International Review of Business Research Papers
Vol.5 No. 1 January 2009 Pp. 202-211

Importance of Info Security at Pakistani Hospitals

Mohamed Nasr[1]

This study is a serious attempt to tie both information and security together being necessary for each other. Computers have become a part of our daily life let alone that of Healthcare. The use of information in a Global economy has made life easier, but made illegal access to such information quite attractive for those with evil intentions. Nature interferes with its share of impact on hospital information, like what happened as a result of the infamous earthquake of October 2005 or Hurricane Katrina in Neo Orleans in August 2005. We visited many times and conducted a pilot questionnaire as well as interviews, in a convenience sample the following 6 hospitals: We applied also the method of obtrusive observations at one public hospital (PGHI) and a private hospital (AHI) during September. The results show that there is a significant difference in applying physical security between public and private hospitals in Pakistan. All hospitals have no computerized info systems (CIS) except AHI (Private) and PIMS (Public); both have started some sort of CIS. Moreover, physical security is not sufficient at all Pak hospitals that have been visited during this study. Contingent loss of millions of rupees and even lives may result out of such weak security systems.

1. Introduction:

The increasing attention paid to the Healthcare Sector by Pakistani Authorities has been regarded as one way to move right into the 21st Century. AHI is the only hospital in Islamabad and Rawalpindi that has an integrated info system, with few added security procedures. No one can get access to his computer without an ID and password. However, an illegal access to one of them makes easy invasion of rest of the computers. So, if the Admissions officer left his/her front desk for a break, that small period would invite outsiders to tamper with the info, delete names and add others at own volition without detection.

Criminals steal identity as well as health cards and use for illegal matters. The use of computers in hospitals has added another prospect to those criminals. Unfortunately, Computer Crimes are not easily detected, and the Criminal Law is not yet developed to counter for such cases. Here are some risks that the info at the patient registration offices are vulnerable to:

1- Viruses that may attack the hard disk of computers from communication with CDs or from remote sites using the Intranet and Internet.

[1] Dr. Mohamed Nasr , CGA is a Canadian Professor (under the foreign faculty hiring program of Higher Education Commission of Pakistan) at COMSATS Institute of Information Technology, Islamabad, Pakistan. E mail: Mohamed_nasr@comsats.edu.pk

2- Intruders may be able to decode the hospital security system codes, and steal important information, alter, or delete, causing harm to everybody.
3- Storage systems may be subject to Natural Disasters such as what happened to AJK University and the city hospital in Muzaffarabad due to the earthquake of October 2005. All patients' files were lost with no backups.
4- Storage systems may be subject to other problems such as changing levels of heat and humidity, temperature, and loss of electricity.
5- Lack of external storage facilities in some developing countries to retrieve information in case of losing those on the primary storage facilities.
6- Centralization of authority over patient registration in few people. Then, info may be misused at any time. According to B. Williams and S. Sawyer (2005) 80+% of perpetrators of Info Technology Crime may be Employees.
7- Absence of strong internal control. Also, there are no compensating controls such as cross checking made by the hospital superintendent.
8- Easy access to the office of registration by outsiders most of the time.

1.1 Importance of the study:

This study ties info to security and provides details of the subject. So, it will be useful for care-givers, patients, and third party too.

1.2 Objectives of the study:

We aim at identifying the hospital's info systems, and tying their security with the hospital's internal control system.

1.3 Limitations of the Study:

We prepared a questionnaire to be filled by different parties at Pakistani hospitals and large clinics. But, most of the approached hospitals have not yet used computers in their operations. Our obtrusive observations were made within 4 hours before and afternoon in 8 visits to both PGHI and AHI due to time limitations. However, if made also during the evening or night shifts more cases of security breaching would have been detected.

1.4 Increasing Need for Information at Pakistani Hospitals:

Hospitals in Pakistan rely heavily on info about patients, diseases, medicine in common use, and instruments in urgent need. But, such info cannot continue to be manual, and will soon be computerized. The continually increasing need for info at hospitals has resulted in an increase in the risks of stealing, loss, alteration, deletion, corruption, or addition to the stored documents of information. Thus, there is an increasing need to safeguard it, keep its quality and have it available in time for users. Risks are not just those of invaders, but extend to the natural hazards such as floods and earthquakes, in addition to man-made hazards such as electricity blackout.

2 Literature Review:

Information is defined in Oxford Dictionary of 1995 as “Knowledge”. New Webster Dictionary added direct perception, understanding, and acquaintance with protected practical skills, and learning.

Rob Mattison (1999) defined Knowledge as “an approach to the study of Business that attempts to describe the effectiveness of organizations as a function of the efficiency with which they create, store, and apply knowledge to the creation of goods and services”. He tied the term “Knowledge Management” to the use of computers, as he observed that all aspects and walks of life use computers on the one hand and different versions of Net Systems on the other hand. He provided the following equation:

[Data + Context + Application to Specific Business Objectives = Business Knowledge]

On the other hand, info security is defined by Elbra A (1992) as protection and safeguarding of all resources used to treat info. So, when we talk about info at hospitals we have to consider the importance of physical as well as computer security and not only speed and accuracy (quality) of info.

To support the importance of information security, Kaiser J (2006) suggested that patient info should be protected from invasion of privacy let alone theft or tampering with. She recommended encryption of patient records so that no unauthorized people would gain access to them.

Dolev-Yao (1983) stated that an intruder could infiltrate the security system and get one message. Then, he could deduce new messages from the one he already knew. With known keys, his deductions could be used to deduce for other messages.

Abdel-dayem M et.al. (2001) provided an alternative form for data hiding to encryption called steganography. They discussed several techniques for embedding secret info into audio signals at different rates. They proposed a digital audio wave files (44.1 MHZ, 16 bits) as a cover signal. The result would bring no subjective distortion to a media signal that could be detected by human auditory systems. This technique can be used to hide any secret patient info type including medical history, prescriptions, and *X*-ray images.

The problem is still with the traditional methods where people commit info crimes such as stealing the hardware with all it has on of software and valuable info. Also, many times, hospitals dispose of old computers by sale or dumping while valuable info have been left not erased off the hard disk. People who gain access to such information may misuse it.

Serapetti A (2005) discussed this problem of info misuse by people, and sections of the US HIPAA security regulations, and stressed the need to use security measures that would improve patient info protection and privacy. He suggested having a separate department to perform internal risk assessment in US hospitals, and prioritize those risks for action. He suggested some balance between excessive security measures and speed of getting info by the clinical professionals who resent excessive security measures. He concluded that only a small group of info system staff should be authorized to coordinate the distribution and smooth handling of patient info to all concerned care givers within the available but limited resources.

However, evil minded people continue to send viruses to destroy hospital computers. To counter against their evil acts, Hanan, A (2007) discussed honey pots. They are embedded in the computer security system to divert the attackers from the critical system's info. Meanwhile, security personnel would keep the attackers busy till they collect info about them. Then, they would inform the authorities to apprehend them and take penal actions.

Silver L. (2006) argued that soon the patients admitted to the ER suffering from a heart attack might have their odds of survival at risk unless the doctors on duty could connect to the internet, type a password, and with few clicks get the patient's medical history. But, present day security measures may not allow such a luxury. She ended with a bold statement that after 9/11/01 the Federal officials in USA and Canada should be able with the help or interconnected mega-systems to spot early evidence of biochemical attacks and epidemics. She added that it usually took 26 days for the Canadian current fragmented info system to process data at the local level, then the provincial level, and at last the country level. She put a price tag of C$150/year per person for 5 years till 2011 to get a fully integrated info system with security measures.

Nasr M (2006) discussed the destructive role of natural hazards to info security such as the Earthquake of October, 2005 which devastated Northern Pakistan. After that earthquake had taken place, the General Hospital of Balacoat was destroyed and all patient info was lost. No external storage was available to compensate for the lost info.

Khan Haroon: (2007) provided an excellent display of the use of computerized systems at PIMS in Islamabad to process patient cases as well as their billing, and other financial and operational documents. However, he confessed that PIMS despite being a pioneer in the use of computerized info systems in Pakistan had only 2 computers and was still far behind in incorporating security measures in it.

3. Methodology and Research Design:

Actually, the amount of security required by any hospital is accessed by three sources, assessing the risk; the legal obligations borne by the hospital and set of principles, objectives and requirements for info processes that support organization's operations. Despite technological changes the hospitals of Pakistan have not yet changed from the ancient manual system. Moreover, security of the manual system is still weak. But, with time, one expects that all Pakistani hospitals will use computers for their operations as well as financial record keeping, and security will be part of the change.

We have prepared a detailed questionnaire of more than 60 questions to be filled out by different departments at each of those hospitals in an attempt to tie the security of info to the physical and computerized environment. However, those hospitals have no CIS, and claim that health services are offered for everybody. So, there is no fear of identity theft. We visited 6 hospitals, and found that even the physical security system was inadequate. This problem would cause loss of millions of rupees even lives due to the ability of invaders to steal info, delete or corrupt it.

3.1 Hypotheses of the Study:

H_{10} Security is not important for any hospital information system

H_{11} Security (Environmental & computer) is necessary for any hospital info system.

H_{20} Public and private hospitals apply physical security at the same level

H_{21} Public and private hospitals are different in applying physical security

We applied the following model for contingent loss (CL) of revenue:

$$CL = \sum_{i=1}^{n} U_i . C_i \quad (1)$$;*I* = 1, 2, …n (number of wards/specialties) and

U_i is the unit of patient admission or clinical observation
C_i is the cost as charged at the private hospital AHI

4. Discussion and Findings:

The only two hospitals having developed some IT infrastructure are PIMS and AHI. But, they have limited IT support staff and the average number of IT staff is 5–15 personnel. Network Administrator is the most responsible person for the security of Information System at AHI. Backup data is generated timely and on regular basis.

Internal Control Systems of almost all the hospitals in the sample are inadequate. Many times the admissions clerk was out of his desk while the files were accessible to intruders.

Table 1 Obtrusive observations at PGHI

Visit-time	Officer inside/ Guard at door	Office closed	Office open, Nobody inside	Nobody inside open office, Files on Desk	Total
Before noon	6	0	1	1	8
Afternoon	5	2	1	0	8
Total	11	2	2	1	16

In 19% of times there was no body at the reception desk, and in 6.3% times files unattended to provided a chance for intruders to either take a file or add some documents that have not been there. However, in all 8 visits to AHI there was no single time that files were left unattended to or the reception office left open without a guard outside. Analysis using Excel provided the following results:

Observation time	*t*-statistic	*p*-value
Morning period	1.559**	0.06**
Afternoon period	1.323	0.11
Overall Observation	1.924*	0.02*

* Significant at 5% level ** significant at 10% level

The result shows significant difference between PGHI (Public) and AHI (Private) is in the morning and overall observations. We expect that conducting those obtrusive observations in the evening or at night would result in much more significant differences. Hence we reject H_{20} and accept the alternative hypothesis. That is why information at point of registration has to be protected. On the other hand, such concern should not result in delaying the smooth communication of info between concerned parties, invading privacy of users, or reducing its quality.

PIMS has the following info about its facilities according to Dr. Khan (2006) Performing contingency analysis using model (1) we conclude that only one illegal utilization of hospital services or tampering with patient files would cost more than 97 million rupee which are more than double PIMS budget.

Activity Item	Service provided	Charge at AHI
Number of beds	610 beds in all divisions	1000 rupee/day
Specialties	20	600 rupee/visit
Outpatients	1238/day during 2006	600 rupee/visit
Operations/surgery	20 per day	6000 rupee average/day
Diagnostics:	300 lab analyses/day	500 rupee average/patient
Radiology	200 patients per day	500rupee average/patient
Pharmacy	250 patients per day	500 rupee average/patient
Budget for 2006	47million rupee	2000 rupee/average

Both PIMS and AHI are using Antivirus to protect their systems against threat of viruses. During in person discussion with senior personnel of both hospitals it is identified that they are going to develop proper and specialized software systems for their operations and financial record keeping in response to the changes in info technology. But, they as well as rest of the sampled hospitals feel that security against patient info theft is not a big issue since medical treatment is offered free of charge at the public hospitals, and those patients treated at AHI are covered by some sort of health insurance.

Hiring security guards for the main computer room (only 2 computes are used at PIMS), and others for all gates of the hospitals is not expensive. Also, peripherals such as printers and remote storage rooms may be guarded physically, and locks should be kept on the doors with keys to authorized personnel only. Also secondary storage media such as disks and tapes, in addition to hard copies of periodic reports for emergency are need. Those should be documented and put in the custody of few trusted officers.

4.1 The office of Patient’s Registrations Info Risks:

We may summarize the risks that database at the patients’ registration office in public hospitals is subject to as follows:

1- Environmental risks, such as Earthquakes, heavy rains, and floods. We may include here such changes in weather due to heat or humidity level. Also there are risks of electrical supply shortage, unintentional fire or caused by arsonists, and theft of computer hardware with all sorts of info on; most of its data are not encrypted or hidden.

2- Unintentional info misuse; for example info about patients of the ER sent by mistake to the outpatient clinic. The result would be wrong decisions, and misleading info of those admitted patients and those discharged.

3- Ability of intruders at AHI to deduce messages of the internet and use to solve subsequent ones using same keys to decrypt what was encrypted.

4- Continued efforts of criminals to develop viruses to invade hospitals, and destroy their info contents. Also, open info to intruders when registration offices are left open and unguarded with computers on.

5- Periodical computer failure due to over-use. Also, inadequacy of storage space and unavailability of remote storage areas for secondary storage.

6- Centralization of work in the hands of few officers. When they are absent, the computer room may be misused by unauthorized people.

7- Routine and red tape that may render info communication late and useless for making sensitive and important decisions.

8- Absence of a strong internal control system, or compensating controls.

When we interviewed some database officers at AHI, we discovered that all the system had available was the use of IDs and passwords.

4.2 Conclusion and Recommendations:

The Info available at the CIS departments of Pak Hospitals is quite vulnerable, especially its connection with the office of patients' registration; security of info at this office is important. So, we recommend the following:

1- Increase number of visible security guards on all gates of Pak Hospitals.

2- Expedite the introduction of CIS at all hospitals to cater for the continually increasing needs for registration of patient medical treatment.

3- Provide all computers, especially the Patients' registration office with locks to be secured when authorized personnel are away.

4- Get effective security software to hide data, and make stolen info useless.

5- Establish an independent department of internal control that subordinates directly to the hospital superintendent. The auditors may evaluate performance of personnel, software efficiency, and effectiveness of the used info security system.

6- Have a secondary storage at remote area unaffected by the change in weather or natural hazards. Also, use the traditional password and codes.

7- Segregate duties to avoid having the same person cross-checking himself.

8- Exchange info with other hospitals inside and outside Pakistan, to keep informed of changes and improvement in info security systems.

9- Do not dispose of old computers unless all hard disks have been cleaned and info properly deleted several times.

10- Provide regular maintenance of computers to prevent sudden failure.

11- Provide the personnel with training on security matters.

12- Continue research in this area to improve performance and reduce waste.

13- Attend international conferences whenever possible in this regard.

References:

Abdel-Dayem M., et al., 2001 "Info security using data hiding techniques" Annual conference on Stat & Comp Science; p 53-69, Cairo U Press,

Abdullah, Hanan, 2007 "Anomaly Detection and Response", paper presented at the Conference on Frontiers of Info Technology in Islamabad,

Bender W., et al., 1998."Techniques for data hiding" IBM J, Vol 35, p 313;

Brandel, Mary. 2005. "Too many T bytes for tape, Hospital network turns to data protection system", Canadian Network System, p 40.

Burgess M, et al. 2004, "A grasph-theoretical model of capacity security" International Journal of Info security, vol 3, issue 2, p 70-85,

Dolev D., Yao AC.1983. "Security of public protocols" AMC 29 pp 198-208,

Elbra,.R.A1992."Computer.Security.Handbook",

Hagland, Mark: 1996 "Healthcare Insurance Portability and Accountability", Journal of Health Management Technology, Vol. 19, pp 24,

Heather JA, Schnedier A.2002. "Equal to task?", LNCS, NY pp 167-177,

Hutt, Arther E. et al.1995. "Computer Security book", John Wiley & Sons,

Jackson, K.M.1992 "Computer Security Ref Book" Butterworth – Heinman,

Kaiser, Joselyn; "Rule to Protect Records May Doom Long-term Heart Study",.Science.pp.1547-1548,.2006.

Khan, Haroon.2006 "Hospital Info System as Future of all Hospitals"; Conference on Frontiers of Info Technology in Islamabad,.

MacVille D.2005. "Don't be the next data"; Network computing, pp 32-34;

Mattison Rob.1999. "Knowledge Management", McGraw-Hill, .

Miller S.2005 "Controlling the uncontrollable", Journal of Info Security,

Murphy, Michael 2004 "Creating a Security Policy in Hospitals", Canadian Healthcare.Technology,.Vol..9.p.13,.

Nasr, M.2005. "Toronto as a Role Model of Info Use in Planning to Protect against Disasters" Proceedings of Islamabad Meteorology Conference, O'Shea, G.1991 "Security in Computer Systems", NCC Blackwell,

Pfleeger, Charles P.1997. "Security in Computers", Prentice Hall,

Rahfaldt, Kim.2003. "Access Control, the most logical system to integrate on a Network", Journal of Security & Distributing and Marketing, p 50.

Serapitti, Arnold 2005."Implementation Challenges for HIPAA Security Regulations", Journal of Behavioral Healthcare, p 513,

Shenk, David.1997. "Data Smog: Surviving the Info Glut", Harper Collins.

Silver, Lynn.2006."The New Threat to Medical Privacy", Journal for Chronic Disease.Prevention,.Vol..71,.p.39,.NY.

Tapp, Ann 2003. "New Developments in Privacy Law" Canadian Nurse, Vol 9 p 32,

Wong, Ken.2005. "Managing Information Security", 1990. Wood, Michael B.: "Guidelines for Physical Computer Security", 1986. Williams B. and Sawyer S.; "Using Info Technology, p 345-355. McGraw Hill,