Future of healthcare vis-a-vis building trust in major stakeholders through Information Security Management (ISM)

Alpana Kakkar, Priyanka Taval, Ritu Punhani

International Research Journal
ISSN 1839-6518
Vol. 3, No. 2, 2013
82800302201304

Future of healthcare vis-a-vis building trust in major stakeholders through Information Security Management (ISM)

Alpana Kakkar,
Priyanka Tayal, Ritu Punhani

International Research Journal
ISSN 1839-6518
Vol. 3, No. 2, 2013
82800302201304

Future of healthcare vis-a-vis building trust in major stakeholders through Information Security Management (ISM)

HEALTHCARE sector is growing leaps and bound, so is its data and information. Security and privacy of this Information has become a crucial issue for this proliferating healthcare industry. In this fast moving global scenario, patients need not carry their medical records in a big bag on move, as in this digital world ,all that patients have to do is to get admitted in a hospital for the treatment , rest all is in hands of Information Assets Infrastructure of these mushrooming hospitals. But due to the increased use of patient's information sharing among doctors, vis hospitals, patients and their families raise an issue for security of their medical data and records. Hence improving the Information Security Management Systems (ISMS) has become the necessity to keep secure digital patient records for success of hospitals and their brands or at large name and fame of Healthcare Industry. Patients are required to share information with doctors for correct diagnosis and treatment. Security concerns arise, in transmitting and processing electronic medical records, personal healthcare records, patients' billing records as well as public health alerts across many parties with varying security, privacy and trust levels. Not all hospitals adopt all the essential security measures. In the present paper, we are studying eight International Hospitals to review their Information Security Management Systems (ISMS) standards , concluding their stands on the basis of proposed five principles and also proposing the future scope of implementation of IS in the hospital. We contemplate an Information Security model based on the proposed five principles of Information Security.

KEY WORDS: DIGITAL PATIENT RECORDS, HIPAA, INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS), ISO 27799

INTRODUCTION

Privacy is an important principle of patient-doctor relationship. Patients are required to share information with their doctors to facilitate correct diagnosis and determination of treatment to avoid adverse drug interactions [1]. However, patients suffering from health problems like Psychiatric, HIV, etc refuse to share important information as the disclosure may lead to social stigma and discrimination. With time, patient's medical

record accumulates significant personal information mainly, identification, history of diagnosis, treatment received, medication history, dietary habits, genetic information, employment history, psychological profiles, income, medical images, etc. Patients' health records serve a range of purposes from diagnosis and treatment to improving healthcare system efficiency. It can also be shared among payer organizations such as insurance, Medicare or Medicaid. Healthcare providers may use records to manage their operations, access service quality and to identify quality improvement opportunities.

As personal health information is digitized, transmitted and mined, new threats on patient's privacy are becoming evident. Certain standards and regulations have been made in lieu to provide cost effective healthcare services to all citizens. These standards are, namely, HIPAA and ISO 27799.

The objective of the proposed paper is, to study the Information Security Management System (ISMS) of eight International hospitals on the basis of defined Principles.

Information Security Management System (ISMS) is known as an initiative from UK Department of Trade and Industry in 1995. ISMS concern itself with the security of information whether in physical or logical form and focuses on 3 areas (quote from ISO/IEC 13335-1:2004):

- Confidentiality
- Integrity
- Availability

These 3 areas together are commonly known as "CIA" [15].

The paper is organized as follows: In section II, security standards for healthcare are discussed. In section III, types of threats to patient's security are explained. In section IV, Importance of Access Privileges and who can breach it are shown in tabular format. In section V, proposed Security Model is given. In section VI, cases of few hospitals are shown along with the technologies they are using to secure their patient's information. Section VII, concludes the paper. And Section VIII gives the future scope of the paper. [5] [13] [15] [16]

SECURITY STANDARDS IN HEALTHCARE INDUSTRY

HEALTH INSURANCE PRIVACY AND ACCOUNTABILITY ACT OF 1996 OR HIPAA

It was enacted by US Congress. The standard is divided into two titles: Title1 covers protection of health insurance coverage for workers and their families and, Title2 covers Administrative Simplification Provision, i.e., it requires establishment of national standards for e-healthcare transactions.

HIPAA creates standards for protecting the privacy of health information, security of health information, electronic exchange of health information [2].

HIPAA affects following:

- Employee who handle, use or know individuals' Protected Health Information
- Healthcare Providers like, hospitals, doctors, health departments, etc
- Health plans
- Trading partners
- Business Associates
- Consumer of healthcare

ISO 27799: SECURITY MANAGEMENT IN HEALTHCARE USING ISO 1779

It is a guide to apply ISO 17799 when securing health information systems or protecting personal health information. Its sole purpose is to provide guidance to health organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of their patients' information by implementing ISO/IEC 17799 [3].

According to ISO 27799, Information is to be maintained in the standard format, as follows:

- Scope
- References (Normative)
- Terminology
- Symbols
- Health information security (Goals; Security within information governance; Health information to be protected; Threats and vulnerabilities)

- Practical Action Plan for Implementing ISO 17799/27002 (Taxonomy; Management commitment; Establishing, operating, maintaining and improving an ISMS; Planning; Doing; Checking, Auditing)
- Healthcare Implications if ISO 17799/27002 (Information security policy; Organization; Asset management; HR; Physical; Communications; Access; Acquisition; Incident Management; BCM; Compliance)
- Annex A: Threats
- Annex B: Tasks and documentation of the ISMS
- Annex C: Potential benefits and tool attributes
- Annex D: Related standards [4]

THREATS TO PATIENT'S PRIVACY

It could be categorized into two broad categories namely, Organizational and Systemic. Organizational threats occur due to inappropriate access of patient's data by internal people, misusing privileges or exploitation of system by external people. While, systemic threats occur due to someone in information flow chain exploiting disclosed data beyond its intended use [16].

IMPORTANCE OF ACCESS PRIVILEGES IN HEALTHCARE TO AVOID DATA BREACH

A tabular view of Access Levels and people who can breach data at the corresponding level is given as under.

An outsider has no access to any information at any Access Level. He can only get access, by hacking into the Network or breaking into the Physical site and steal. Only the person responsible for maintaining the Hospital site is responsible for any information loss. An employee of the hospital has access to the Hospital site and the whole system. It is the responsibility of the vendor or the consultant company to take care of the privacy of data and system. Doctors and nurses have the whole responsibility of Hospital, its system and data of patients. It is very essential for the people to fulfil their roles and responsibilities with loyalty. And do not breach the trust of patients as well as the name of hospital. [16]

PROPOSED INFORMATION SECURITY MODEL FOR HEALTHCARE

In the proposed security model, hospital's ISMS can be judged on the basis of five principles along with HIPAA and ISO 27799 standards. The five principles are as follows:

1. Replication of data for Availability
2. Access Privileges assigned to hospital staff
3. Encryption or use of Virtual Private Networks (VPN) for secured data transfer.
4. Store summarized data for some time for instant analysis and decision making
5. Warnings or Alerts for any internal misuse and external threats

CASE STUDY OF HOSPITALS

A short description of hospital's history, problems faced by them and what technology they used to eliminate it is provided. The case is concluded on the basis of proposed security model. On the basis of future scope, hospitals can improve their ISMS.

LEHIG VALLEY HOSPITAL

It is located in Allentown, Pennsylvania, USA. It is the largest hospital in the Lehigh Valley and the flagship hospital of the Lehigh Valley Health Network (LVHN). It has 783 beds and is a general medical and surgical facility. It had reported 43,495 admissions in the most recent years. It performed 12,163 annual inpatient and 11,687 outpatient surgeries. Its emergency room had 109,092 visits [17].

They wanted a HIPAA-compliant environment. They needed a solution that would monitor and correlate critical log data from disparate geographically dispersed devices to detect unauthorized access, logon/logoff failures and other patterns of behaviour that might suggest a security breach in progress. And in order to enable quick remediation and stop hostile behaviour before it causes damage, real-time policy-based alerting shall be used. They also needed comprehensive reporting to demonstrate compliance and conduct forensic analysis on security incidents. Different functional groups shall be provided with different privileges and access settings [9] .

They used Prism Microsystems Event Tracker for reporting and alerting. It comes with a number of preconfigured reports mapped to HIPAA requirements that allow them to demonstrate compliance. EventTracker allows them to insert customized business logic. With it, they are notified instantly when a workstation accesses areas it is not authorized to access. It produces predefined and customized reports on a scheduled or adhoc basis [9].

Conclusion: ISMS fulfills Principle 1, 2, 4 and 5 of the proposed security model (i.e. it provides Replication of data, Access Privileges, quick Alerts and also stores summarized data). It also follows HIPAA standard.

Future Scope: It can further improve its Security system by encrypting the data that it transfers using Internet. It should also comply with ISO 27799 standard.

HOSPITAL DA LUZ

It was founded in 2007 and is located in the capital city of Portugal, Lisboa. It has more than 400 Physicians, who had performed more than 20,000 surgeries till date. It had done more than 3 million diagnostic tests.

It relies heavily on its network as a business platform. Medical equipment wired or wirelessly connected to the network. Using their equipments, employees can access Internet; have voice chat; can capture, store and share images; or get medical appointment and reschedule it. They use BioMedical Network Admission Control (BioMed NAC) as proposed by Cisco to cope with endpoint and user authentication, privilege assignment and the automatic download of parameters to the network access devices [6].

BioMed NAC provides following features [6]:

- It has the flexibility to identify endpoints and users based on a variety of methods, so that virtually any machine which is requesting access to the network is identified and classified as corporate medical equipment, corporate PC, corporate IP phone, or guest PC, etc.
- It provides the possibility of combining user, their machine, its location, and the time stamp information to assign privileges and restrict access to resources. For example, only medical staff can have access to patient's records, while salary information can only be confined to HR staff and that too during their business hours, etc.
- Behavior tracking of users and their machines as they navigate through the network by comparing the traffic they generate to what would be expected, given the type of device. Normally, single-purpose machines, such as printers, medical equipment, and IP phones have a fairly determined behavior when they are functioning properly that can be used to protect the network when they either inject anomalous traffic or someone succeeds in disguising their PC as a printer or other device.
- Automatic and real-time updated inventory of all connected endpoints, allowing the decrease of the operational overhead.

- Scalable to tens of thousands of devices and hundreds of authentication requests per minute.
- Redundancy is also guaranteed by the automatic replication of databases and configurations throughout the main components.

Conclusion: Its ISMS follows Principle 1 (i.e., Replication of data) of proposed Security Model along with HIPAA AND ISO 27799 standards.

Future Scope: Hospital has to improve its Information Security System by providing required Encryption of data, Assigning Access Privileges, storing the summarized data and providing Alerts for any misuse.

SHANGHAI SHUGUANG HOSPITA

It is located in China. With increase in business, amount of data also increased. And so does the cost of maintenance and administration of separate servers. Hence hospital started using, SQL server. They also used an infrastructure proposed by Fujitsu, which was based on PRIMEQUEST 1800E and ETERNUS DX440 data storage. By using PRIMEQUEST 1800E and ETERNUS DX440, hospital's performance was improved. Excellent scalability was achieved to meet the requirements of continuous business growth. Ideal data protection functions were applied to ensure information security [7].

Conclusion: Its ISMS follows Principle 1 and Principle 3 of the proposed security model (i.e. it provides Replication of data and also provides Encryption feature for Information's security) along with HIPAA.

Future Scope: Hospital has to improve its Security System by providing Access Privileges, Alerts and summarized data for analysis. It should also comply with ISO 27799 standard.

TOP INSURANCE COMPANY

It has more than 500,000 members. It is using IBM InfoSphere Guardium and implemented database auditing in order to comply with SOX and HIPAA

Need of InfoSphere Guardium:

- To access and monitor all critical databases, including access by privileged insiders
- Create centralized audit trail for all their database systems
- Implement proactive security via real-time alerts for critical events.
- Easy implementation in existing environment

- Remote access and management
- Should not rely on database-resident functions like triggers, trace or transaction logs, etc

They are using 50 database instances that need constant monitoring for unauthorized or suspicious access.

IBM InfoSphere Guardium is used for preventing information leaks from data center. It ensure integrity of enterprise data. It is being used by more than 400 customers worldwide. Guardium was the first solution to address the core data security gap by providing a scalable, cross-DBMS enterprise platform that both protects databases in real-time and automates the entire compliance auditing process. It is a part of IBM InfoSphere; an integrated platform for defining, integrating, protecting and managing trusted information across your systems. The InfoSphere Platform provides all the foundational building blocks of trusted information, including data integration, data warehousing, master data management, and information governance, all integrated around a core of shared metadata and models. The InfoSphere Platform provides an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster [16].

Conclusion: ISMS fulfills Principle 1, 4 and 5 of the proposed security model (i.e. it provides Replication of data; provides Alerts and also stores summarized data). It also follows HIPAA standard.

Future Scope: It can further improve its Security system by providing Access Privileges and Encrypting the data that it transfers using Internet. It should also comply with ISO 27799 standard.

ARTEMIS

ARTEMIS hospital is located in Gurgaon, Haryana. It has developed a semantic web service based P2P interoperability infrastructure for healthcare information systems. Healthcare providers can join ARTEMIS network to access medical web services that enables access to electronic healthcare records maintained by other healthcare organizations. Healthcare information systems operate within a strict regulatory framework that is enforced to ensure the protection of personal data against processing and outlines conditions and rules in which processing is allowed. A core requirement in ARTEMIS is for very robust, but highly flexible approach to security and privacy. The approach supported by ARTEMIS is to allow healthcare providers to codify their particular preferences and requirements for data security (confidentiality, integrity) and privacy (authorization and anonymisation) in accordance with overarching organisational security policies. In ARTEMIS, healthcare providers define privacy policies that state

which healthcare professionals are able to access specific medical data. Since medical data are described using the clinical concepts, authorization are enforced based on the role of the healthcare professional and the clinical concept being accessed by them [8].

Conclusion: Its ISMS follows Principle 1, 2 and 3 of the proposed security model (i.e. it provides Replication of data, Access Privileges to the staff and also provides Encryption feature for Information's security) along with HIPAA and ISO 27799

Future Scope: Hospital can further improve the Security system by providing Summarized data for instant analysis and issuing Alerts for any threats or misuse.

POTOMAC HOSPITAL

It was founded in 1972. It is a non-profit community hospital located in Virgina. It has 183 beds, more than 1,000 employees including 250 medical professionals. They do not have the IT staff to manage large, complex networks or technology that does not perform as required. For the solution, they installed SonicWALL on hospital storage rack as a firewall. Later on, it was used across whole of the hospital's network. [10]

SonicWALL combines multiple network and security functions into a single integrated appliance. Wireless Access Points (WAPs) were integrated along with the SonicWALL firewall. Doctors can use Virtual Private Networks to transmit confidential documents to concerned patients or fellow doctors. It provide backup and recovery [10].

Conclusion: Its ISMS follows Principle 1, and 3 of the proposed security model (i.e. it provides Replication of data and also provides VPN technology for secure data transfer) along with ISO 27799.

Future Scope: It can further improve its Security system by providing Access Privileges, summarization of the information, and also providing Access Privileges to the staff. It should also comply with HIPAA standard.

GOOD SAMARITAN HOSPITAL

It was founded in 1908 and is located in Los Angeles, California, US. It is a non-profit healthcare system serving Indiana and Illinois with 8,000 inpatient per year and 250,000 outpatients per year. It does a lot of community work. When moved from paper records to electronic medical records, Good Samaritan needed to make sure it was taking the right precautions for the privacy and security of their patient's information. They chose AT&T Security Consulting to assess their security system. Through extensive onsite interviews and research, AT&T compared Good Samaritan's information security processes with industry's best practices. AT&T also conducted system penetration tests

to identify procedural weaknesses and "unlocked doors." They found several databases in engineering that didn't even have passwords. They changed the rules associated with our secure email so we can appropriately track and capture the information. Now hospital can extend their branches with no worry of database or network security. [11]

Conclusion: Its ISMS follows Principle 1, 2, 3 and 5 of the proposed security model (i.e. it provides Replication of data, assigns Access Privileges across all the hospital staff, provides Alerts and also provide VPN technology for secure transfer of information) along with HIPAA.

Future Scope: It can further improve its Security system by providing summarized data, for instant analysis and Decision Making. It should also comply with ISO 27799 standard.

NORTHWESTERN MEMORIAL HOSPITAL

Federal legislation through HIPAA; provided incentives for healthcare organizations to standardize their processes for log collection, analysis and retention; to better protect the confidentiality of patient's data. To comply with HIPAA regulations and gain greater insight into the IT infrastructure, Northwestern Memorial, which is located in Chicago searched for a log management solution that provided 100 percent log data collection and aggregation, as well as reporting and management features that would save time and reduce costs, while providing a high degree of security, scalability, and data accessibility. The Northwestern Memorial IT department maintains more than 12,000 IP devices to run its numerous programs and to support its staff. [12]

They were looking for a log management solution that could address the following challenges [12]:

- Collect security data from multiple VPNs, firewalls, and other network gear and keep it in a centralized repository.
- Access the data through fast searches and create meaningful [security] reports
- Generate alerts on data to improve insight into user activity and possible threats to the IT infrastructure.
- Store the data and access it later, with drill down capabilities to pinpoint network issues and threats.
- Seamlessly interoperate a heterogeneous network environment with different vendor devices and applications.

They selected LogLogic's Log Management solution and its features include [12]:

- It processes all syslog messages from connected devices, servers and applications in real time environment.
- It stores parsed and summarized copy of data upto 90 days for instant analysis or for decision support problems
- It can create graphical or text-based reports in minutes
- It can generate upto 13,000 custom reports
- Alerts can be set on device or group of device.
- Network and Security Managers can monitor log data and receive early warning of insider misuse or unusual behavior.
- Puts our eyes and ears on the network and gives the transparency to see whats happening in electronic frontiers
- We can see, virus infected devices, traffic denied by firewall and active connections in VPN.
- Using it, analysis has become faster
- IT department has gained insight into critical network log data

Conclusion: Its ISMS follows all the five principles along with HIPAA

Future Scope: It should also comply with ISO 27799 standard.

CONCLUSION

With this paper, we emphasize on the security of patients' data in various healthcare units with the help of cases of various international hospitals, which understood the need to protect the data and their IT infrastructure. Hence they started using various software or technologies, to overcome the issue. By doing so, they not only prohibited the entry of any unauthorized user but also gained the confidence of their patients. When patients feel confident of their privacy and the security of their information, they trust their health providers and share certain confidential but valuable information with their doctors. Thus, doctors can give correct diagnosis and treatment to them.

FUTURE SCOPE

Based on the comparative study of the eight International hospitals covered in this paper, a Capability Maturity Model of ISM process could be designed on the basis of defined principles for measuring the maturity of ISMS of few Indian Hospitals which is required for future growth of mature and reliable healthcare industry [14].

REFERENCES

1. A case study - LogLogic Improves Prognosis for Risk Management at Northwestern Memorial Hospital, https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCsQFjAA&url=http%3A%2F%2Fstructuredweb.com%2Fsw%2Fswchannel%2FCustomerCenter%2Fdocuments%2F7769%2F19285%2FlogLogic_Health_Care_Case_Study.pdf&ei=xtfDUarBOY7JrQfNm4CQBw&usg=AFQjCNERINVG_-gxhXJctP7PnXulFajcZg&sig2=CZ8IzfOJoL0XQkMV_XTY-g&bvm=bv.48293060,d.bmk
2. About ISO 27799, http://sl.infoway-inforoute.ca/downloads/ross_fraser_-_iso_27799.pdf
3. Alpana kakkar, Dr Ritu Punhani, Dr S Madan, and Dr D Jain. An Assessment of ISMS Process Maturity based on Readiness and Awareness of team members of team members of selected IT organizations. IARS International Research Journal, ISSN 1839-6518 vol 2 No 2, 2012
4. Alpana Kakkar, Ritu Punhani and D. Jain. Process Capability and Maturity in Information Security. IARS International Research Journal, ISSN 1839-6518 Vol 1, No2, 2011
5. Alpana Kakkar, Ritu Punhani, Dr S Madan and Prof D Jain. Implementation of ISMS and its Practical Shortcomings. IARS International Research Journal, ISSN 1839-6518 Vol 2, No 1, 2012
6. ARTEMIS: Towards a secure Interoperability Infrastructure for Healthcare Information Systems by Mike Boniface and Paul Wilken, https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CDUQFjAA&url=http%3A%2F%2Fwww.srdc.com.tr%2Fmetu-srdc%2Fprojects%2Fartemis%2Fpublications%2FBoniface-HG05-security-interoperability_final.doc&ei=adfDUdrELYP3rQfSu4CgBw&usg=AFQjCNEwiVmNA25bElyR3Kq4_Of4vDaceg&sig2=EwAe_9Y-19ybKGm_054rQw&bvm=bv.48293060,d.bmk
7. Case Study by FUJITSU, on Shanghai Shuguang Hospital, https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCsQFjAA&url=http%3A%2F%2Fwww.fujitsu.com%2Frs%2FImages%2FCS_Shanghai-Shuguang-Hospital.pdf&ei=VNfDUcr1KYSyrAfNxoG4Bg&usg=AFQjCNFmYgNYqFBYWnT1VKtIt9D5R5xbiA&sig2=gLcHfvUFlIxNZzh2K950YA&bvm=bv.48293060,d.bmk
8. Good Samaritan Hospital gets a security check-up – A case study by AT&T, http://www.business.att.com/enterprise/resource_item/Family/network-security/consulting/Case_Study/good-samaritan-hospital-security-consulting/
9. HIPAA, http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act
10. Hospital da Luz implements Cisco BioMedical Network Admission Control Technology to Increase Security. A case study by Cisco, https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCsQFjAA&url=http%3A%2F%2Fwww.cisco.com%2Fweb%2Fstrategy%2Fdocs%2Fhealthcare%2Fd

aLuz_hospital_cStudy.pdf&ei=I9fDUaHHNcaCrgf_0YHIBg&usg=AFQjCNEe68So2QpDgin9ZiC6bLepdm7iQg&sig2=a2AVsSX-ErLG0mmNAFLmTw&bvm=bv.48293060,d.bmk

11. IBM Case Study: Implementing database activity monitoring and auditing in a leading healthcare payer organization, https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCsQFjAA&url=http%3A%2F%2Fwww.ibm.com%2Fcommon%2Fssi%2Fcgi-bin%2Fssialias%3Finfotype%3DPM%26subtype%3DAB%26appname%3DSWGE_IM_DM_USEN%26htmlfid%3DIMC14608USEN%26attachment%3DIMC14608USEN.PDF&ei=fdfDUcixJM3JrAfRwoDgAQ&usg=AFQjCNFCeSsctM_8Xv_oIXfFhahqon9ffw&sig2=3naeT4gTNPArUuH3Nq847Q&bvm=bv.48293060,d.bmk
12. Information security and Privacy in healthcare: current state of Research by Ajit Appari and M. Eric Johnson, Published in Aug 2008
13. ISO 27799 standard format, http://www.27000.org/iso-27799.htm
14. Lehig Valley Hospital, https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=30&cad=rja&ved=0CHkQFjAJOBQ&url=http%3A%2F%2Fwww.eventtracker.com%2Fwp-content%2Fuploads%2F2012%2F08%2FLeHigh-Valley-DMReview-Case-Study.pdf&ei=r6bGUdnjNsyXrAer04DYCA&usg=AFQjCNHbUaxgSxTlaRgFUyTAykQyJ-voug&sig2=Csb9NnM5KiSd1pO4JwENUw&bvm=bv.48293060,d.bmk
15. Potomac Hospital Case Study, https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCsQFjAA&url=http%3A%2F%2Fwww.sonicwall.com%2Fapp%2Fprojects%2Ffile_downloader%2Fdocument_lib.php%3Ft%3DCS%26id%3D149&ei=l9fDUbTjA4LprAfH6IGAAg&usg=AFQjCNG29U-uH9u1cofSk1mSPG90uzMYig&sig2=rq1Taw40z0RocVMtPYs4sA&bvm=bv.48293060,d.bmk

– END –

Certificate of Recognition

This certificate is awarded to

Alpana Kakkar

in recognition of his contribution

"Future of healthcare vis-a-vis building trust in major stakeholders through Information Security Management (ISM)"

to Vol. 03, No. 01, 2013 *of*

IARS International Research Journal

.....

Chief Managing Editor

IARS International Research Journal 29 AUG 2013