical specifications. The third sever is used as a standby in the event of failure or can be used for test purposes for new hardware and software.

On the system exists an un-interruptible power supply (UPS). This conditions the mains voltage to protect the server(s) from voltage transients, and uses an internal battery to maintain the supply for a short time in the event of a power failure. If the power failure exceeds about 5-10 minutes, the UPS will automatically signal to the server to shut down safely, thereby preventing data loss.

The backup battery is not however able to allow the system to continue to be used normally. However in most cases the hospitals emergency generators will start to provide power before the servers are instructed to shut down.

During a power failure the majority of PCs will loose power. Special additional arrangements must be made if it is necessary to continue to use a PC during a mains power failure.

Currently, it is not planned that the system is used during a power failure.

Four UPS units are currently used in the server room, each protecting the four servers on the system.

## The Major issues

The major issues that I will research and report on are:

- The ***Legal issues*** which affect St. Anthony's Hospital and its employees in both major departments in their use of an ICT based application. There are several implications for users of IT systems related to health and safety and legislation, which requires compliance from organisations and their employees. The items of legislation are specifically:

- The 1988 Copyright, Design and Patient Act
- The 1990 Misuse of Computers Act
- The 1998 Data Protection Act and the European Union Directive on Data Protection
- The Freedom of Information Bill

All these will be scrutinised and the effect on the users examined.

- The ***Social issues*** relating to operating an ICT based application particularly:

  - Whether the working environment provides a suitable and safe one for employees and whether the training needs of staff are addressed.
  - Whether the monitoring processes of the company employs in it's monitoring of staff in their use of the system and whether this infringes on privacy.
  - The hospitals policy and contingency plans and its effect upon staff – including data backup, system protection and data security.

The implications of such issues have shaped the hospitals policy and have influenced the systems specification and software library. They have had a huge impact upon the users of the ICT system at St. Anthony's. This is explained:

## Aspect 1 –

## Legal Issues

In the past then years there has been an unprecedented rise in the surveillance and monitoring of individuals and groups, and the collection of personal data for a number of purposes. The new communications and information technologies have played an important role in the development of this.
New Legislation has been drafted over the past few years to address the speed of technological and social change. These legislations are:

- 1988 Copyright, Design and Patient Act
- 1990 Misuse of Computers Act
- 1998 Data Protection act and the European Union Directive on Data Protection
- Freedom of Information Bill

The drafting of new legislation to keep on top of the increased use of Information and Communication Technologies' (ICT) is not confined to the UK. Since the United Kingdom is a member of the European Union, subsequent legislation from the European Parliament is also abiding and is ruled according to the different commissions within the European Union. These include the European Court of Human rights and the European Court of Justice.

## 1988 Copyright, Design and Patient Act

This act gives the creators of literary, dramatic, musical and artistic works the right to control the ways in which their material may be used.
The rights cover; broadcast and public performance, copying, adapting, issuing, renting and lending copies to the public. In many cases, the creator will also have the right to be identified as the author and to object to distortions and mutilations of his work.
Literacy is described as "manuals, computer programs, documents or articles,"
This act applies to a number of operational policies within the hospital.
Firstly, the act prohibits the hospital from copying information, which is under a copyright mark. This means that certain documents or written patient information cannot be copied without the holders consent. An example in the hospitals case is visible on the bottom of the hospitals website, (http://www.stanthonys.org.uk) where the following line is displayed:

*Copyright 2000*$^{©}$ *St. Anthony's Hospital.* All rights reserved. Copies of information on this World Wide Web site may be printed for personal use only. No part of this World Wide Web site may be reproduced or reused for any other purpose without prior written permission of St. Anthony's Hospital.

This protects the hospitals information and 'leaflet' online so to speak from being used by another person or company without authorisation.
In protecting itself, however the company has to follow the legislation also. This act can therefore be applied to the use of software on the network.

When you purchase software, you have to accept its terms of conditions before using it, and on a network, certain licensing agreements have to be met. All commercial software in use must be licenced. Software piracy is the unauthorized copying or distribution of software in violation of licence agreements. When you purchase or otherwise obtain software (e.g. by getting shareware or freeware from friends or the Internet), you are actually acquiring a licence that permits you to use the software. You do not own the software. As with any system it has to be made sure that it reaches all the legal requirements of the software, that is to say that all licenses are filled in fully and renewed when necessary. Currently there are 69 software licences in St. Anthony's hospital. At the hospital, licences are kept in the system's administrator's office in a file, which is logged telling when licences have to be filled out and renewed.

The two main packages that need licences on the system at St. Anthony's are Microsoft Office 2000 and the MEDAX2000 software package. These, according to the Systems Administrator cost a "fortune" and in the case of St. Anthony's are renewed yearly. Microsoft state that a licence also gives product support and upgrade advantages with all the latest product releases during the term of the licence, keeping up to date on Microsoft software but at a price. It's the easiest way to manage new software enhancements, and replaces version Upgrades, Product Upgrades, Competitive Upgrades and Language Upgrades. This therefore offers a moral obligation for the systems administrator if he is committed to managing an effective system.

The 1988 Copyright, Design and Patient Act has however, little effect upon the specific users of the Hotel Services department. Users mainly use the ICT system for either data processing using Microsoft Offices Database, spreadsheet, word processing and presentation applications. Users are however informed of the legislation upon starting work, so if a situation did arise where the legislation was abiding, they would be more than capable to follow the law. Users in the Finance department are however slightly more prone to situations concerning Copyright. The role of the Finance department brings about a lot of data transfer between different departments and organisations. Therefore the issue of copyright arises. If documents are to be copied and stored, then the authors express permission will have to be granted if a copyright patient has been placed upon it. This can add to an employees administrate workload. The majority of documents however do not have copyright protection therefore only in a few documents will be listed as obtaining one. These are usually clearly labelled with the words "*Copyright"* combined with the year it came into effect and usually the year it expires. The icon $^{©}$ is usually visible meaning ironically 'copyright'. If this is seen on a document then the 1988 Copyright, Design and Patient Act will have to be followed.

If the law is not followed and a complaint is made then Civil and or Criminal penalties may be imposed on the company. Whether there are significant checks in place to ensure the law is being followed is debatable, but the filing system in the Finance department does appear to sort files so that items under copyright are filed separately. However administrate errors do occur, but since copyright "wardens" do not exist, checking to see if a copyright infringement has taken place is rare.
Software Copyright law is however checked constantly due to the high percentage of computer piracy. The Systems administrator therefore takes care of the software licences, but if he fails to do so then the company is at fault not the individual. The other members of the ICT department should however spot any discrepancies in licence agreements and I'm sure the software producers wouldn't fail to give reminders of licence renewal dates!

## 1990 Misuse of Computers Act

Unlike other legislation, the Misuse of Computers Act is by comparison, a short succinct act with the main aim of preventing unauthorised access or 'hacking' to a system.
It is not necessarily theft or vandalism, although it is rare that an individual is ever prosecuted for simply entering another system.

Malicious hacking is still relatively rare, and with better security as well as better incentives for potential hackers not to hack, incidences of unauthorised access are on average relatively low. On the other hand, it is difficult to get a clear picture of the scale of hacking, as many companies are reluctant to go public for fear of loss of consumer confidence.

Throughout the 1980's there was an assumption that computer hacking was illegal, as such it was not thought necessary to provide for hacking a separate piece of legislation. Exiting laws of criminal damage, Theft and Fraud would take care of any unauthorised entries.

However, not all hackers have these intentions, many do it for the sheer challenge and sense of accomplishment for hacking a system. The hacker may then just 'look around' on the computers files bring up all sorts of legal problems associated with data protection. This brings about the issue of data security.

Because of the sensitive nature of patient health records, the systems administrator has a legal duty to ensure that data on the system remains secure and safe. Because only few of the computers are actually connected to outside lines, the defenses for hacking can be concentrated in a specific area on the network. Hacking is prevented on the system by a simple password access screen protected by a firewall. This, according to the systems administrator is all that is required for adequate security. Patient records are available under the MEDAX2000 software using additional password and login procedures.

When it comes to accessing the computer system the user has to enter a login name and password. All logins are recorded so any irregularities on the system can be traced.

When the user has gained entry onto the system they can only gain access to programs to which concerns them.

The Finance Department's security has to be more tightly guarded since it processes more confidential information such as wage slips and administrative budgeting.

The physical security of paper files in the Finance Department is kept in locked filing cabinets inside the main building, various camera and detection systems exist in the hospital to prevent theft of such data. Office doors are always locked. All computers have to be logged into via the Windows 98 Password protections system. Additional security on selected documents is also sometimes undertaken together with the other security features of the MEDAX2000 software.

Only the systems administrator has the ability to 'un-lock' the system, but even then he would still be unable to enter selective areas on the hard disk that do not concern him.

In 1988 the House of Lords found that the simple act of entering into another's computer was not illegal, therefore, the systems administrator has an additional 'moral' role to ensure that the privacy of an individuals computer is secure.

A hacker cannot only compromise security but also damage computer files or even hardware on the network. The simple act of planting a 'computer virus' can be devastating to a system. Viruses however can sometimes infect a system because of accidental insertions. This is discussed later under the 'social' aspects later in the report. Militias' use of viruses can constitute 'Criminal damage' under British law; therefore the protection systems for anti-hacking are required. If however the person places the virus while already within the system, (such as an employee), they can be traced via their login name. Even if the user was unaware of a virus on an external disk, they would still face disciplinary action because of the companies policy of not allowing users to insert floppy disks into ‘client’ drives, unless otherwise approved by the ICT department.

Therefore the 1990 Misuse of Computers Act has a great effect upon all users of the ICT system. It’s shaped hospital policy and has affected users in a number of ways. Users are told to ‘Log off’ a client PC whenever they leave the room. This according to the Hotel Services manager is very frustrating because of the time it takes to log off and on the system. Since the network is not connected to a Wide Area Network such as the Internet, outside security risks are minimal. Therefore any information Misuse has to come directly from inside the network. All prospective employees who apply for a job using the network are checked out and are informed of the strict terms of use for the system. If they are broken then disciplinary or even criminal action will be taken. Combined with the MEDAX2000 security features of only allowing certain user names to access certain functions and files the warning seems to of effectively secured the system and according to the systems administrator, a security breach has yet to occur.

## 1998 Data Protection act and The European Directive on data protection

Much of the concern over the use and misuse of data has been driven by marketing and credit card companies: the loyalty card that provide customers with small incentives to shop at a particular supermarket, buy petrol from a particular garage and so forth, also monitor every transaction you make for the purposes of building up a personal profile of you and your consumer habits. Such information can be ‘sold’ to associated advertising and retail organisations; the type that send you junk mail in the post or try and sell you double glazing when you’re having your dinner. The question of personal freedom and the collection and processing of data can take on a far more sinister veil when we turn our attention away from consumer durable products, and on to insurance and other such services. Whilst insurance companies many not be able to freely sell or pass on your personal data to others, they can purchase data from companies – this could in affect cause public embarrassment and a loss of Patient-Doctor confidentiality within a hospital such as St. Anthony’s.
The Data Protection Act contains eight Data Protection Principles. These state that all data must be: Processed fairly and lawfully; Obtained & used only for specified and lawful purposes; Adequate, relevant and not excessive; Accurate, and where necessary, kept up to date; Kept for no longer than necessary; Processed in accordance with the individuals rights (as defined); Kept secure; Transferred only to countries that offer adequate data protection.

The hospital therefore has a legal and moral obligation to protect the confidentiality of its patient’s health records. Mainly, these are on paper, and are locked in secure filing cabinets, but information transferred on the network has to be dealt with with the utmost security and integrity. The hospital is therefore forbidden to foreclose medical or financial records without the consent of the owner. This means, no information can be read, sold or transferred out of a secure location without the proper authorisation of the owner.

Because the Finance Department deals so hugely with the NHS and with insurance companies, data and information has to be passed on in accordance with the law.
The systems password security protection ensures this is so.
In addition, employees dealing with sensitive and confidential material have to sign an official hospital document from the Department of Heath stating the rules of data protection and processing. This is similar to the official secrets Act that many civil servants and Government Ministers are obliged to sign.

Because of the United Kingdoms membership of the European Union, certain legislation is also abiding.
St. Anthony's deals with many overseas companies. This is where the European Directive on Data Protection comes into place.
The Directive on the protection of personal data has been formally adopted by the Council of Ministers. ``I am pleased that this important measure, which will ensure a high level of protection for the privacy of individuals in all Member States, has been adopted with a very wide measure of agreement within the Council and European Parliament" commented Single Market Commissioner Mario Monti. ``The Directive will also help to ensure the free flow of Information Society services in the Single Market by fostering consumer confidence and minimising differences between Member States' rules. Moreover, the text agreed includes special provisions for journalists, which reconcile the right to privacy with freedom of expression," he added.

The Directive will establish a clear and stable regulatory framework necessary to guarantee free movement of personal data, while leaving individual EU countries room for maneuver in the way the Directive is implemented. Free movement of data is particularly important for all services with a large customer base and depending on processing personal data, such as distance selling and financial services. In practice, banks and insurance companies process large quantities of personal data on such highly sensitive issues as credit ratings and credit-worthiness. If each Member State had its own set of rules on data protection, for example on how data subjects could verify the information held on them, cross-border provision of services, notably over the information superhighways, would be virtually impossible and this extremely valuable new market opportunity would be lost.

The Directive aims to narrow divergences between national data protection laws to the extent necessary to remove obstacles to the free movement of personal data within the EU. As a result, any person whose data are processed in the Community will be afforded an equivalent level of protection of his rights, in particular his right to privacy, irrespective of the Member State where the processing is carried out.
St. Anthony's therefore has as an additional legal obligation to ensure that data is treated appropriately. It is the job of the departmental management to ensure that data is securely transferred, but in retrospect, all the staff have already been highly trained therefore no recommendations have to be put forward since the hospitals policy ensure that data is treated accordantly.

The legislation affects the users of the ICT network in a number of ways. Notably it increases the workload of the user and takes up time, but this is more than counterbalanced by the social and legal implications of data security. Data protection at St Anthony's has become expected so users are obliged to follow the law. The Security password system on the network also ensures that confidential information is seen only be those it is concerned to. Therefore members of the Hotel Services Department will not be able to access the files of the Finance department and vise versa.
Additional security features such as "locking" documents in Microsoft Office also offer an additional level of security for information.

## Freedom of information Bill

Unlike in the United States, the legislation for freedom of information has yet to go through parliament. Charter88 – a pressure group campaigning for the Freedom of information Act have called on the government for *"a radical overhaul of the government's deeply flawed and disappointing"* draft Freedom of Information bill. They go on to say that in its present form the bill fails to give the public the effective right to know that the Labour party has been promising for 25 years. Since the legislation has yet to be passed and when it does get passed it looks as though it will be ineffective, the hospital has no legal or moral obligations to provide information. Therefore users at St. Anthony's are unaffected.

## Health and Safety

Many procedures within the hospital ensure that health and safety standards are properly met. This has been somewhat taken to seriously on the ICT system. An example given to me by the Systems Administrator showed how a whole office block had to be equip with expensive plasma flat screen computer monitors mealy because a nearby air conditioning system generates minuet, if not undetectable vibrations.
These 14" monitors cost more than the actual computers themselves! Although St. Anthony's does have a legal obligation to ensure health and safety regulations are properly met, this seems somewhat extreme and uneconomical. However, since the offices are small, all space needs to be maximized therefore the flat monitors provide an additional social and moral benefit to the workforce.
The systems structure ensures safety of its employees and equipment is of the highest standard. Equipment safety checks are also done every quarter year.

During my interview with the systems administrator, I was told of a burglary at the Hotel Services Office. Six computers were consequently stolen but Mr. Emeritus ensured me that all secure data is kept on the server's main hard disk. Therefore taking a 'client' PC has no breach on the security of data.
Since the break in, additional physical security has been implemented including a new alarm system directly linked to the police and hardened fire doors to prevent entry when locked.

All PC's comply with legal and moral specification on noise and safety and all wiring is safely built into the walls of the offices making it impossible for electrical fires or injuries (trips and falls) by employees.
Users are therefore provided with safe equipment adding an additional moral boost to the workforce as well as ensuring proper safe computer hardware. The issue of a comfortable working environment is discussed later.

## Aspect 2 –

## Sociological Issues

Computers can have both a positive and negative impact on our lives. As they become increasingly important, these machines have the potential to deprive us of our privacy and even the jobs we needs to support ourselves. On the other hand, they can enhance the quality of human life by producing unimagined freedom from drudgery and want. Associated with each application of the computer are various issues that affect our society.

In this section I shall be discussing the following implications of using the IT system within the hospital:

- Working Environment e.g. the provision of comfortable furniture and additional hardware/software on the system to ensure a pleasant working environment.
- The training of the workforce.
- Data Backup
- Monitoring Processes of employees using the system
- System Protection
- Hospital policy and Contingency plans
- Data Security from a social perspective

### Working Environment

People spend many hours in their offices. There are few legal requirement of a company to ensure that an employee is adequately 'comfortable'.
Research has show that continued use of a PC over number of hours could significantly reduce a person's health. People stare at computer screens straining their eyesight and damaging their muscles by the position they sit in. This can cause many hours of lost working time through illness. Therefore it is up to the company to ensure that their employees are adequately looked after.

St. Anthony's is a rich hospital; they spend thousands of pounds on medical equipment and building refurbishment. The staffs using the ICT system are no exception. During a brief tour of the main offices, the systems administrator and the Hotel Services manager – Mr. Paul Sonnex showed me how staffs are looked after.
Firstly, in order to ensure an employee's eyesight isn't stained excellent fluorescent lighting is provided. Offices are also painted in light colours, often white to boost this effect. Blinds are also available on windows facing the sun.
On the network, special protective filters cover the PC monitors on the computer. These ensure that eyestrain is minimised. A picture of this is displayed:

Long hours working at a computer terminal can mean headache-causing eyestrain. The filter is a slim, easy-to-install screen filter that reduces the glare that causes eyestrain. It cuts 99% of the glare without distorting the image and color. Its flat plug and conductive coatings can reduce Elf/VLF radiation by up to 99.9 percent.

Furniture is of high quality wood and are of a height high enough to avoid back strain. In addition to this, the chairs are comfortable and come with pump adjustment facilities so that the user has the ability to use a PC at a height suitable to them.
As mentioned earlier, computer wires are hidden and the monitors of selective PC's are flat in order to maximize desk space and comply with moral health and safety standards. All PC's are quiet and offices air-conditioned in order to comply with the moral and legal aspects of employee comfort including the 'Offices, shops and railway premises Act 1963' and the 'Factory Act 1961'.
Offices are also relatively large and offer stress-reducing facilities including a fish tank in the Finance Departments Offices and a visible garden.
Nearby beverage facilities also provide colleges with coffee, snacks and full meals.
Mouse pads with wrist rests also ensure the user is comfortable while using the system.

The comfortable working environment combined with the added Operating System software "disability" features allowing certain aspects of the display to be enlarged or magnified for the hard to see gives the user a comfortable working environment, improving productivity and staff moral.

## The training of the workforce

Before being employed in the hospital, colleges have to have the required skill of typing and basic computer procedures.
Training is an important part to any company, which allows them to keep with the times and learn new ideas and techniques, which, at St. Anthony's are being used to good effect. By having well trained staff, the efficiency and speed of the employees is greatly increased. Training for the system is only really restricted to specialist software, since at interview applicants are expected to be able to use the Windows operating system and Microsoft Office applications.
The system's administrator at St. Anthony's told me that the delivery of the MEDAX2000 software was both late and over budget so in order to cut costs the training program was abolished. This has lead to many employees picking up the bad habits of other employees when using the software. This has lead to multiple errors and problems with files.
Any training within the department is done either by the systems administrator or from an external trainer. The trainer then makes a course involving the specific topics.

Since my interview, the ICT department has been looking for a more efficient and effective program to replace MEDAX2000.
When asking about MEDAX2000 I was told that its was produced by ALT Medisys Ltd and was designed for MSDOS so is vastly outdated and difficult to use. I was later informed that ALT Medisys Ltd has created a new updated version but the £500,000 license price tag was too much for the hospital. Other products are now being looked at.

## Data Backup

All of the data that is entered on the St. Anthony's system is backed up and is saved on the servers drive.
When a user clicks save, the data is saved automatically to their user name, accessible only to them.

On the network there are six servers. One of which is being used as a standby in the event of failure, or it can be used for test purposes for new hardware and software.
On the system exists an un-interruptible power supply (UPS). This conditions the mains voltage to protect the server(s) from voltage transients, and uses an internal battery to maintain the supply for a short time in the event of a power failure. If the power failure exceeds about 5- 10 minutes, the UPS will automatically signal to the server to shut down safely, thereby preventing data loss.
The backup battery is not however able to allow the system to continue to be used normally. However in most cases the hospitals emergency generators will start to provide power before the servers are instructed to shut down.
Four UPS units are currently used in the server room, each protecting the four servers on the system. This, together with disk backups keeps data secure and saved. Normal windows back-up procedures also ensures data is safe.

Often physical paper documents are printed also and stored or sent off to appropriate locations.
These backup procedures ensure that users at St. Anthony's do not get frustrated if they 'loose' their work, as it can be fully recovered.

## Monitoring Processes

Most people value their freedom and individuality. We do not like to think that we are being constantly monitored and assessed, that our private and personal details may be available for purchase on the open market, or that government bodies may have access to our personal correspondence and communications. Where such overt bureaucratic interference exists we are inclined to think of the state that allows it as being unduly oppressive and intrusive, Yet, in the past ten years there has been an unprecedented rise in the surveillance and monitoring of individuals and groups, and the collection of personal data for a number of different purposes. The new communications and information technologies have played an important role in the development of this "surveillance society".
There have been many cases heard on the news of employees being dismissed because of misuse of a companies computer system.
St. Anthony's doesn't really have this problem since only a small number of PC's are connected to the Internet.
In order to save hard drive space and improve staff efficiency many features on the Windows operating system has been disabled including games and LAN chat programs.

When a user logs onto a computer, the time and location is recorded and is accessible by only by the systems administrator. Therefore if any illegal action is performed, the user can be traced and tracked down.
The setup on the server means that no two people can log on to different computers with the same user name and password.
If a user forgets their password, they will have to see the systems administrator to get it reset.
Users of the network are not allowed to store pictures of 'explicit' content nor are they allowed to bring in software from home.
Only selective PC's have access to the Internet, and when they do use the net, various blockers are in force to prevent access to adult or game websites for example.

The hospital policy and equipment has had a great effect upon the users of the system. Since only a selective few computers are connected to the internet, abuse of the network is virtually non-existent and the "blocking" features on many websites by the ICT department combined with the fact, every time an internet site is visited a "cookie" is left displaying the address of that website ensures that if an employee were to try they wouldn't get away with it! Whether this abuses ones personal privacy is arguable but it can have a debilitating effect upon staff moral as many staff could be led to believe that management doesn't trust them!

System protection

As well as data security, the data also has to be protected from software corruptions and viruses.
At St. Anthony's anti-virus software protects the computers and servers from computer viruses. The hospital uses the Sophos anti virus software. At the core of all Sophos products is a sophisticated virus detection engine, developed and supported by Sophos experts. The software's platform-independent architecture ensures the same network functionality is enabled, regardless of the operating system being used. The virus checker is updated weekly Via the Sophos website - http://www.sophos.com/ which gives additional programming to conquer new viruses. Updates are distributed across the network from a single point at the ICT department block and with great ease.

The hospital policy of 'no disks unless checked by the ICT department' is according to many employees at St Anthony's "very annoying". If a user wishes to save a file or open one off an external disk then they would literally have to walk across the hospital to the ICT department. This has led many people to dislike the ICT department for their persistent stubbornness! While at the interview with the Systems administrator, I asked if anyone had ever disobeyed this – he told me of an event that had taken place the previous year where a user had inserted a disk without having it checked causing a computer virus to be unloaded upon the system. That employee was subsequently dismissed due to the damage on the network (but the data backup procedures ensured that no important information was lost).

Hospital policy and Contingency plans

The policy of the hospital is not necessarily legally binding but more contractedly and morally. There are a number of formal and informal guidelines.
The ICT department, in order to ensure safety of data has invoked a formal policy where no external disks are allowed to be entered into a client without first being virus scanned by the systems administrator.
However, the use of disks is still physically possible so to ignore the systems administrator's rules brings about both ethical and moral issues to the user. If a disk is used that is infected with a computer virus, the system can be damaged. During my interview with the administrator, I asked if this has ever happened. He replied that it had once and the employee concerned was consequently tracked and dismissed as a result of the ensuing chaos in the system. The dismissal set an example to all employees who disobey company policy.
Due to the multiple servers on the system no data was lost as a consequence although the network was out of action for around a week hugely disrupting company work.
Socially this policy has caused much irritation for colleges, as it is difficult to take work home with them.
Another formal hospital policy is the order that users 'log off' their user name when they leave the room regardless of how long they'll be gone. This ensures data protection and the privacy of the users work area.

Informal policy is not really that important and just requests small things such as ensuring the computer is physically clean and that disks and software instructions are appropriately looked after. Users are requested to shut down clients when not in use for a prolonged period of time and are requested to keep printing to a minimum as it creates queues on the server.
As mentioned earlier, employees only have access to programs, which concerns them. They are also obliged legally and morally to ensure that data is treated accordingly. The Data Protection Act and the others mentioned earlier are all constitutionally binding in the hospitals policy.

Users are advised to save work on a regular basic just in case of a client or server crash. The Contingency plans for such a crash happening if a user hasn't saved their work is that it is recovered via the Windows recovery system built into the software. If however this fails to operate then a users work is effectively lost if it wasn't saved. This will be viewed as the fault of the user.
In the event of a power cut, the server can still operate, saving data before the network shuts down. On the system exists an un-interruptible power supply (UPS). This conditions the mains voltage to protect the server(s) from voltage transients, and uses an internal battery to maintain the supply for a short time in the event of a power failure. If the power failure exceeds about 5-10 minutes, the UPS will automatically signal to the server to shut down safely, thereby preventing data loss.
The backup battery is not however able to allow the system to continue to be used normally. However in most cases the hospitals emergency generators will start to provide power before the servers are instructed to shut down.
During a power failure the majority of PCs will loose power. Special additional arrangements must be made if it is necessary to continue to use a PC during a mains power failure.
Currently, it is not planned that the system is used during a power failure.

## Data Security from a social prospective

If someone is already logged on to a computer and someone else wants to use it then the employee is requested to log off the previous user before starting any work. This is to ensure the privacy of the individual and security of any documents on that employee's user area.

Computers are situated in offices that can be locked ensuring additional privacy to the user when operating the system.

In order to gather a wider perspective on the impact of the social issues upon the users of the system I conducted an interview with the Deputy Hotel Services Manager – Sarah Dowell. The minutes are displayed: (my questions appearing in **bold**, answers in *italic*)

Interview date: December 5th – Afternoon.
Interview subject – Deputy Hotel Services Manager – Sarah Dowell.

- **How long have you been working for the Company? -** *Just under 1 year now*
- **Are you a regular user of the IT system?** *– I use it 3 maybe 4 hours a day, yes*
- **What do you think of the office Working Environment? (Such as comfortable furniture etc) –** *Its great! I have this lovely leather chair*
- **How about on the Computer?** *– Well, I have a screen filter thingy that reduces eyestrain and a nearby coffee machine!*
- **What do you think of the ICT department?** *Arrogant, cynical bastards!*
- **Why so?** *All they do is moan and their stupid disk check policy means I have to walk all the way across the hospital.*
- **Do you find it difficult to follow legal guidelines?** *Not at all, its pretty much automatic now.*
- **How reliable is your computer terminal?** *It hasn't let me down yet*
- **What do you think of the MEDAX2000 program?** *Its quite hard to use but once you get the hang on it, its fine*
- **Did you receive any formal training for the program?** *Nope – When I started work, a few of the lads showed me how it works*
- **Do you believe this has affected staff moral?** *– I think it's made a lot of people frustrated.*
- **Do you believe the system has overall boosted staff moral?** *Well it's always nice to have a comfy chair and working PC!*
- **Do you have an Internet connection on your workstation?** *Nope, my job doesn't really require it*
- **Do you think the monitoring processes of the hospital affects privacy?** *Not really, if you break the rules then that's your fault.*
- **Have you ever lost any work because of a computer error?** *– Not yet*
- **Does the IT system offer adequate disabled access?** *- I think it does, the offices make it physically possible to get to a PC and the 'accessibility' feature on windows helps me when I don't have my glasses!*
- **Any comments or recommendations for the system?** *I wouldn't mind a personal printer – saves me having to get up and go to the main office every time I print something!*
- **Can this pose a Privacy/Security risk?** *Now that you mention it, if I can't get to the printer fast enough it does leave print jobs available to read by other staff.*

Interview End

From the interview I gathered additional knowledge as to the effect of the system upon a regular user. The interview pretty much summed up what I had already mentioned earlier however it exposed a concern as to the security and privacy of printed material. I am informed that this risk has been accessed but due to a number of factors including lack of space, budget constraints and lack of power terminals. But the overall factor is that it is not “economically viable” as commented by the systems administrator. Therefore only cost seems to be the constraint for improving the system.

## Conclusion

My investigation of the system has uncovered many legal and social issues associated with not just the IT system at St Anthony’s but also systems throughout.
Legally, St. Anthony’s is an excellent establishment. They obviously take care and consideration to ensure that the system complies with the law. The 69 software licenses are clear evidence that this is being implemented.
After a tour of the network in the offices of the Hotel Services and Finance departments I saw clean, safe and up to date computers.
It is clear that St. Anthony’s looks after their employees. The number of facilities available on the network including the ‘wrist rests’, screen filters and comfortable furniture prove that socially the system is compliant. My interview with Sarah Dowell proves this. The effects on the users has been overall good and has improved staff moral, ensured good staff health and has ensured that law and policy is being followed without hesitation.

The MEDAX2000 software has had a moral and social impact on the users. On the one hand, it has been a useful program that has been widely used by the hospital but as the systems administrator told me MEDAX2000 is both hard to use and out of date. ALT Medisys Ltd; the producer of the software have been proved inefficient and unreliable. The applications belated arrival caused the training program to be abolished. This has had far reaching implications on the staff, causing increased program errors due to user error creating a higher work load for the ICT department and generally diminishing staff moral.
This has had a bad social effect on the system with possible legal implications as a user might accidentally send a file to an insecure location. The problems associated with the lack of training and because of MEDAX2000’s non-user friendly interface has in the words of the systems administrator “caused me a lot more bloody work!”

Few other problems exist except for the ageing hardware in selective offices. These however are soon to be replaced for more advanced stable systems.
Economically the legal and social expenses have been huge. But in spending all this money, St. Anthony’s has ensured good solid employee morale and has created a model system for hospitals across the country.
The system has proved effective, stable, secure and efficient and has overall provided well for the needs of the hospital. As long as investment remains at its current level, I see no problems with the system in the foreseeable future.

Limited improvement recommendations therefore exist for me to comment on. But I will however suggest that training procedures for the company be improved so that the users are trained how to use the MEDAX2000 and any other future replacement to its most effective means.

I agree with the system administrator that the MEDAX2000 software should be replaced soon but restrains of funding prohibit future improvement of the software library available on the system.
In my view more client connections to the Internet could make applications quicker and cheaper to send and could in the long run create better business opportunities for the hospital for example if an internet connection was set up in the office of the hotel services department, then cheaper suppliers could be found and ideas developed for certain restaurant menus etc. The system administrator informs me that this proposal has yet to be decided on but is looking likely to be implemented. Doing this however would bring up the question of Internet monitoring, data security and safety.
My only real remaining concern is that of the shared printers – whereby a printed confidential document may be left unattended for minutes posing a security/privacy risk. This matter as discussed earlier is yet to be added and is unlikely to do so.
Legal bureaucracy has added to the system users workload, but it has ensured that data is kept secure and available only to whom it concerns upon request.

I believe I have identified a relationship between a comfortable working environment and high staff moral and on the contrary a relationship between lack of training and increased errors and thus lower staff moral. Hospital Policy has proved effective in ensuring data security and the hardware on the network has created a stable, adaptable, safe and secure platform for data storage and access.

In all, the system at St. Anthony’s has proved legally compliant and socially friendly and has affected users in a number of good and bad points but overall the Pro’s outweigh the Cons.