**Project for Heix 701 Otago University**

****

09

**Survey of Security Measures for Hospital Electronic Medical Records**

**Results and Recommendations**

**Ian Campbell (ID:7179250)**

# Table of Contents

[Table of Contents 2](#_Toc232854276)

[Introduction 3](#_Toc232854277)

[Method 3](#_Toc232854278)

[Results 4](#_Toc232854279)

[Server: 4](#_Toc232854280)

[Recovery plans 5](#_Toc232854281)

[Software Security: 5](#_Toc232854282)

[Internet: 5](#_Toc232854283)

[Workstations: 5](#_Toc232854284)

[Wireless network 5](#_Toc232854285)

[E-mail: 5](#_Toc232854286)

[Discussion 6](#_Toc232854287)

[Recommendations 7](#_Toc232854288)

[References 9](#_Toc232854289)

# Introduction

“Privacy groups fear 'Medishare' card scheme”

This newspaper [front page title](http://www.news.com.au/couriermail/story/0%2C23739%2C25601319-952%2C00.html) [[1]](#endnote-1)is typical of the public and media’s view of most forms of Electronic Medical Records.

The article goes on to say: “Patients’ private medical files will be shared among health professionals under a Rudd Government plan for a contentious healthcare card.”

“From the middle of next year, the Medicare card will provide doctors, dentists, pharmacists and paramedics with an encyclopedia-like file on patients' medical histories, medications and treatments.”

"This sounds like a good first step towards introducing electronic records which can help improve patient safety and health outcomes," Dr Pesce (AMA President)said."However, patients need to have control over what is placed in their records and must be assured rigorous privacy safeguards are in place."

Being mindful of such words as these, I undertook a survey of the hospitals in which I work, to ascertain their levels of security present to safeguard their patients’ confidentiality. I will present my findings and recommendations.

Any storage of patient data in NZ must comply with the privacy act which is primarily concerned with **Privacy and confidentiality**. These two concepts are often used interchangeably and relate to the rights of patients with regards to, the information stored in their health records, and, who has access to this information. Informational privacy refers to the rights of the individual to determine the parameters for the sharing of personal information. Confidentiality specifically refers to the use of information for its intended purpose.

Legal obligations for the collection and use of patient information, in New Zealand is determined and applied by the Privacy Commissioner. Privacy obligations are set out in the [Health Information Privacy Code 1994.](http://www.privacy.org.nz/privacy-act-summary/)[[2]](#endnote-2)

I made the assumption that the institutions surveyed complied with the act.

# Method

The survey I used to question the IT administrators at the various hospitals was based on a Microsoft Access database. I utilized the ability of Access [[3]](#endnote-3)to compile and email a questionnaire via Microsoft Outlook. Their responses are received in Outlook and it automatically populates the various fields in the Access database, allowing it to be queried and results reported.

The surveys format in an email is shown in the figure 1.

Once the reply option is selected, the person surveyed can fill in the form and once completed selects send to return the form to my email address.

The data then populated the below database form for ease of reading.

With only four records it was easy to see the results so, although possible to design and run queries, I felt it wasn’t merited in this situation.

# Results

Four hospitals were surveyed and one Auckland City Hospital gave me information by way of personal communication.

The four hospitals were;

Mercy/Ascot
Southern Cross Gillies
laparoscopy Auckland
Eye Institute

The first comment made accompanying the survey, from each of the institutions, was that they really did not have a true EMR system, but what they had amounted to fragmented software programs each holding some aspects of clinical data, and were not linked to each other. Thus the security measures they had in place were common throughout their organizations.

Each has been using electronic data for approximately ten years, and their servers are all on site, with the exception of Gillies Hospital. It is a Southern Cross Affiliated institution and therefore has links to their central IT dept by the use of data channels.

Server: Each protects their servers with temperature controlled environments, and UPS power supply. One has a mirror off site backup. Two respondents used back up with a “**RAID 1** “system, i.e. (mirrored settings/disks) duplicates data across every disk in the array, providing full redundancy. Two (or more) disks each store exactly the same data, at the same time, and at all times. Data is not lost as long as one disk survives. The other two use tape backup. The rate of back up depends on the frequency of their changing data. Some data is changing every 15-20 minutes so required frequent back up. All institutions performed a full backup every 24 hrs usually in the evenings.

Recovery plans and times, varied greatly, but all claimed to be up and running less than 2 hours from a complete loss of power/server, one claims a time of 20 minutes.

Software Security: Thankfully each institution had a secure login and password system to protect the clinical data. Mercy/Ascot requires each of their staff to have their own unique password at login, which is stored encrypted. However there is also a generic “ward work station password” which is changed at regular intervals. This is issued by the IT department.
Auckland City Hospital uses a “Single sign-on” system.

Internet: Three of the four allowed internet access at work stations, through individual login. The fourth has separate PCs for staff to access the internet during their free time. All restrict access or even ban access to certain web sites e.g. Facebook and Trademe. The down loading of most things other than PDF files is also banned. All have appropriate, regularly updated antivirus software and also anti spyware/malware.

Workstations: All do not allow the user to utilize software other than that approved by the IT department and certainly no access to the USB ports is allowed.

Wireless network: None of the hospitals have a wireless network. However Mercy/Ascot are considering providing a Wi-Fi network in the operating theatre floor, thus allowing their visiting medical staff to have access to their rooms and limited internet access. There are no plans to integrate the Wi-Fi with the hospital’s EMR system.

E-mail: At the work stations of all institutions no personal email accounts are allowed, through Outlook, however ward and department email can be accessed through Outlook after appropriate login.

These results indicate that the physical side of security is well handled, and is consistent throughout these hospitals, and reflects the trends in most IT departments both in public and private sectors. The attempts to secure their software whilst technically good and correct, can be left open to breaches by the human factors of those responsible for the workstation once they have logged in.

On this front the hospitals I surveyed, are having to contend with similar problems as their larger counterparts and also the large corporates.

# Discussion

It appears that the technology of data storage and its associated techniques employed to secure it, is heading in the right direction and that despite the continuing threat from “hackers” the software makers are keeping ahead.

This threat is ever present and will increase as systems begin to utilize the public internet, more and more, to integrate their various sites and even into the homes of the clinicians.

Fragmented, partial and not seamlessly integrated small EMR systems are causing major security and privacy concerns. In the USA only 2% of hospitals have totally electronic Medical Record Systems. The ideal is to strive for integration of large systems.

This is a flow diagram of the Orion Health product ***Concerto[[4]](#endnote-4)***, which is used by Auckland City Hospital, as their EMR system. It, as you see, provides a complete Electronic Clinical System integrating all aspects of the hospital and community.

In many respects this is an ideal system, because of it seamless integration and single sign-on approach. It ensures that all data is secure and private, and there are no compatibility issues of a fragmented system.

Further patient privacy is ensured by use of a Physician Portal, which allows access only to his/her scope of work determined by their user group.

Built in is an Inactivity time-out, if suddenly called away from screen the user is auto logged out.

***Concerto*** also uses a full audit log for all user activities which is stored on a separate audit database, for later review. On many occasions physicians have been reminded to stick to accessing data only relevant to their case load.

This leads onto the most insecure part of any EMR system which is the human security issues. Confidentiality agreements are signed by all staff and health workers are mainly aware of their duties through the privacy act to preserve a patient’s confidential data. However human nature is such that temptation and carelessness abound a so security breaches are still occurring. Worryingly, this is also occurring inside the IT depts. of organizations.

As in this news item: [[5]](#endnote-5) Twelve months after the Cyber-Ark "Trust, Security & Passwords" survey they discovered that 33 percent of IT staff used their IT administration rights to snoop around networks to access privileged, corporate information such as HR records, layoff lists, customer databases and M&A plans, a repeat of the survey has discovered that the situation has escalated.

A paper describing a similar survey of the Hospital in Israel[[6]](#endnote-6), showed that: 75% of respondents were concerned about inappropriate access to patient’s clinical records from someone in the organization already with authorized access, to the system. Also 55% of respondents were concerned about unauthorized access from persons outside their organization.

These are obviously not system faults or breaches but never the less it has become part and parcel of the design of EMRs to ensure security is tighter.

Access control is an essential part of the EMR and provides for its confidentiality by checking if a user has the necessary rights to access the resources he/she requested. Access control: how can it improve patients' healthcare?[[7]](#endnote-7)

The utilization by medical organizations, of security products such as Cyber-Ark will go a long way to providing security for the data to provide the media and privacy groups with certainty that patient confidentiality is being maintained.

 With its Privileged Identity Management Suite v5.0, Cyber-Ark becomes the only vendor to offer a full lifecycle solution to secure, manage, log and monitor all privileged accounts - including the sensitive application identities embedded within applications and scripts, and administrative passwords found in routers, servers, databases and workstations. The Suite features a single, central infrastructure and provides administrators with greater fine-grained access control and advanced web-based reporting capabilities to address important audit and compliance questions. With new session recording capabilities and multiple password inventory reports, administrators can better answer not only "who" accessed sensitive information, but also "what" was done with that information once it was accessed.

Possibly the use of independent software programs such as, KeePass password safe [[8]](#endnote-8) , which provide randomly generated passwords for individuals which are stored encrypted and have only one master password, could provide peace of mind for individuals faced with providing numerous passwords on throughout their daily work and play, without using easily guessed ones. The random generation would prevent their information being hacked. This would only work on individuals with an allocated PC not a common workstation.

As hand held devices become more ubiquitous, and their utilization of wireless networks allows their point of care use, securing a wireless network is paramount. Wireless networks are wide open to hackers unless several steps are taken to secure them.

The Wi-Fi network requires encrypted password access, with secure passwords, non broadcasting of the network name and using Mac address filters to ensure only certain devices are given secure access. This also allows audit of individuals’ activity.

As you can see from this discussion the biggest challenge facing EMR providers, is satisfying both patients and privacy advocates that their data is in safe secure and unhackable hands.

# Recommendations

The wider use of healthcare information systems and the easier integration and sharing of patient clinical information can facilitate a wider access to medical records.

The main obstacles to this wider use are cost and privacy concerns. Smaller institutions and/or organizations cannot afford the larger integrated secure EMR systems available and thus often build their own fragmented systems. This causes great concern for the privacy advocates, as these systems are never as secure. One recommendation is to standardize and have governments subsidize these EMR systems as part of building a national patient database.

In time all patients will in fact “own” their own medical records, which will be stored on a secure server of national size, and have the right to provide appropriate access to health professionals who they come in contact with, which will provide much better healthcare and allow information to be disseminated over great distances and patients travel around.

Studies published by Ferreria and others [[9]](#endnote-9)revealed that patients' access to medical records can be beneficial for both patients and doctors, since it enhances communication between them whilst helping patients to better understand their health condition. The drawbacks (for instance causing confusion and anxiety to patients) seem to be minimal. However, patients continue to show concerns about confidentiality and understanding what is written in their records. The studies showed that the use of EMR can bring several advantages in terms of security solutions as well as improving the correctness and completeness of the patient records.

When patients allow health professionals to access their details, an audit log must be provided and diarized for the patient as well as the organization holding the data such as a small clinic or x-ray facility.

To overcome the major concern of the wrong people accessing patients’ data, often out of pure curiosity, I believe a new culture of privacy is required and we must move away from the media driven thirst for gossip and scandal and such reality TV shows, and return to a culture of respect for each other and our right to privacy.

If this is achieved the advances in technology which are providing the secure environments to store our data will be successful.

# References

1. Courier Mail, Brisbane 8/6/9 [↑](#endnote-ref-1)
2. The NZ Privacy Act [↑](#endnote-ref-2)
3. <http://office.microsoft.com/en-us/access/HA100154271033.aspx> [↑](#endnote-ref-3)
4. <http://www.orionhealth.com/solutions/ehr> [↑](#endnote-ref-4)
5. <http://www.cyber-ark.com/news-events/pr_20090610.asp> [↑](#endnote-ref-5)
6. Isr Med Assoc J. 2004 Oct;6(10):583-7. [↑](#endnote-ref-6)
7. Stud Health Technol Inform. 2007;127:65-76. [↑](#endnote-ref-7)
8. <http://keepass.info/index.html> [↑](#endnote-ref-8)
9. Stud Health Technol Inform. 2007;127:77-90 [↑](#endnote-ref-9)