Dissertation in

Jaypee Medical Centre, Noida

On

Planning of security and access control system in a tertiary care hospital

A Dissertation Submitted in partial fulfilment of the requirements for the award of

Post Graduate Diploma in Health and Hospital Management

By

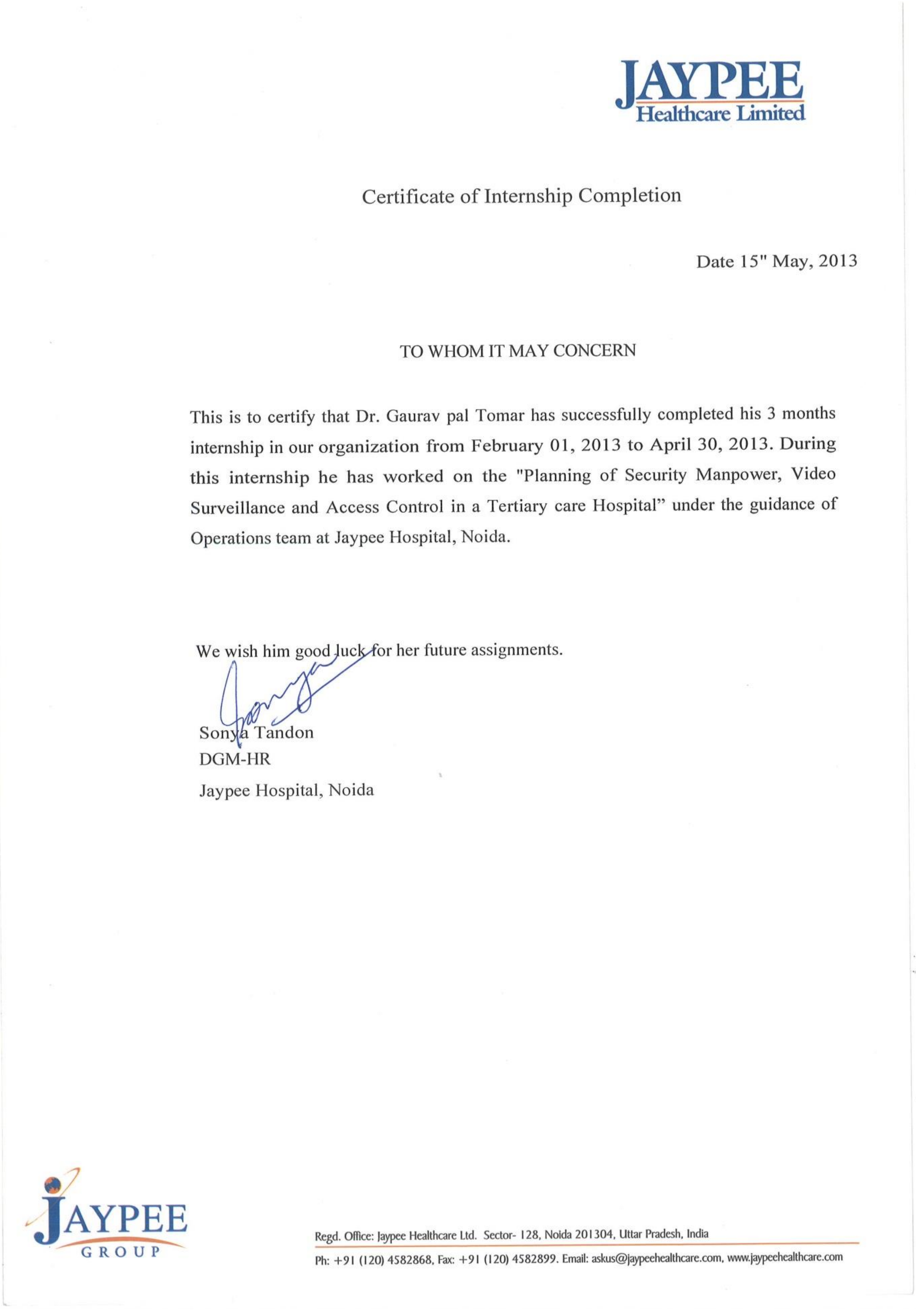
Dr. Gaurav Pal Tomar

(PG/11/028)

International Institute of Health Management Research

New Delhi – 110075

May, 2013



JAYPEE
Healthcare Limited

Certificate of Internship Completion

Date 15" May, 2013

TO WHOM IT MAY CONCERN

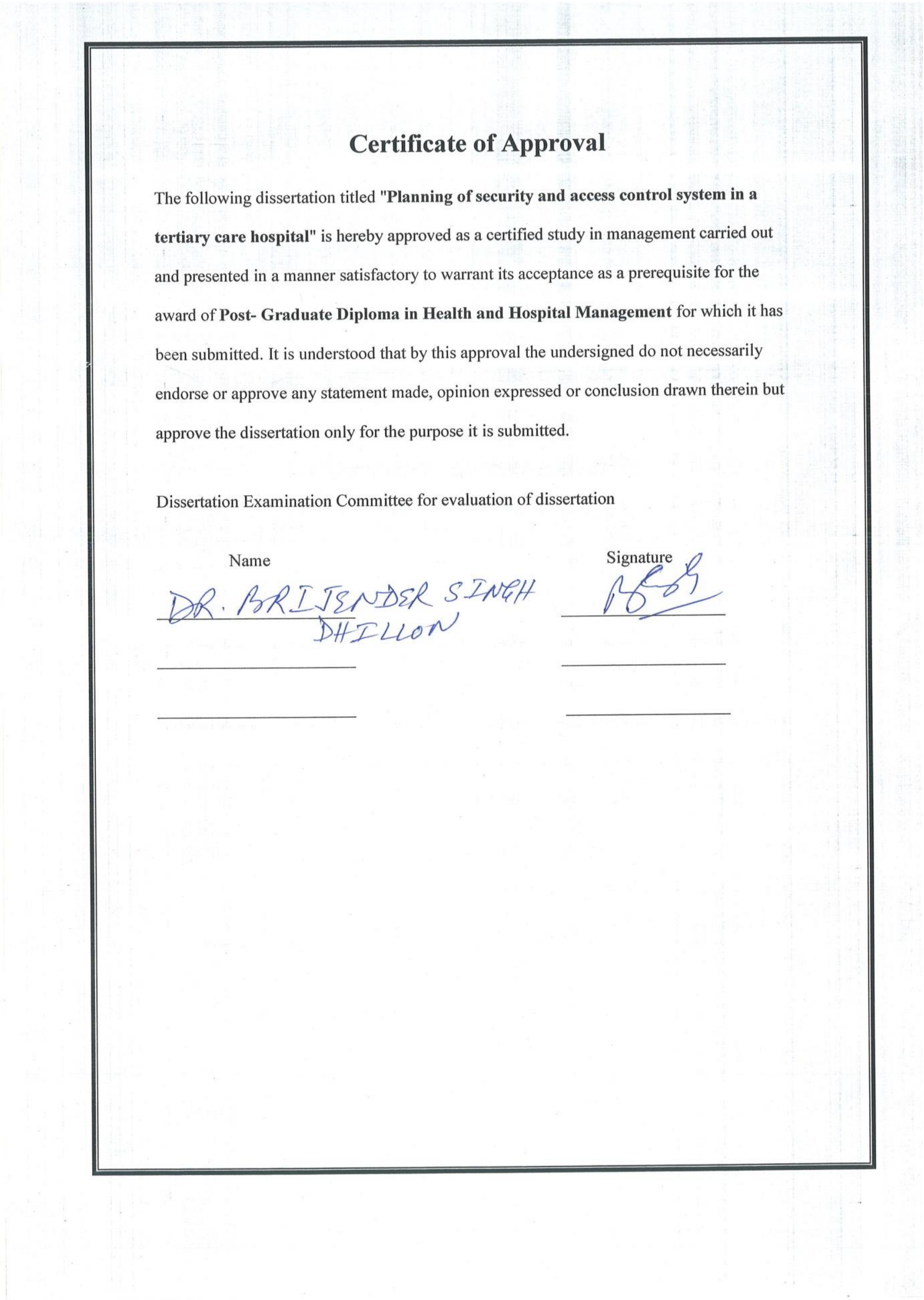
This is to certify that Dr. Gaurav pal Tomar has successfully completed his 3 months internship in our organization from February 01, 2013 to April 30, 2013. During this internship he has worked on the "Planning of Security Manpower, Video Surveillance and Access Control in a Tertiary care Hospital" under the guidance of Operations team at Jaypee Hospital, Noida.

We wish him good luck for her future assignments.

Sonya Tandon
DGM-HR
Jaypee Hospital, Noida

JAYPEE
GROUP

Regd. Office: Jaypee Healthcare Ltd. Sector- 128, Noida 201304, Uttar Pradesh, India
Ph: +91 (120) 4582868, Fax: +91 (120) 4582899. Email: askus@jaypeehealthcare.com, www.jaypeehealthcare.com

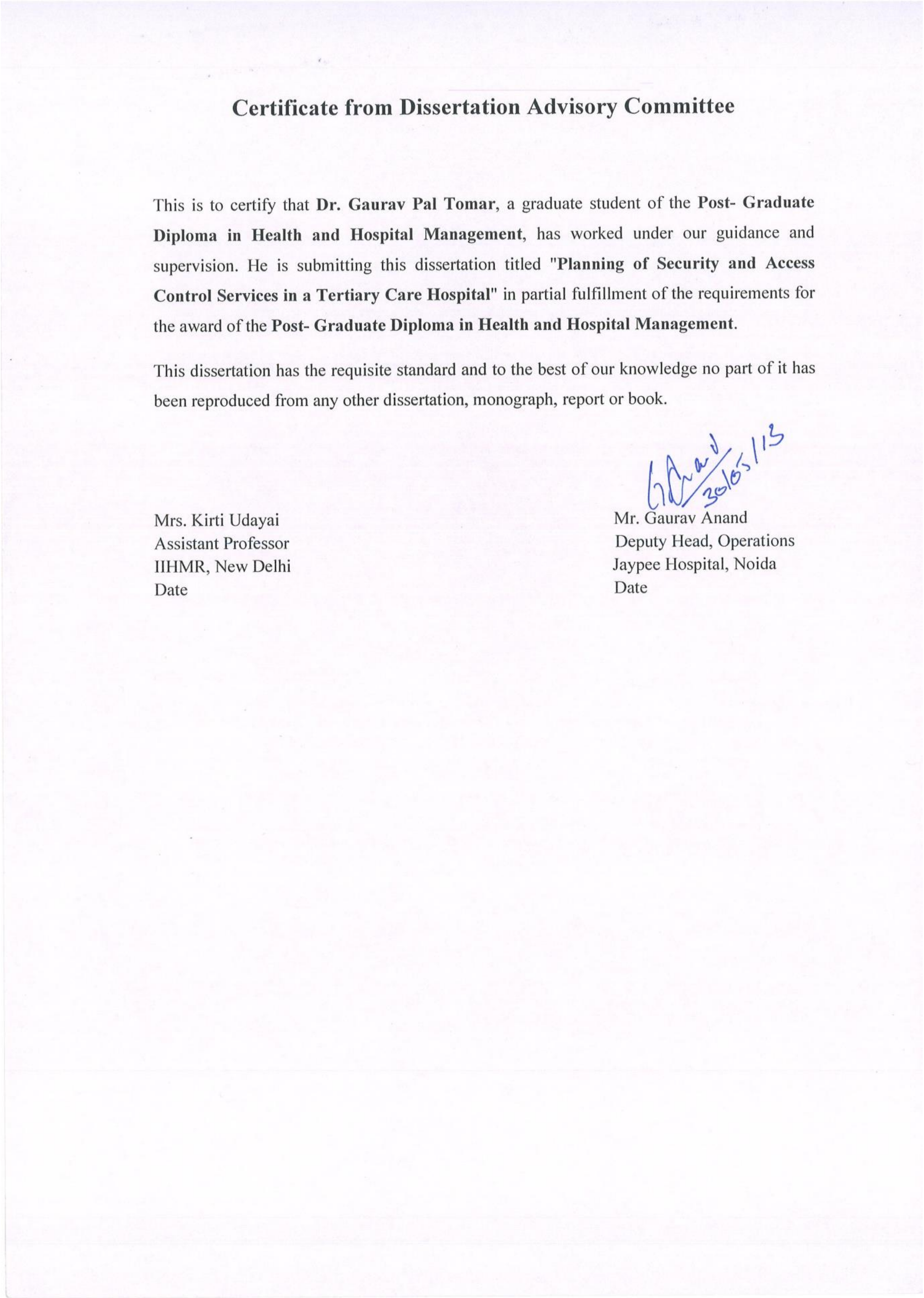


Certificate of Approval

The following dissertation titled **"Planning of security and access control system in a tertiary care hospital"** is hereby approved as a certified study in management carried out and presented in a manner satisfactory to warrant its acceptance as a prerequisite for the award of **Post- Graduate Diploma in Health and Hospital Management** for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the dissertation only for the purpose it is submitted.

Dissertation Examination Committee for evaluation of dissertation

Name	Signature
DR. BRIJENDER SINGH DHILLON	



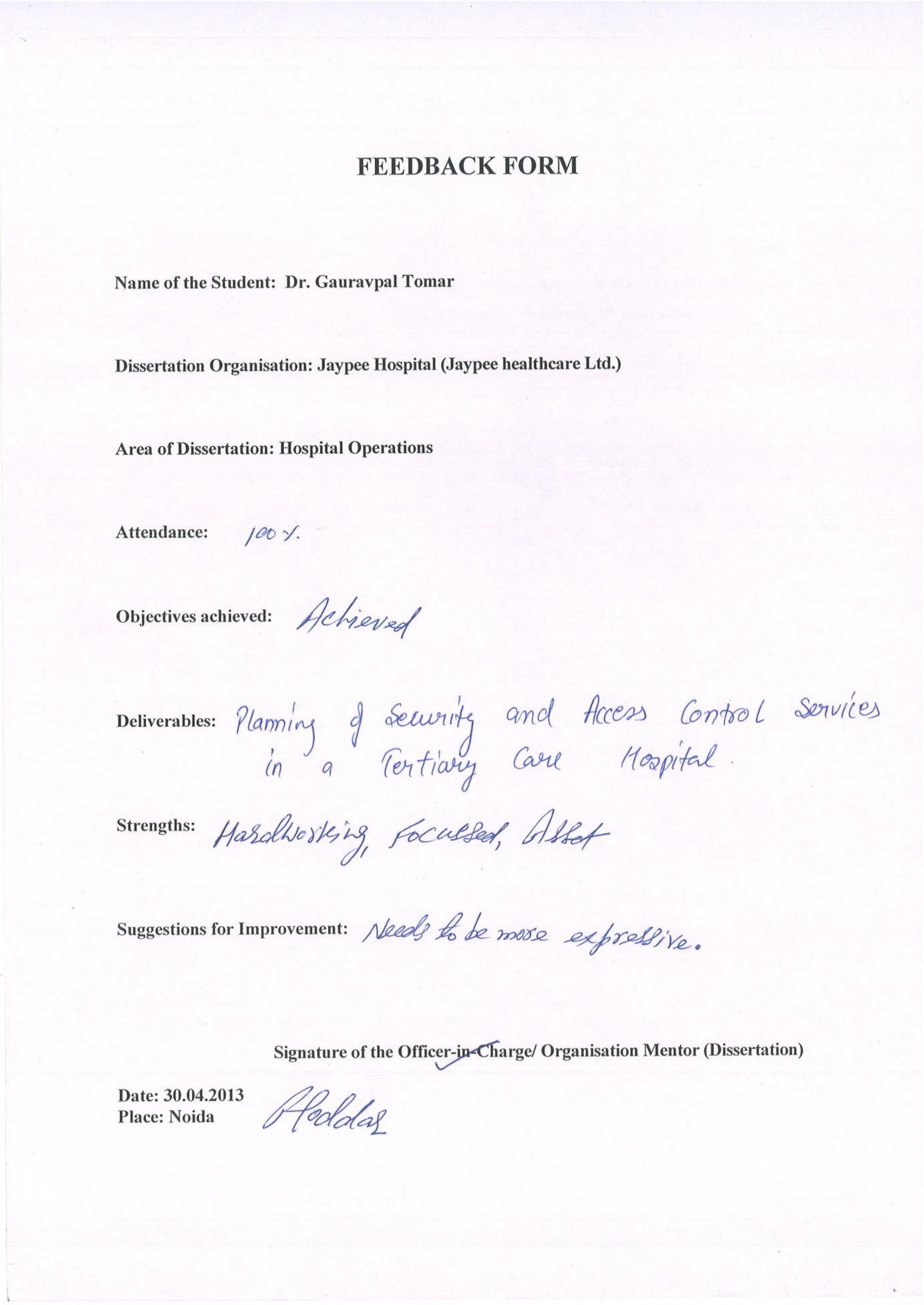
Certificate from Dissertation Advisory Committee

This is to certify that **Dr. Gaurav Pal Tomar**, a graduate student of the **Post- Graduate Diploma in Health and Hospital Management**, has worked under our guidance and supervision. He is submitting this dissertation titled **"Planning of Security and Access Control Services in a Tertiary Care Hospital"** in partial fulfillment of the requirements for the award of the **Post- Graduate Diploma in Health and Hospital Management**.

This dissertation has the requisite standard and to the best of our knowledge no part of it has been reproduced from any other dissertation, monograph, report or book.

GAnand
30/05/13

Mrs. Kirti Udayai	Mr. Gaurav Anand
Assistant Professor	Deputy Head, Operations
IIHMR, New Delhi	Jaypee Hospital, Noida
Date	Date



FEEDBACK FORM

Name of the Student: Dr. Gauravpal Tomar

Dissertation Organisation: Jaypee Hospital (Jaypee healthcare Ltd.)

Area of Dissertation: Hospital Operations

Attendance: 100%.

Objectives achieved: Achieved

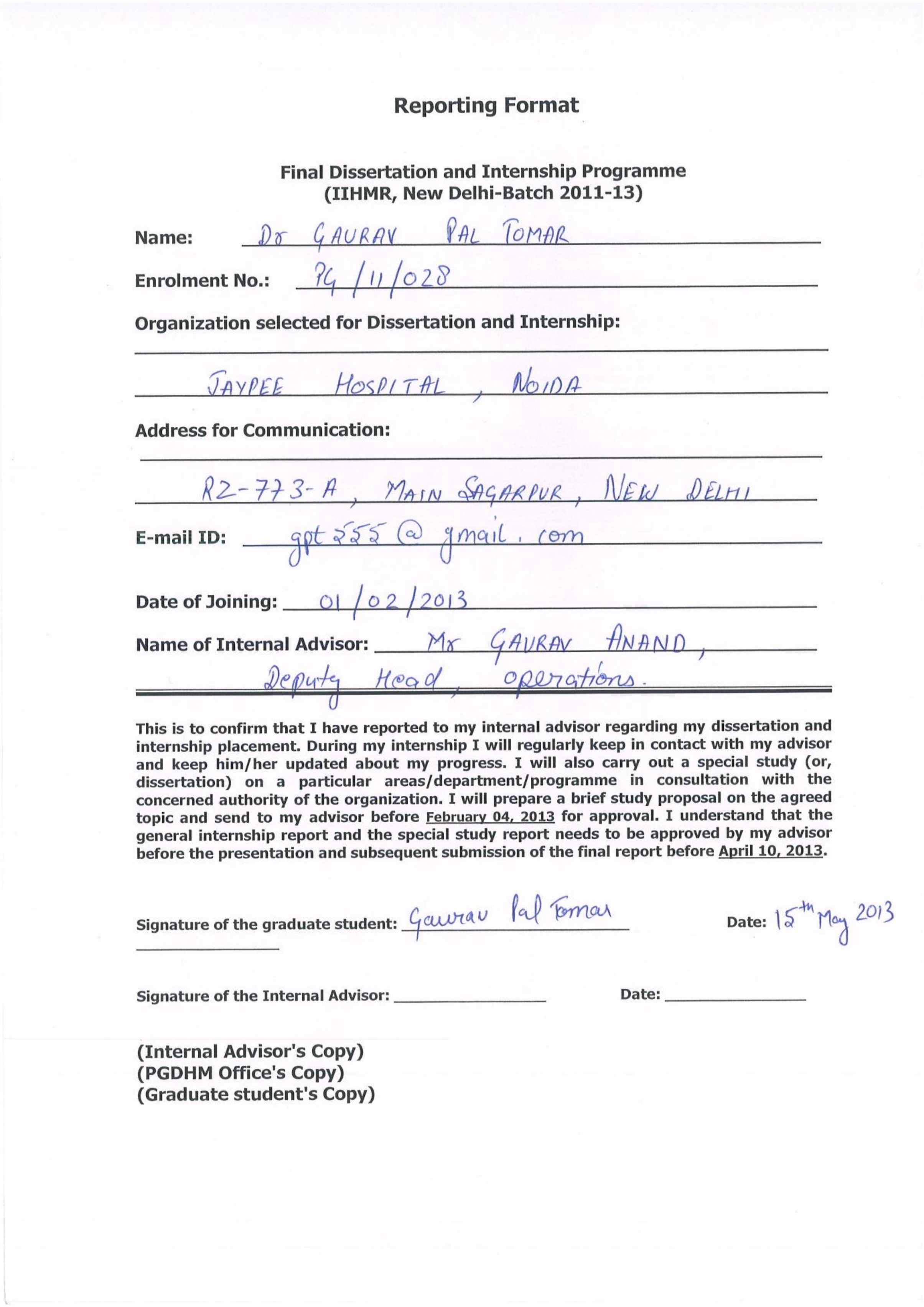
Deliverables: Planning of Security and Access Control Services in a Tertiary Care Hospital.

Strengths: Hardworking, Focussed, Asset

Suggestions for Improvement: Needs to be more expressive.

Signature of the Officer-in-Charge/ Organisation Mentor (Dissertation)

Date: 30.04.2013
Place: Noida



Reporting Format

Final Dissertation and Internship Programme
(IIHMR, New Delhi-Batch 2011-13)

Name: Dr GAURAV PAL TOMAR

Enrolment No.: PG/11/028

Organization selected for Dissertation and Internship:

JAYPEE HOSPITAL, NOIDA

Address for Communication:

RZ-773-A, MAIN SAGARPUR, NEW DELHI

E-mail ID: gpt555@gmail.com

Date of Joining: 01/02/2013

Name of Internal Advisor: Mr GAURAV ANAND, Deputy Head, operations.

This is to confirm that I have reported to my internal advisor regarding my dissertation and internship placement. During my internship I will regularly keep in contact with my advisor and keep him/her updated about my progress. I will also carry out a special study (or, dissertation) on a particular areas/department/programme in consultation with the concerned authority of the organization. I will prepare a brief study proposal on the agreed topic and send to my advisor before February 04, 2013 for approval. I understand that the general internship report and the special study report needs to be approved by my advisor before the presentation and subsequent submission of the final report before April 10, 2013.

Signature of the graduate student: Gaurav Pal Tomar **Date:** 15th May 2013

Signature of the Internal Advisor: ________________ **Date:** ________________

(Internal Advisor's Copy)
(PGDHM Office's Copy)
(Graduate student's Copy)

Acknowledgment

Apart from hard work, the success of any project depends largely on the encouragement and guidelines of many others. I take this opportunity to express my gratitude to the people who have been instrumental in the successful completion of this project.

I show my greatest regard to **Dr. Rajesh Bhalla** (Dean Academics, IIHMR, New Delhi) and to my mentor **Mrs. Kirti Udayai** (Assistant Professor, IIHMR, New Delhi) for helping me out and guiding me during my dissertation.

I would like to show greatest appreciation to **Dr Vikram Singh Raghuvanshi, CEO** at **Jaypee Hospital** and **Mr Gaurav Anand (Deputy Head, Operations)** at **Jaypee Hospital, Noida** for providing me the opportunity to do Project on Planning of Security and Access Control Services in a Tertiary Care Hospital and for providing complete support throughout my dissertation. Without their encouragement and guidance my work would not have materialized.

I would like to extend my sincere thanks to **Mr Rajesh Dixit, Mr Santosh Mudilar, Mr. Jaideep** & **Mr. Laxmikant** who always guided me in difficult times of my work.

I will also thank all my colleagues of both IIHMR Delhi and IHMR Jaipur who have willingly helped me out with best of their abilities. I owe a lot to their generosity and nice gesture.

Table Of Contents

List Of Tables

List Of Charts

Abbreviations

JMC – Jaypee Medical Centre

JSS – Jai Prakash Seva Sansthan

CCTV – Closed Circuit Television

DVR – Digital Video Recorders

HIPAA – Health Insurance Portability and Accountability Act

RFID – Radio Frequency Identification

OPD – Out Patient Department

IPD – In Patient Department

ROI – Return on Investment

SOP's – Standard Operating Procedures

CSO – Chief Security Officer

SSO – Senior Security Officer

SO - Security Officer

QRT – Quick Response Team

DFMD – Door Frame Metal Detector

HHMD – Hand Held Metal Detector

HOSPITAL PROFILE

ABOUT JAYPEE GROUP

- The Jaypee Group is a 15,000 crore well diversified infrastructural industrial conglomerate in India.

- Shri. Jaiprakash Gaur, Founder Chairman of Jaiprakash Associates Limited after acquiring a Diploma in Civil Engineering in 1950 from the University of Roorkee (now Indian Institute of Technology Roorkee), had a stint with Govt. of U.P. and branched off on his own, to start as a civil contractor in 1958, group is the 3rd largest cement producer in the country

- Jaypee Group is five decade old conglomerate based in Noida, India, involved in various industries that include Engineering, construction , Cement, Power, Hospitality, Real Estate, Expressways, Highways, Education and Social Commitment.

Figure 1 : Prototype of Jaypee Medical Center

- The groups cement facilities are located today all over India in 10 states, with 18 plants having an aggregate cement production capacity of 24 Million Tones and same is poised to become 36 Million Tones before October 2011

SPREAD OF THE COMPANY

CEMENT

- Jaypee Group is the 3rd largest cement producer in the country. The group produces special blend of Portland Pozzolana Cement under the brand name ‘Jaypee Cement’ (PPC). The company is in the midst of capacity expansion of its cement business in Northern, Southern, Central, Eastern and Western parts of the country and is slated to be 35.90 MnTPA by FY12 (expected) with Captive Thermal Power plants totaling 672 MW

ENGINEERING & CONSTRUCTION

- The Engineering and Construction wing of the Group is an acknowledged leader in the construction of multi-purpose River Valley and Hydropower projects. It has the unique distinction of having simultaneously executed 13 Hydropower projects spread across 6 states and the neighboring country Bhutan for generating 10,290 MW power

SPORTS

- The Group finished the construction and execution of India’s first ever F1 Grand Prix on 30th October, 2011. In addition to F1, the track will also host other top-level international motorsports events from 2012 onwards.

HOSPITALITY

- The Group’s hospitality business owns and operates 6 properties spread across New Delhi, Uttar Pradesh and Uttarakhand. The 4 Five Star Hotels, two in New Delhi and one each in Agra and Missouri have a total capacity of 644 rooms.

EDUCATION

- “People of resources must contribute towards making a better tomorrow for all”. Shri Jaiprakash Gaur ji, Founder Chairman of the Group firmly believes that quality education on an affordable basis is the biggest service which, as a corporate citizen, we can provide. Education is the cornerstone to economic development and the strength of 1 billion Indians can be channelized by education alone to build India into a developed nation

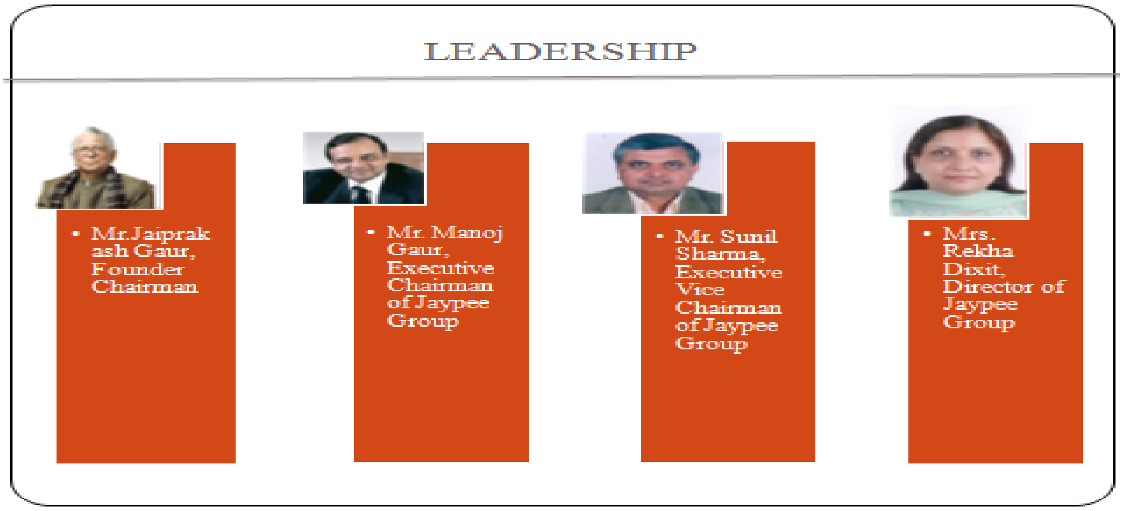
REAL ESTATE AND EXPRESSWAYS

- The Group is a pioneer in the development of India's first golf centric Real Estate. Jaypee Greens - a world class fully integrated complex consists of an 18 hole Greg Norman Golf Course. Stretching over 452 acres, it also includes residences, commercial spaces, corporate park, entertainment and nature in abundance. Jaypee Greens also launched its second project in Noida in November 2007. India's First Wish Town, is an Integrated Township spread over 1162 acres of land comprising one 18 hole and two 9 hole golf facility & world class residences.

SOCIAL COMMITMENTS

- The Group has always believed in "growth with a human face" and to fulfill its obligations it has set up Jaiprakash Sewa Sansthan (JSS), a 'not-for-profit trust' which primarily serves the objectives of socio – economic development, reducing the pain and distress in society. For over 4 decades now, Jaypee Group has supported the socio-economic development of the local environment in which it operates and ensured that the economically and educationally challenged strata around the work surroundings are also benefited from the Group's growth by providing education, medical and other facilities for local development .

LEADERSHIP TEAM



LEADERSHIP

- Mr.Jaiprakash Gaur, Founder Chairman

- Mr. Manoj Gaur, Executive Chairman of Jaypee Group

- Mr. Sunil Sharma, Executive Vice Chairman of Jaypee Group

- Mrs. Rekha Dixit, Director of Jaypee Group

Figure 2 : Leadership Team

THE LOGO OF JAYPEE MEDICAL CENTRE:

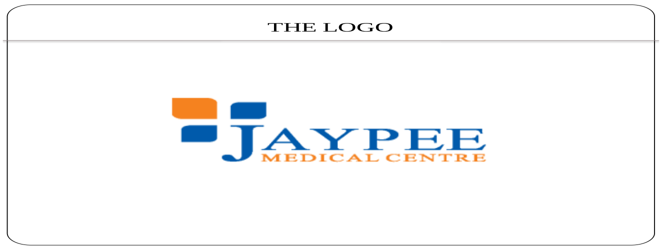


Figure 3 : Logo

- **The leaf** represents that we are environment friendly and follow medication safety. The sharp edges and corners represent the modern side (cutting edge technology and world class infrastructure) and the rounded corners represent the patient-care side of Jaypee Medical Center.

- **The Blue in Jaypee** is identified with Confidence, Credibility and Competence, represents Jaypee Medical Center’s multi-disciplinary capability, cutting edge technology and service foundation built on world-class infrastructure and processes.

- **The Orange** represents the vibrancy, high energy and 'let's make it happen' attitude of our people.
- **The Orange in leaf and Medical Center** represents that we are a New Life in the group which is supported by Blue Leafs and J of Jaypee Group as pillar of strength.

VISION

"Promoting healthcare to the common masses with the growing needs of society by providing quality and affordable medical care with commitment."

-Founder Chairman's Vision on Healthcare

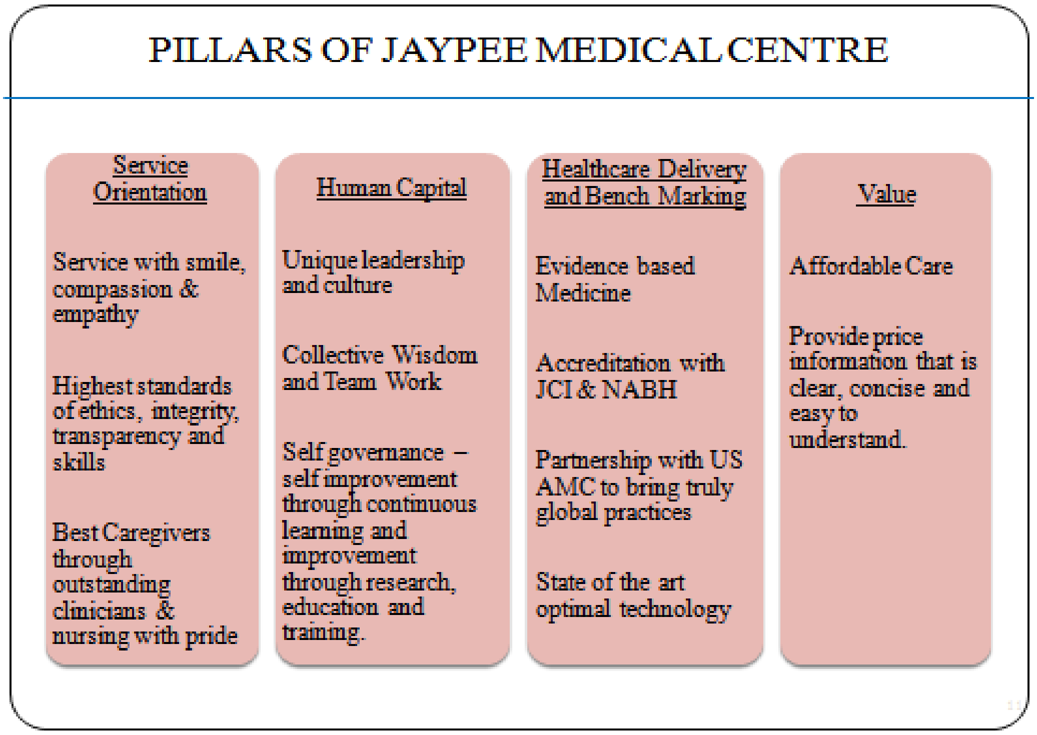
MISSION

"The Jaypee Group is committed to meet the healthcare needs of the population in Noida and the surrounding regions through building Jaypee Medical Center as a super specialty hospital with advanced healthcare facilities, the latest diagnostic services, and state-of-the-art technology focused on medical specialties that meet the needs of the population. The Jaypee Medical Center will be the ultimate choice for medical care."

JAYPEE GROUP –HEALTHCARE PHILOSOPHY

- Three Secondary care medical facilities currently operational at –Bhutan, Rewa (M.P) & Baspa (H.P) providing care to approximately One million lives treated annually.
- Other Healthcare Initiatives - Medical Camps, Pulse Polio Camps, Maternity camps, Health Checkup of Village Children, Health & Hygiene Awareness Camps
- Mobile Medical Van (with Lab and other diagnostic facilities) Diagnosis and medicine distribution free of cost (about 100 patients per day).

PILLARS OF JAYPEE MEDICAL CENTRE



PILLARS OF JAYPEE MEDICAL CENTRE

Service Orientation	Human Capital	Healthcare Delivery and Bench Marking	Value
Service with smile, compassion & empathy	Unique leadership and culture	Evidence based Medicine	Affordable Care
Highest standards of ethics, integrity, transparency and skills	Collective Wisdom and Team Work	Accreditation with JCI & NABH	Provide price information that is clear, concise and easy to understand.
Best Caregivers through outstanding clinicians & nursing with pride	Self governance – self improvement through continuous learning and improvement through research, education and training.	Partnership with US AMC to bring truly global practices	
		State of the art optimal technology	

Figure 4 : Pillars of Jaypee Medical Centre

OVERVIEW OF JAYPEE MEDICAL CENTER[1]

- Flagship Hospital of the Jaypee Group
- Spread over 110000 Square Meters of campus
- Total Beds: 1000 beds. (505 Beds in Phase 1)
- Proposed Nursing School on campus
- Would be a LEED Certified building
- Would target for Joint Commission International accreditation in first year

SERVICES TO BE OFFERED

CENTERS OF EXCELLENCE

Specialties and Super Specialties:

- Cardiac Science
- Neuro science
- Bones and Joints
- Minimal invasive surgery
- Cancer Unit
- Critical Care Medicine
- Trauma
- Mother & Child Care
- Gastroenterology
- GI Surgery
- Internal Medicine
- General Surgery
- Endocrinology/Rheumatology
- Urology & Nephrology
- Physical Medicine
- Rehabilitation Services
- Advanced Diagnostics-Lab Medicine/Radio Imaging/Transfusion Medicine
- Aesthetic Medicine Centre
- Behavioral Science

Figure 5 : Services to be offered

FLOOR WISE DEPARTMENTAL PLANNING

Sl. No.	FLOOR	DEPARTMENTS
1	Seventh	Wards
2	Sixth	Wards
3	Fifth	Wards
4	Service	IT Server, AHU, PTS station and MEP
5	Fourth	OT Complex, ICCU, Cath lab.
6	Third	Economy Bed, IVF, MICU, SICU, NICU, LDR
7	Second	Chemotherapy, Cosmetology, Endoscopy, Physiotherapy, Paediatric, Office.
8	First	Behavioural science, Ortho. , Neuro. , Gen. Surgery/MAS, Pulmonology, Opthal. , Dental, ENT, Diabetes Cardiac.
9	Ground	Executive Health Check up, Dialysis, Radiology, Day care, Emergency and Trauma, Pharmacy.
10	Upper basement	Blood Bank, Pathology Laboratory, Nuclear medicine, Kitchen, Administration.
11	Lower basement	Bio-medical Eng., Radiation Oncology, Laundry, Mortuary, CSSD.

TASK PERFORMED IN THE ORGANIZATION

- Assisted in nursing man power planning of Jaypee medical center
- Assisted in nursing man power planning of Jai Prakash Seva Sansthan, Rahogarh, Guna
- Assisted in planning of swing doors and steel paneled doors for Jaypee medical center
- Assisted in planning switches for an upcoming hospital of Jaypee in Chitta
- Assisted in designing of consent forms for Jai Prakash Seva Sansthan, Rahogarh, Guna
- Assisted in designing a Fire plan & Signage plan for Jai Prakash Seva Sansthan, Rahogarh, Guna
- Assisted in preparing a Budget plan for Jai Prakash Seva Sansthan, Rahogarh, Guna and Vivekanand Medical Institute, Palampur
- Working on hospital policy manual according JCI & NABH for Jaypee medical center
- Working on consent forms for Jaypee Medical center
- Working on making marketing plan for 2013-14 for Jai Prakash Seva Sansthan, Rahogarh, Guna and Vivakanand Medical Institute, Palampur

LEARNINGS

- Learned basics of nursing planning in a hospital
- Learned basics of Fire plan and signages plan for any hospital
- Learned how to plan out a budget for any hospital
- Learned how to make policies for a hospital with help of a systematic format
- Learned how to make a marketing plan for a hospital
- Learned how to do security and access control planning for a hospital

Introduction

Hospital security is a unique challenge. Considering the variety of people who access a hospital environment - patients, staff, vendors, physicians, visitors and even their relatives. Considering the place many different rooms and spaces, high-value equipment and consumables, accessibility to drugs (narcotics), many entrance and exit points and ease-of-movement around the building and premises.

Therefore the security plan of a facility needs different approaches to security. It should be such that it does not hinder the accessibility to patient but at the same time restricts unwanted movement inside the hospital. Hospital managers base their security decisions on the basis of law, costs, and fear of litigation that protects their facility's reputation.

.Professionals should look at the threats likely in specific areas:

- the emergency/trauma department (gang fights, vendettas, domestic conflicts, child custody conflicts, VIP patients);
- infant care area (infant abduction, need for CCTV and infant security);
- pharmacy/drug storage area (alarm and access control systems);
- prisoner care area (receiving, elevator lock-off, surveillance, command center);
- operating rooms (access control, delayed egress hardware, CCTV),
- labs (access control, duress alarms, CCTV);
- nuclear medicine area (access control, CCTV);
- geriatric care area (patient locators, CCTV);
- psychiatric care area (lock-down capability, access control, staff duress, solitary room);
- morgue (decedent services area, access control, alarm system, CCTV);
- PBX area (late-night security, rest room security, door release, duress alarm).

Don't forget such places as the parking lot (lighting, access control, CCTV in stairwells, duress alarm at fee collection booth), food service area (duress alarm), gift shop (burglar alarm, duress alarm) and shipping/receiving areas (CCTV, patrol). And study the threat potential of biohazard waste storage and disposal (CCTV, access control).
New products such as alarm pagers, infant abduction detection systems, patient wandering systems,

CCTV video pursuit systems, people trackers and asset protection systems can each enhance hospital security. *Hospitals have grown with time and so is the need of security.*

In Past

Hospitals and churches have always been considered sacred. It was inconceivable that anyone would violate the sanctity of a hospital and commit a crime, much less steal a baby. Unfortunately, hospitals are no longer immune from criminal assault. Crime continues to find its way into our hospitals at an alarming rate. Why does this happen? Well, for one thing, hospitals are institutions of tradition, and historically have resisted becoming bastions of security. The emphasis has always been on providing open and friendly access to the public.

Part of a hospital's image has been to maintain an open door policy for anyone and everyone that wished to visit a sick family member or love-one. People used to go to the hospital just to see the babies. There was nothing unusual at all for strangers to be seen on the baby floor. [2]

In Present

As crime continues to grow in country, we find we are not safe in our businesses or in the schools, and now, even in the hospitals. All of these places have become targets of criminal assault, and as a result, we have been forced to increase security in every facet of our public and private life to keep crime away. Most hospitals have been slow to follow suit. Even today, many hospitals still have the same open door policy they have practiced for decades.

Hospitals are targets because they are open to the public 24 hours a day, seven days a week. These public access facilities have been conditioned over the years to allow scores of people from all walks of life to enter these institutions unchallenged. The definition of "public access" means that all persons who enters a hospital seeking treatment, or to visit a love-one, have the right to come and go as they please. This mind-set does not take into consideration there are people in our society that hold no institution sacred, and their sole reason to enter a hospital is to commit a crime against a person, or the hospital, or both.

Unfortunately, because of the continuing criminal threat against hospitals, it's no longer possible to practice an open door policy. For a hospital to be safe in today's world everyone coming into and going out of the facility has to be identified and their access controlled. This is essential to prevent unauthorized persons from entering a hospital to cause harm. *Access control* has been extremely difficult in the past because of unrealistic and misinterpreted fire codes. Strict enforcement of fire codes have prevented hospitals from securing fire doors that lead to the outside. An unsecured fire door leading to the outside provides an escape route for anyone that has committed a criminal act against a hospital. After what seems like forever, old fire codes are now being replaced with new codes which will now allow fire exits to be locked and alarmed by a time-delay lock and alarm system. This type of "lockdown" capability can prevent unauthorized persons from entering or leaving the hospital undetected.

Another significant problem with providing security for older hospitals is their inherently open design which makes them more difficult to secure. Traditionally hospitals have been designed for patient and family convenience. Security was never taken into consideration during the design and construction phase. Because of this inherent problem, retrofitting security protection in older facilities is a security nightmare, not to mention unbelievably expensive.

In Future

Even though hospitals are faced with enormous downsizing and decreasing revenues as a result of "Managed Care", hospitals do have options. First, they can accept the risk and hope that nothing ever happens. Or they can reduce the risk by developing a plan that incorporates physical security, access control, and staff education into a state-of-the-art security management program. The Joint Commission for the Accreditation of Healthcare Organizations requires that organizations develop a written security management plan as well as conduct annual security assessments to identify security vulnerabilities.

Hospital facilities are usually comprised of a number of buildings with many entrances, rooms, areas with high-value equipment, supplies, drugs and a variety of people - patients, visitors, staff and vendors - with a need to move about freely. Controlling this environment from a security perspective requires knowledge of current and future physical and logical access needs, coupled with an understanding of the standards and regulations facing today's health care practitioners. As part of physical security, health care security practitioners are implementing the latest state-of-the-art security systems for access control, video monitoring and communication, which will also improve their staff's productivity.

Points of Entry

Visitor control in this type of environment for the hospital security practitioner is one of their most difficult tasks.

As part of controlling patient visitors, some hospitals have implemented a *visitor management system* which enables security officials to track who is in the building and ensures visitors are only allowed access to certain areas of the hospital. Hospital security staff and/or volunteers can scan the visitor's driver's license. The visitor's information is automatically entered into a database and a visitor pass is printed on a label, which is then worn by the visitor for the duration of their visit. The system can also be integrated onto the hospital's network for continual update with the patient data system to verify that the patient is registered. Some children's hospitals have implemented a feature that checks a visitor's name against the national sex offender registry.

Video cameras should be located in the immediate lobby areas and typically include the gift shop. They provide the security officer the ability to view and assess a potential security issue on video monitors or video workstations that may be located at the concierge/security post. All video cameras throughout the hospital facility should be recorded at all times.

Respective community crime factors and quality-of-life issues are mirrored within each hospital environment and are most evident in the ER (emergency room) waiting area of urban and inner-city health care institutions. It is not uncommon for ER staff members to be subjected to verbal and sometimes physical abuse that may arise from domestic conflicts, child custody disputes, gang violence, drug users and psychiatric patients.

Triage staff members, in particular, are usually the target of verbal abuse - particularly by patient family members. In response to that potential event, each triage station should be provided with a duress device or personal alarms that summons the security officer. Proper deployment of video cameras in the ER should ensure that these stations are also within camera view. The ER pedestrian and ambulance entrances, the waiting room and the psychiatric observation rooms are areas where cameras should also be deployed.

Since emergency rooms in hospitals operate around the clock, most institutions will provide continuous security personnel presence in the area. The officer is normally positioned at a fixed post that has sub components of the facility's security system which provide the ability to monitor ER alarms, view all ER cameras and remotely control the operation of doors in the immediate area.

Using card access-controlled doors between the waiting room and the ER treatment area can be very useful in limiting patient visitors and eliminating unwanted and distracting pedestrian activity between the two areas. Card access control may also be applied at the ambulance and pedestrian entrances as well as entrances leading into the ER treatment area from other areas of the building.

During certain periods - typically on weekends - some hospitals will deploy magnetometers to scan individuals who seek treatment in their ER.

Common Areas of Security Concern

Access Control: The application of access control can be one of the most important elements of a hospital's security solution. Access control refers to managing who is allowed to enter where and when, including limiting access to people, places, and things and - via an audit trail - having the ability to track and monitor individuals and assets. According to the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), one element of performance by which a hospital's environment of care is measured is that "the hospital controls access to and egress from security-sensitive areas, as determined by the hospital."

A high level of security is required for areas such as operating theatres and diagnostic suites, to ensure entry by authorized staff members only. Card access control devices for these critical areas need to be reliable, fast, hands-free and easy to use.

Material Storage: A primary problem with loading dock and material storage security is that most hospitals lack permanent security supervision in these areas. Add to this the sometimes relaxed attitude of the shipping and receiving operation by leaving doors open or the area unattended, and many hospitals are left dangerously vulnerable to theft.

Proper loading dock security starts with comprehensive policies and procedures for shipping and receiving operations. Card access control on doors, asset management systems, inventory management systems, intelligent video management and advanced integration of these should help in limiting the losses.

To minimize pilferage of foodstuff, dietary services departments should use card access control combined with video cameras in their food storage rooms as well as walk-in refrigerators and freezers.

Compliance: To maintain compliancy with HIPAA regulations, some healthcare organizations are combining smart card technology with biometrics for access to patient and employee records as well as pharmacy access control.

Infant Protection: A hospital administrator's biggest concern is the fear of litigation and a potential incident that would damage the institution's image. The abduction of an infant from the hospital's maternity ward would probably lead to both. To prevent such an incident, many hospitals that provide birthing centers with maternity and pediatric wards have installed infant monitoring systems.

An infant protection system is comprised of a small, tamper-proof tag that is placed on the infant's ankle or wrist immediately after birth. Should an infant be carried toward an exit door, the system will automatically set off an alarm with video at the local nurse's station and at the central security room, activate door locks including stairwell exit doors and hold selected elevators. These systems will integrate with access control systems, video cameras located at the various doors, public address systems, pagers, fire systems and other security alarms. Some systems also have the ability to automatically confirm that the right baby is with the right mother by providing an audible signal when the infants and mothers are correctly matched.

Terrorism: Large medical centers with research facilities may be using Cesium 137 Blood Irradiators. Recent world events have raised a concern that the radioactive material in them could be used by terrorists to construct a so-called "dirty bomb."

The NRC (Nuclear Regulatory Committee) has mandated strict requirements - some of which include biometric access controls with alarm detection and video assessment, background checks for personnel with access to the materials, assessment and response capabilities; transportation controls; and Information protection.

Laboratory Security: Hospitals with research capabilities will probably also have laboratories and vivariums that house the animals that are used as part of their research. These areas also require stringent access control not only from a security perspective but also to ensure that these areas are maintained within a controlled environment.

Card Access Solutions

As one of the most common card technologies, the magnetic stripe has been in use for many years in the healthcare environment due to their relatively low cost. Today, with higher associated maintenance costs, many healthcare campuses are installing new proximity card readers that provide more functionality combined with less maintenance.

Proximity cards are read rapidly and easily by simply presenting the cards within a prescribed distance to the reader. Magnetic stripe cards require the motion of "swiping" or insertion, which at times necessitates several attempts for a valid read. In vital applications such as in a hospital - where time to access an area could involve a life-and-death situation - the proximity readers certainly provide the superior functionality.

For hospitals contemplating a switch to proximity, dual-technology cards (magnetic stripe and proximity) would provide a solution during the transition period to support the older technology while moving to the more reliable, higher functionality.

For years, many healthcare facilities have relied on multiple card credentials to fulfill different tasks. It is still not unusual to enter a hospital and find staff members wearing multiple badges for various reasons. Many hospitals are contemplating and switching to a smart card to create a one-card solution. Using both contact and contactless smart chip technologies, a single credential can handle a bar code for inventory control, a photo of the employee for identification, a dollar value for use in the cafeteria, a biometric template for data protection in the IT department, and proximity technology for access control.

Video Solutions

The application of video cameras in most healthcare facilities is used primarily as an investigative tool to assist in the review of an incident that has occurred. Video cameras provide additional and remote "eyes" that enable minimal security staff to observe multiple remote locations, either in real-time or recorded for future review. They are also an overt reminder that a security system is present. Where possible, camera views should be associated with alarm conditions to assist in alarm assessment. For instance, upon an alarm condition on the infant monitoring system, associated camera views can automatically be displayed at the pediatric ward nurse's station, the lobby security post and the hospital's security response center.

Healthcare facilities typically record and store camera views on computer hard drives for at least 31 days. These computers or digital/network video recorders have the capability of residing on the hospital's IT network or on a private network dedicated to security.

Unlike analog video cameras that rely on point-to-point cabling, IP or network cameras are designed to transmit over a network where video signals and power are transmitted on the same cable. IP cameras are becoming a popular and an important part of the healthcare security infrastructure due to their cost-effective ease of installation.

Video Analytics is a fairly new technology which has been applied in the healthcare environment. Examples of video analytics applications include: counting the number of people entering a hospital's lobby door or vehicles entering a hospital's parking lot.

Video analytics can also be used to generate an alarm when individuals attempt to enter a restricted or closed off area of a hospital. It can also determine the location, speed and direction of travel of pedestrians and vehicles and can be used to identify suspicious behavior of people.

Today's ever-changing and evolving health care facilities and hospitals present unique challenges for security. Security practitioners need to be proactive and adopt a non-conventional approach to maintain that same pace.

The efficiency for ‘Building Evacuation’ is therefore highly improved with the RFID technology as all persons, assets and equipment can be located, directed and accounted for within seconds. Various tags increase the number of applications manageable by access control operators for tampering, tracing, tracking and auditing.

Deliveries and Collections security is enhanced as the RFID technology tag and system tracks the assets from when it obtains the tag until the asset is moved or leaves the premises.

High value assets, trade secrets, laptops, 3G tablets, samples, equipment can be traced quickly and zoned to specific departments for higher security measures, and therefore speedily a ‘stock take’ can be viewed instantly.

Improved Environmental Security is enabled for temperature or humidity as alarming can be enabled into the system. To elaborate, there may be samples, fridges or equipment that is reliant on specific temperature or humidity conditions.

Applications adapt the system and equipment to suit the needs of all vertical markets, for example: health care; whereas, a hospital requires a higher level of access control for quarantine security, or anti wandering device for the mentally ill to the kidnap protection system of new born children.

‘Securing Research and Development departments’, or ‘Patent Attorneys’ have safes, filing cabinets safeguarding information worth millions of dollars in value. The addition of the RFID motion detectors or tamper alarming, provide a higher level of maximum security against industrial espionage.

In case of power outages, the system has rechargeable batteries, and therefore remains in active mode thus sustaining the system.

The “New Generation Access Control System” now incorporating the RFID matured technology provides the operators a fully fledged management system that can be used for applications which could be used by other departments such as the Financial and Accounting division or Warehouse and Stores Manager.

Security and Parking: The entire security service of the hospital and parking management of the hospital includes:

- 24 hours security service of the hospital
- Crowds management in OPD, IPD and other areas of the hospital
- Security personnel to take initiative during disaster management and safety management of the hospital in coordination with other staff of the hospital
- Vehicle parking system to be manage properly to reduce crowding in the hospital campus
- Parking lot to be maintained properly and parking charge to be collected as per agreement with the hospital.

Access Control Systems

Possessed Object Access Systems

A possessed object access system is a control system that uses certain physical objects in your possession for identity. Examples of these objects include USB security keys, smart cards, magnetic cards and USB flash drives. The access control systems are put in place to prevent unauthorized persons from gaining access to a specific area or privileged information. The execution of restrictions and limitations on private property ensures safety. Several access control systems are in place and each has its benefits and drawbacks.

- The advantage is that apart from protecting against unauthorized access, some objects can store additional security credentials. They are also portable.
- The disadvantages are that you can easily lose the object and it can be used by an unauthorized person if he gets hold of it.

Biometric Access Systems

The use of unique physical characteristics to identify individuals is called biometrics. Examples of these unique characteristics include the fingerprint, iris, voice and hand geometry. Biometric systems perform both identification and authorization using these unique characteristics. It is employed where high security is required, such as prisons, businesses, law enforcement agencies, hospitals and in the military.

- The advantages of this system is that it is very accurate because the odds of two people having similar characteristics are very minimal, it is very fast as it captures your details in seconds, it cannot be lost or stolen or forgotten and it is very efficient.
- The main disadvantage is that the hardware and software required are very expensive.

Two-factor Authentication Systems

This system involves the use of two access control systems. For instance, you can use a combination of privileged information, like a password, and a biometric system. This method is very well established in commercial firms since it comes with a high level of security and has an extra level of complexity

- Hackers are less likely to get information on two different types of required factors.
- The main disadvantage is that it requires both the purchase and integration of separate authentication systems, and the deployment of a physical authenticator component to every system user.

Advantages

1) Electronic Keys are difficult to duplicate

While physical keys can be copied very easily, duplicating electronic keys requires a much higher degree of sophistication.

This makes your access system much more secure than it could ever be with physical keys.

2) You never have to change the locks

An electronic user database means that you never have to change locks at your sites. If a keycard is ever lost, it can be immediately removed from the database and a new one can be issued. If an employee leaves your company, his or her access rights can be deleted within seconds. This greatly lowers your overall exposure to risk.

3) You only have to remember one key

With electronic access, your single key or access code grants you access to every door you need to access, so there’s no chance of forgetting the key for a particular door. If you get to a site where you need access and you are not recognized by the system, a network operator can add you or your supervisor to the list instantly.

4) Electronic keys reduce Windshield and Repair Time

If a tech needs additional access to handle an emergency in the field, his or her rights can be updated immediately. This way, the tech can travel straight to the emergency without returning to the office, reducing costly windshield time and accelerating repairs.

5) Complete History Logging

With an electronic access system, every entry to your sites is logged for later review. This can be an invaluable tool when investigating vandalism or theft, or for tracking response times or technical activities internally.

6) Electronic Access Control is completely customizable for every user

Electronic access control gives you the ability to set user-level access rights all the way down to individual doors and times. This minimizes your exposure to risk by granting no more site access than is necessary.

7) Electronic locks permit remote “Buzz In”

If a tech or outside contractor needs access to a locked site, you can open that door remotely from your central terminal. This gives you an extra degree of flexibility while making sure that you know about entries into your sites.

8) You won’t waste time and pocket space with electronic access

With electronic access control, you’ll never have carry (or risk losing) a large ring of keys.

9) Electronic access systems can notify you of propped doors

If a tech or anyone else decides it’s a good idea to prop open a door at a secured site, you’ll receive a prompt notification.

CCTV Camera System

Advantages

1. Deters Crime

The presence of CCTV camera system for surveillance will reduce petty thefts and vandalism. Since the activities are being monitored, fewer nuisances are likely to be created.

2. Helps Maintain Records

The images and videos captured by a CCTV camera system are often recorded and stored into a database. These are helpful in maintaining records so that they can be easily retrieved later, when needed.

3. Protects Employees

This is particularly helpful in customer service centers. The employees providing customer service may sometimes be subjected to verbal abuse or physical attacks. CCTV camera system helps to identify such instances and act immediately. It is also helpful to keep a tab on the activities of the employees.

4. Evidence in Lawsuits

In legal cases of thefts and other forms of crime, videos and images provided by the CCTV camera system can serve as a valid proof and evidence against the defaulter. This assists in making legal claims as well.

CCTV Camera System

Disadvantages

1. Do Not Work Always

CCTV camera system cannot monitor every area of your office or home at all times. Hence it cannot be considered as a foolproof method for crime prevention.

2. Privacy Concerns

Invasion of privacy is the major issue when it comes to any security system device like the CCTV camera system. It lowers the employee morale and hampers productivity at times. Constant monitoring of every activity might put the workers ill at ease.

3. Initial Costs

The initial costs incurred per camera are high. The installation may also increase the initial expenditure. It depends upon the complexity of the CCTV camera system as well.

RFID Technology

Lee and Shim (2007) identify the following perceived benefits associated with the use of the RFID in healthcare:

(i) overhead cost reduction;

(ii) reduced error rates;

(iii) improved customer service; and

(iv) Improved hospital image.

Ability to trace high value assets in the hospital and the ability to track assets over time. The RFID could be used in patients who are put "on hold," such as those with head injuries or drug overdoses. If these patients try to leave the hospital, a sensor will detect their movement and trigger an alarm. The other costly option was a full-time security guard

This system presents also a high, rigorous and simultaneous capacity of reading (So and Liu, 2006) in aggressive environments such as fire, ice, ink, noise and different temperatures (Knill, 2002).

Inventory Management:

- Efficient management of distribution and warehouse, store space.
- To identify products that may have been recalled, to respond rapidly to unforeseen changes in the supply chain, to react quickly to problems within the supply chain, to check on expiry dates and to determine when products will arrive in store.
- Reduction in the number of incorrect manual counts, unreported stock loss, mislabelling and inaccessible/misplaced inventory.

Advantages of RFID

(i) Patient flow management;

(ii) Improve productivity;

(iii) Reduce human errors;

(iv) Reliable accurate and secure measures for tracking and authentication of pharmaceuticals (Reynes, 2007);

(v) A triage system which employs facing massive casualty incidents through the news every RFID tags, which are silicon chips with IDs, radio frequency day. We also position it as a start point for new horizons in function and some additional logic and memory (Want *et al*., 1999, Hewkin, 2004)

(vi) Speed of data access and multiple item identification without need to have the tags on the line of sight;

(vii) Safety of electronic matches, item identification and data transfer;

(viii) Automation of some process activities and information flows;

(ix) Chance to implement workflow management rules, bounding health workers to follow the implemented procedures;

(x) Remote item / people tracking and real time process monitoring (Sini *et al*, 2008)

Disadvantages of RFID

i. High implementation and operation costs, the lack of standardization, and unawareness of its importance.

ii. Complexity of this technology

iii. ROI uncertainty.

iv. High cost of individual tags

Review of literature

Schneider electric (2008)[3] made an attempt to discover that by applying best practices there are many technologies that can aid a well-trained healthcare security staff in preventing crime and managing security incidents. The key systems of security are intrusion detection, access control, emergency communications, and video surveillance. If each of these systems is purchased separately, administration and training can burden a company or property owner. Intrusion alarms occur on one system, access badges are administered in a stand-alone database, and intelligent digital video technology runs on dedicated computer equipment. Each system requires service, maintenance, administration, and training.

By integrating these separate security systems under a flexible building automation system (BAS), hospital executives realize a lower upfront investment for a considerably more powerful security solution. Installation and training occur on a single system. Operational costs like administration and maintenance are also reduced. A single system enables greater flexibility to add security components that can be easily integrated into the overall system, keeping the cost of capital expenditures low, and requiring little additional training.

These three systems ***intrusion detection, access control and visitor management system, and video surveillance*** in the hands of competent and capable security staff, apply technology effectively to reduce crime and protect people and property. We will examine each system individually, and then in combinations to demonstrate how integrating security into the building automation system leverages these systems in multiple ways, increasing security and reducing operating and training costs.

Finally, this paper will show several examples like **University of Chicago Hospitals and Moffitt Cancer Center** where Schneider Electric has effectively applied building automation products and related services to provide effective integrated security for its customers.

A study conducted by **Justice Department of USA** in 2008 reveals that hospital emergency departments across the country treat more than 1.3 million people a year for injuries caused by violent attacks, which can escalate and continue within the hospital itself after the initial incident. According to Bureau of Labor Statistics data for 1993, workers in the health care field experienced the highest incidence of assault injuries. One study found that 82 percent of nurses surveyed had been assaulted on the job, 56 percent had been assaulted in the year prior to the survey, and many assaults go unreported. The same study shows that the greatest number of assaults (25%) occurred in emergency departments. In these situations discussed above planning of appropriate security services become very important.

Author **Jeff Aldridge**[4] (a healthcare security consultant) and others from Security Assessments International discussed the changing needs of security in hospital settings, and will be addressing new technologies, procedural changes and new issues affecting today's healthcare facilities. A hospital's *security management program* should be designed to teach, implement, monitor, assess, and improve components that are part of the hospital's existing program. Security is a system concept which requires on-going training, corroboration, monitoring, and swift attention to problem identification.

He further said that Physical protection may include but is not limited to:

- CCTV
- Time delay lock & alarm system
- Panic Alarms
- Special Locks
- Protective Barriers
- Security Presences
- Dedicated Security Patrols

Unique policies include, but may not be limited to: access control, visitation, identification procedures, information security, and patient privacy.

Sensitive areas should identified with a Risk Value Rating 1-5, where:

1. No Risk or not applicable
2. Minimal Risk
3. Moderate Risk of Injury / theft
4. Significant Risk without history of injury / theft
5. Significant Risk with history of injury / theft

The hospital security assessment should evaluate a facility beginning in the parking lot and continue all the way to the roof. Some of the components that should be considered are:

- Geographical Location (Inter-City, Suburb, Rural)
- Physical Design and layout of campus and surrounding property
- Number of uncontrolled access points into and out of the Facility
- Criminal Demographics surrounding the hospital and campus
- Security Incident data within the hospital as well as incidents on campus
- Level of physical security protection.
- Previous Security Sentinel Events
- Quality of the Security Department and Security Management Program
- Employee Security Awareness associated with on-going educational programs
- Administration and Management Support
- Patient, Staff, Employee, vendor, and visitor identification
- Emergency Department Security
- Violence in the Workplace issues, (Clinical and other locations)
- Birthing Center Security
- Pediatric Security
- Pharmacy
- Employee Education
- Patient Education

An article ***''New Generation of Access Control''*** published by **ISIO – International Security Industry Organization**[5] discusses that Asset tracking and monitoring is now a function of Access Control for people for example visitors, staff, temporary workers and assets such as deliveries or equipment are tagged on arrival at the reception desk of the particular site. Systems also now integrate with other departments such as accounting, stores, customer care and departments besides the security department.

The tags are zoned for access to specific areas. The route then is tracked under the antenna umbrella range. The system can connect to the Internet and therefore the Safety and Security Manager is able to interact via a 3G Tablet, Laptop or PC. This enables the highest form of efficiency by managing staff in concert during an event in play or locating assets. Managers can therefore be informed if persons or assets are entering an authorized or unauthorized zone. Access to an unauthorized zone is possible with an authorized escort.

Staff can be informed by SMS or E-mail if breach of the system has taken place, if an object is being moved which has been secured by a motion detector, or is being tampered with or persons being in restricted areas.

This provides for a 'pro active defense' position for the Security manager, as the trail can be followed of persons or assets entering a site which could lead to a search of the route taken if necessary.

In a case study of Matrix Security systems[6] - ***Providence Hospitals*** faced with an expensive security upgrade, chose to scrap its old system in favor of state-of-the-art technology that tied together its two hospital campuses, increased access control usability, and saved tens of thousands of dollars in the integration and installation costs. "There was little accountability, security officers continually struggled with the system's software usability, adding doors was expensive and upgrade costs paralleled those of a new cutting-edge system.

Therefore, the Providence security upgrade selection team chose the open-architecture system, Frontier™ Universe from Matrix Systems, Miamisburg, Ohio, which has developed a value-added reseller (VAR) network to perform its systems integration, staff training and localized 24/7 customer support services. The system offers the flexibility of both web browser and server-based operation. Its open architecture platform allows the integration of cost-saving wireless components, biometric readers, time and attendance equipment and high technology additions when the facilities expand.

The new system accommodates a variety of functions from one unified employee ID badge versus the multiple cards employees needed because of the previous system's fragmentation. So it was easier to authorize an employee for a new area by making a new card versus the more efficient method of just adding a new authorization level to the existing card. In the future, Providence would like to add more biometric fingerprint readers with anti-microbial features in four operating room entries, which will help minimize microbial infiltration because staff members won't need to handle badges.

In another case study of Matrix Security systems[7] - PHS (Promedica Hospital security) also uses cutting edge technology to cut security costs without sacrificing functionality. For example, the Matrix Systems Gateway—an IP-centric device that substitutes for more expensive full-fledged systems of security personnel, database servers, building controllers and workstations—is used at remote facilities, such as clinics, doctor offices and other locations that have a minimum amount of doors to control. These facilities still have full monitoring with CCTV and DVR's, plus physical door strike/lock capabilities all handled from a PHS central security office via the hospital's network.

Fred Miehl in the paper "*Hospital security strategies"* discusses that from the front door to the loading dock, healthcare security measures should be visible and abundant.

For the hospital security practitioner Visitor control in this type of environment is one of their most difficult tasks. As part of controlling patient visitors, some hospitals have implemented a visitor management system which enables security officials to track who is in the building and ensures visitors are only allowed access to certain areas of the hospital. Hospital security staff and/or volunteers can scan the visitor's driver's license[6]. The visitor's information is automatically entered into a database and a visitor pass is printed on a label, which is then worn by the visitor for the duration of their visit. The system can also be integrated onto the hospital's network for continual update with the patient data system to verify that the patient is registered.

Proximity cards are read rapidly and easily by simply presenting the cards within a prescribed distance to the reader. Magnetic stripe cards require the motion of "swiping" or insertion, which at times necessitates several attempts for a valid read. In vital applications such as in a hospital - where time to access an area could involve a life-and-death situation - the proximity readers certainly provide the superior functionality.

For hospitals contemplating a switch to proximity, dual-technology cards (magnetic stripe and proximity) would provide a solution during the transition period to support the older technology while moving to the more reliable, higher functionality.

The application of video cameras in most healthcare facilities is used primarily as an investigative tool to assist in the review of an incident that has occurred. Video cameras provide additional and remote "eyes" that enable minimal security staff to observe multiple remote locations, either in real-time or recorded for future review. They are also an overt reminder that a security system is present. Where possible, camera views should be associated with alarm conditions to assist in alarm assessment. For instance, upon an alarm condition on the infant monitoring system, associated camera views can automatically be displayed at the pediatric ward nurse's station, the lobby security post and the hospital's security response center.

Many hospitals are contemplating and switching to a smart card to create a one-card solution. Using both contact and contactless smart chip technologies, a single credential can handle a bar code for inventory control, a photo of the employee for identification, a dollar value for use in the cafeteria, a biometric template for data protection in the IT department, and proximity technology for access control.

Rationale of study

Hospital security department and staff are especially challenged to provide safe environment for employees, patients and visitors. Hospitals, by their nature, are designed to be open and accessible to the public, which means street crime and other dangers can easily enter through hospital doors if not properly protected.

Medical equipments, supplies, and controlled substances can be targets of theft; large, urban hospitals often serve as many as 1,000 visitors in a single day, in addition to hundreds of patients. The dichotomy of a hospital is such that it should have restricted entry yet open to all. Keeping all these aspects in consideration, a defined and well equipped security plan for hospital is need of the hour.

Since security, access control and video surveillance are not revenue generating areas in hospital therefore a cost effective planning is essential. Here arises the need for comparing outsource system and in-house system while planning of security.

Objectives

General Objective

To plan Security, Video Surveillance and Access Control services in a new tertiary care hospital.

Specific Objectives

1. To identify the Critical Areas in hospital and accordingly plan security manpower, video surveillance and access control system for them.

2. To compare in house and outsourced system for security (manpower and equipments), video surveillance and access control system

3. To integrate and analyze security, video surveillance and access control system and propose a solution based on cost comparison for security services.

Methodology

Study Design: Cross-sectional Descriptive Study

Study Area: Jaypee Medical Centre, Noida

Study Duration: 3 months (February to April)

Data collection:

Primary data : Focus Group discussion

Secondary data: literature review related to hospital security, Past security plan of the hospital

Study tools – Observation, SOP's, Records, checklists.

Data Collection

FLOOR WISE DEPARTMENTAL PLANNING

Sl. No.	FLOOR	DEPARTMENTS
1	Seventh	Wards
2	Sixth	Wards
3	Fifth	Wards
4	Service	IT Server, AHU, PTS station and MEP
5	Fourth	OT Complex, ICCU, Cath lab.
6	Third	Economy Bed, IVF, MICU, SICU, NICU, LDR
7	Second	Chemotherapy, Cosmetology, Endoscopy, Physiotherapy, Paediatric, Office.
8	First	Behavioural science, Ortho. , Neuro. , Gen. Surgery/MAS, Pulmonology, Opthal. , Dental, ENT, Diabetes Cardiac.
9	Ground	Executive Health Check up, Dialysis, Radiology, Day care, Emergency and Trauma, Pharmacy.
10	Upper basement	Blood Bank, Pathology Laboratory, Nuclear medicine, Kitchen, Administration.
11	Lower basement	Bio-medical Eng., Radiation Oncology, Laundry, Mortuary, CSSD.

Identification of Critical Areas

First of all we will identify Common Critical Areas on each floor inside the hospital related to Security (Manpower and required equipments), Video Surveillance and Access Control services.

Table no. 1 – Critical Areas

S.No.	Critical Areas Identified	Security	Video Surveillance	Access Control
1	Lift Lobby	✓	✓	✓
2	Stair case	✗	✓	✓
3	Hub Room	✗	✗	✓
4	Stores	✓	✓	✓
5	Rooms	✓	✓	✓
6	Corridors	✗	✓	✗
7	Parking	✓	✓	✗

After Discussion with security officials it was found that there are few critical areas in a hospital which need security personnel or video camera or access control system. The above table shows a list of critical area and requirement of these areas in term of security, video surveillance and access control.

After identification of the critical areas on each floor of the hospital, planning of security manpower was done and technicalities associated like video cameras, access points were located.

Planning Of Security Manpower and Equipments

A) In - House

On the basis of critical areas identified a detailed floor wise manpower planning was done. Few points were kept in mind while doing manpower planning

1. **Designations and Pay Structure**

Table No. 2 – Designations and Pay Structure

S.No.	Designation	Pay Structure / month	Qualification
1	Chief Security Officer	50000	Experienced
2	Senior Security Officer	35000	Experienced
3	Security Officer	25000	Ex - serviceman

4	Supervisor	15000	Ex - serviceman
5	Gunman	15000	License Holder
6	Guard (Male / Female)	10000	10th pass

Table no 2 shows designations with their respective salaries and educational qualification. Salaries of officials are according to minimum wages act of UP.

2. **No. of shifts (12 Hours shift)**
   i. Morning
   ii. Night

3. **Leave Reserve / Buffer (30%)**
   Leave reserve was taken as 30% of manpower (supervisor and guards).

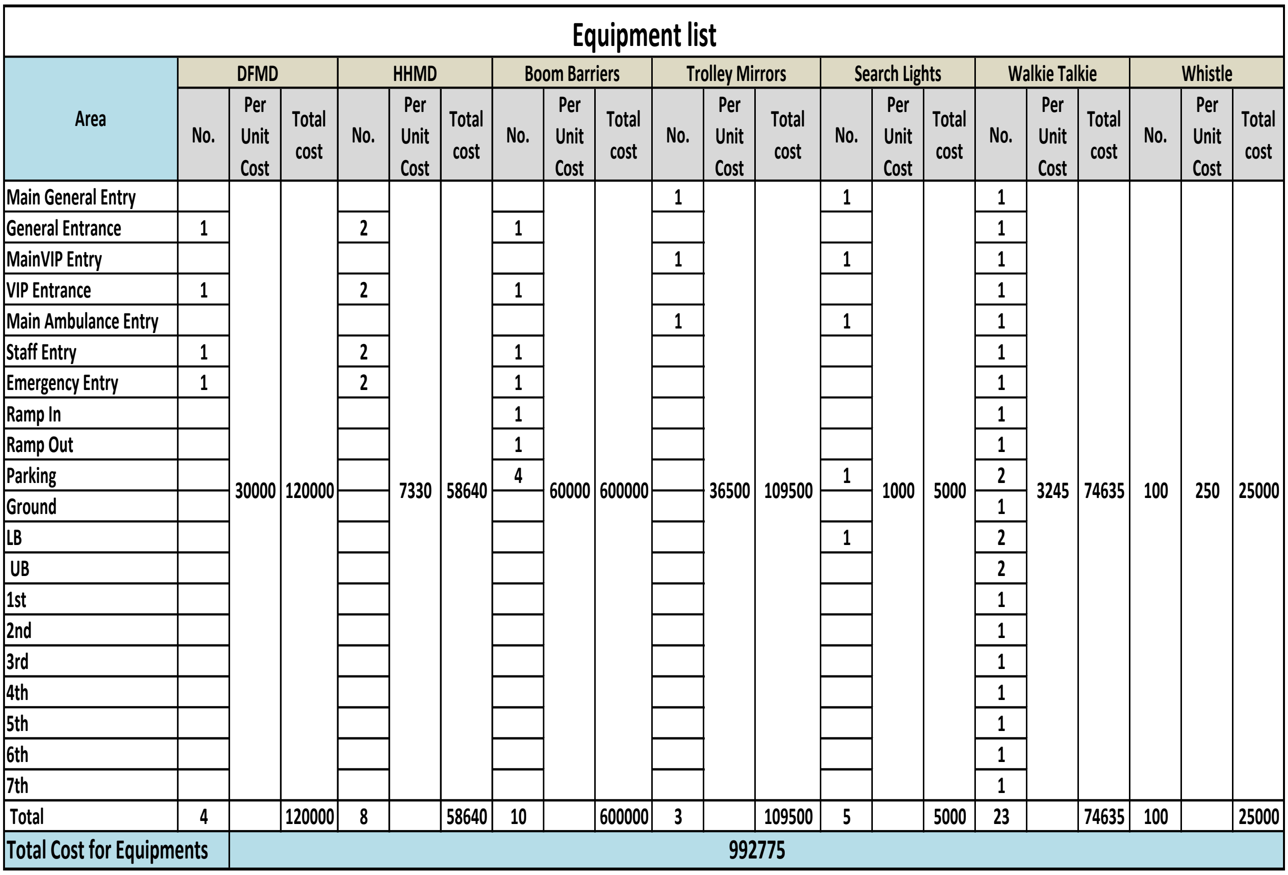
4. **Contingency plans (QRT – Quick Response Team)**
   Quick Response Team reaches the security spot at the call time with the quest for problem solving. It is composed of officer and security personnel mainly from retired Army person in vehicle, it is 24 hours operational.
   It comprises *Security Officer, Gunman & Security Guard*.

The floor wise detail of Manpower planning is placed in Annexure

Along with manpower planning Equipment Planning was also done. Following types of equipment were required:

- DMFD (Door Frame Metal Detector)
- HHMD (Hand Frame Metal Detector)
- Boom Barrier
- Walkie Talkie
- Trolley Mirror
- Search Lights
- Whistle

Table No. 3 – Equipment List



Equipment list

Area	DFMD			HHMD			Boom Barriers			Trolley Mirrors			Search Lights			Walkie Talkie			Whistle		
	No.	Per Unit Cost	Total cost	No.	Per Unit Cost	Total cost	No.	Per Unit Cost	Total cost	No.	Per Unit Cost	Total cost	No.	Per Unit Cost	Total cost	No.	Per Unit Cost	Total cost	No.	Per Unit Cost	Total cost
Main General Entry		30000	120000		7330	58640		60000	600000	1	36500	109500	1	1000	5000	1	3245	74635	100	250	25000
General Entrance	1			2			1									1					
MainVIP Entry										1			1			1					
VIP Entrance	1			2			1									1					
Main Ambulance Entry										1			1			1					
Staff Entry	1			2			1									1					
Emergency Entry	1			2			1									1					
Ramp In							1									1					
Ramp Out							1									1					
Parking							4						1			2					
Ground																1					
LB													1			2					
UB																2					
1st																1					
2nd																1					
3rd																1					
4th																1					
5th																1					
6th																1					
7th																1					
Total	4		120000	8		58640	10		600000	3		109500	5		5000	23		74635	100		25000
Total Cost for Equipments	992775																				

Above table shows total cost of the equipments which is INR 9,92,775. A round off figure of INR 10,00,000 has been taken.

Now after planning total manpower, equipments required along with their cost we will derive total cost of the in-house security services.

Table No. 4 – Man power plan (In house)

Security Manpower (In house)							
Floors	**Security**						
	Personnel						**Total Cost**
	CSO	**SSO**	**SO**	**Gunman**	**Supervisor**	**Guard**	
Lower	0	0	0	0	4	10	1,60,000
Upper	0	0	0	0	0	4	40,000
Ground	1	1	2	0	4	30	4,95,000
QRT	0	0	0	2	1	2	65,000
First	0	0	0	0	0	2	20,000
Second	0	0	0	0	0	4	40,000
Third	0	0	0	0	0	2	20,000
Fourth	0	0	0	0	0	4	40,000
Fifth	0	0	0	0	0	2	20,000
Sixth	0	0	0	0	0	2	20,000
Seventh	0	0	0	0	0	4	40,000
Service	0	0	0	0	0	2	20,000
Buffer (30%)				1	3	20	2,60,000
Total	**1**	**1**	**2**	**3**	**12**	**88**	12,40,000
Total Salary For 5 years							7,44,00,000
Equipments							11,50,000
Grand Total							7,55,50,000

Table No 4 shows total cost of In-house security planning which is INR 7,55,50,000. The break up of security personnel and their salaries is also shown in table. Cost of security equipments is also added in the table.

B) Outsource

In terms of number, planning of security manpower and equipments is same as of in-house but the difference lies in providing leave reserve (buffer), cost of equipments and pay structure of employees provided by outsourced agency.

Comparison of Different Vendors

After comparison of different vendors, on the basis of availability of trained manpower, cost of manpower and equipments, immediate back up facility and various other factors Vendor was decided for outsourcing security manpower and equipments.

Table No 5 – Vendor Comparison (Man power)

	Jaypee (Jupiter)			IRONMAN			SIS			G4S			Knightwatch			Securitas			PACER		
	Manpower	Cost per person	Total Cost	Manpower	Cost per person	Total Cost	Manpower	Cost per person	Total Cost	Manpower	Cost per person	Total Cost	Manpower	Cost per person	Total Cost	Manpower	Cost per person	Total Cost	Manpower	Cost per person	Total Cost
Security Guard	65	10093	656,020	65	10060	653,895	65	12309	800,088	65	14000	909975	65	9184	596947	65	11424	742552	65	9663	628107
Lady Guard	3	12164	36,491	3	7392	22,177	3	12309	36,927	3	14000	41999	3	9184	27551	3	12835	38505	3	9663	28990
Gunman	2	15475	30,949	2	12391	24,783	2	14130.8	28,262	2	20531	41063	2	12096	24192	2	15135	30269	2	12064	24127
Security Supervisor	9	15748	141,732	9	13603	122,423	9	15214	136,926	9	20237	182133	9	11478	103304	9	15135	136211	9	12064	108573
Security officer	2	20929	41,859	2	32327	64,655	2	19349.8	38,700	2	49236	98472	2	19028	38055	2	36454	72908	2	25822	51645
TOTAL	**907,051**			**887,934**			**1,040,902**			**1,273,641**			**790049**			**1,020,444**			**841441**		
Equipment charge/year	200000			215000			250000			205000			190000			200000			220000		
As per minimum wages act	yes			yes			SIS			yes			yes			yes			yes		
Immediate Back up				Got their own barrack at sec - 31, Noida						QRT present at Sec - 4, Noida			office at Noida			office at Noida			office at Noida		
Training				Yes			Yes			Yes			Yes			Yes			Yes		
Associated Hospital				G. M Modi Hospital, Jeevan Hospital, , Banarsidas Chandiwala Hospital, Puspawati Singhania Reasearch Institute, Tirath ram Hospital, Vimhans Hospital, Metro Heart Institute, Metro Khera Hospital (rlkc), Metro Anand Hospital Cancer Care Centre.			AIIMS, Safdarjung, Fortis			Pushpanjali Hospital, Shroff eye Hospital, OPDs of AIIMS, Yashoda Hospital,Kailash hospital,			Apollo Hospitals, Dharamshila Cancer Hospital, Al-Shifa Hospital.			Medanta - the Medicity, Wockhardt(Now Terminated), Artemis(Now terminated),					

NOTE: The above rates are calculated on 12 hrs shift basis. Service Tax will be charged extra.

Now after comparing vendors on all the points for security manpower and equipments **Knightwatch** was selected amongst all and according to their rates total cost was derived. The selection of this vendor was also influenced by the type of hospitals it was associated to.

Table No. 6 – Man power plan (Outsourced)

Security Manpower (outsourced)							
Floors	Security						
	Personnel						Total Cost
	CSO	SSO	SO	Gunman	Supervisor	Guard	
Lower	0	0	0	0	4	10	
Upper	0	0	0	0	0	4	
Ground	1	1	2	0	4	30	
QRT	0	0	0	2	1	2	
First	0	0	0	0	0	2	
Second	0	0	0	0	0	4	
Third	0	0	0	0	0	2	
Fourth	0	0	0	0	0	4	
Fifth	0	0	0	0	0	2	
Sixth	0	0	0	0	0	2	
Seventh	0	0	0	0	0	4	
Service	0	0	0	0	0	2	
Total	**0**	**0**	**2**	**2**	**9**	**68**	**7,90,049**
Total Salary For 5 years							**4,74,02,940**
Equipments (for 5 years)							**9,50,000**
Grand Total							**4,83,52,940**

Table No 6 shows total cost of Outsourced security planning which is INR 4,83,52,940.

Planning of Video Surveillance and Access Control

A) In House

On the basis of critical areas Video Surveillance and Access Control services were planned.

Table No. 7 - Video Surveillance and Access Control (In house)

In house					
Floors	**Video Surveillance**			**Access Control**	
	Camera		**Total Cost**	**Access Point**	**Total Cost**
	Box	**Dome**			
Lower	10	22	6,59,000	32	6,59,064
Upper	6	11	3,58,000	23	3,58,040
Ground	6	35	7,66,000	15	7,66,056
QRT	0	0	0	0	0
First	8	26	6,70,000	9	6,70,043
Second	3	32	6,29,500	11	6,29,546
Third	4	13	3,35,000	30	3,35,047
Fourth	6	19	4,94,000	28	4,94,053
Fifth	6	15	4,26,000	13	4,26,034
Sixth	6	17	4,60,000	12	4,60,035
Seventh	2	9	2,10,000	12	2,10,023
Service	0	19	3,23,000	4	38,000
Buffer	0	0	0	0	0
Total	**57**	**218**	**53,30,500**	**189**	**50,45,941**
Preventive Maintenance (5 years)			**7,99,575**		**7,56,892**
Miscellaneous			**13,50,000**		**13,50,000**
Grand total for five years			**1,46,32,907**		

As the above table shows there are two type of camera used – Box and Dome with different ranges at different places according to their use. Box camera has higher range than dome camera.

Video Surveillance

Costing of both the camera is divided into four heads:

- **Camera Cost**
- **Installation Cost**
- **Cable Cost** – 300 m available for Rs 6000

  70 m = 6000*70/300 (70 m for 1 camera)

  = **Rs 1400**
- **Server Cost -** 1 server cost is 1,50,000

  For 280 cameras – 150000/280 = **Rs 540**

Table No. 8 – Cost of Camera

S.No.	**Type of Cost**	**Box Camera**	**Dome Camera**
1	Camera Cost	25137	13860
2	Cable Cost	1400	1400
3	Installation Cost	1000	1000
4	Server Cost	540	540
	Total	**28,077**	**16,800**

Box camera – INR 28500 (Total + Buffer)

Dome camera – INR 17000 (Total + Buffer)

Preventive Maintenance – 3% of total cost per year = **5330500 * 0.03 *5**

= 7,99,575

Miscellaneous cost includes Salary of 1 service engineer and 1 electrician

Table No 9. - Salary of Service engineer and Electrician

S.No.	Designation	Salary / Month	Salary for 5 year (salary/month*12*5)
1	Service Engineer	30,000	18,00,000
2	Electrician	15,000	9,00,000
	Total	**45,000**	**27,00,000**

The Service Engineer and Electrician will be responsible for both, video surveillance and access control system.

Access Control System

Planning and Costing of Access Points is divided into 3 heads:

- Gateway
- Reader Module
- Output Module
- Server

Gateways

- The Cisco Physical Access Gateway is an integral component of the Cisco Physical Access Control solution, and is the primary module used to connect door hardware (readers, locks, etc.) to the IP network. The gateway can connect to a maximum of two doors and associated inputs and outputs.
- The Cisco Physical Access Gateway is a mandatory component of any access control deployment. The following optional modules may be connected to the Cisco Physical Access Gateway to control additional doors, inputs, and outputs:
  - ➢ Cisco Physical Access Gateway Reader Module
  - ➢ Cisco Physical Access Gateway Input Module
  - ➢ Cisco Physical Access Gateway Output Module

Reader Module

- The Cisco Physical Access Reader Module is an optional component of the Cisco Physical Access Control solution. The module can be connected to a Cisco Physical Access Gateway in order to expand the solution to include additional doors.
- The Cisco Physical Access Reader Module can connect to a maximum of two doors and associated inputs and outputs. It must be used in conjunction with the Cisco Physical Access Gateway, and cannot be used standalone.

Output module

- The Cisco Physical Access Output Module is an optional module that can be connected to the Cisco Physical Access Gateway to expand the solution to include additional outputs.
- The Cisco Physical Access Output Module can connect up to 8 outputs, each of which can be configured as Normally Open (NO) or Normally Closed (NC). The module must be used in conjunction with a Cisco Physical Access Gateway, and cannot be used standalone.

Cost of 1 access point includes:

Gateway – Includes 8 reader module (can include 15 also)

Reader module – For 2 doors

Output Module - For 2 doors

Cost of 1 Gateway = 10951 / 8 = **1370**

Cost of 1 Reader module = 5636 / 2 = **2818**

Cost of 1 Output Module = 5675 / 2 = **2838**

Server Cost = 3*150000 = 450000 (Cost of 3 severs)

= 450000 / total no of access points

= 450000 / 190

= **2370**

Total Cost of 1 Access Point = 1 Gateway + 1 Reader module + 1 Output Module + Server Cost

= **1370 + 2818 + 2838 + 2370**

= 9500 (approx)

B) Outsource

For outsourcing Access Control and Video Surveillance services comparison amongst different vendors and its analysis was done.

Table No 10 – Vendor Comparison (Access Control and Video Surveillance)

	Allied digital			**Siemens**			**IV Communication**		
	Video Surveillance	**Access control**	**Total**	**Video Surveillance**	**Access control**	**Total**	**Video Surveillance**	**Access control**	**Total**
Instrument cost	63,00,000	16,00,000	79,00,000	73,50,000	20,00,000	9350000	68,50,000	18,00,000	86,50,000
Installation	10,00,000		10,00,000	18,00,000		1800000	15,00,000		15,00,000
Training	8,00,000		8,00,000	0	0	0	10,00,000		10,00,000
Preventive maintenance	8,00,000	50,000	8,50,000	10,00,000	60,000	10,60,000	8,00,000	54,000	8,54,000
Total (INR)			**1,05,50,000**			**1,22,10,000**			**1,20,04,000**
Back Up	Yes			Yes			Yes		
Additional points	Have agreement with CISCO			No agreement			No agreement		
	Relatively new			Best in this sector					
	Will provide services for 5 years			Will provide services for 5 years			Will provide services for 5 years		
	Training charges included in contract			No charges for training			Training charges included in contract		

After the comparison and analysis amongst different vendors ***Allied Digital*** was selected for outsourcing Video Surveillance and Access Control. Apart from cost factor the selection of this vendor was also influenced by the contract which it possesses with Cisco Company.

Table No. 11 - Video Surveillance and Access Control (Out sourced)

Outsourced					
Floors	**Video Surveillance**			**Access Control**	
	Camera		**Total Cost**	**Access Point**	**Total Cost**
	Box	**Dome**			
Lower	10	22		32	
Upper	6	11		23	
Ground	6	35		15	
QRT	0	0		0	
First	8	26		9	
Second	3	32		11	
Third	4	13		30	
Fourth	6	19		28	
Fifth	6	15		13	
Sixth	6	17		12	
Seventh	2	9		12	
Service	0	19		4	
Buffer	0	0		0	
Grand Total	**57**	**218**		**189**	
Preventive Maintenance					
Misc					
Grand total for five years			**1,05,50,000**		

Table No. 11 shows the total cost of video surveillance and access control system when it is outsourced. This outsourcing means that allied digital will be responsible for all purchasing of equipments plus their preventive maintenance for 5 years.

Data Analysis

A. Manpower Requirement (In house V/S Outsource)

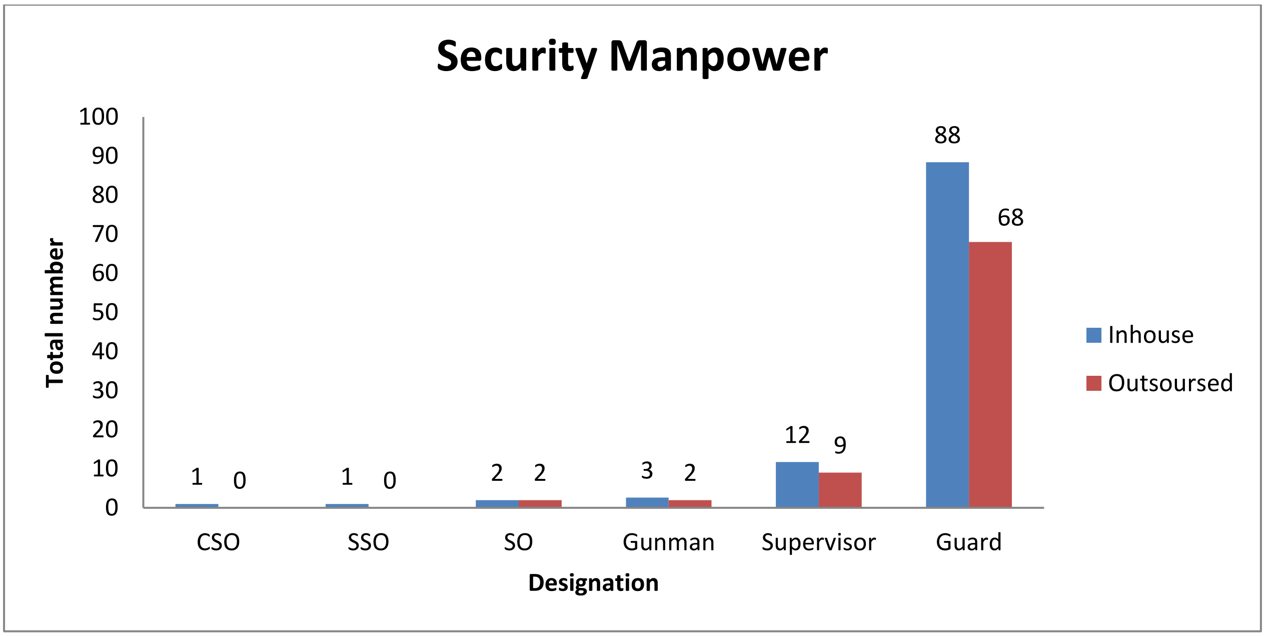


Chart 1 - Chart showing Manpower Requirement (In house V/S Outsource)

On analyzing we found that man power requirement is less when system is out sourced. This is because we do not have to take leave reserve when system is outsourced.

B. Total Cost of Manpower - Salary & Equipments (In house V/S Outsource)

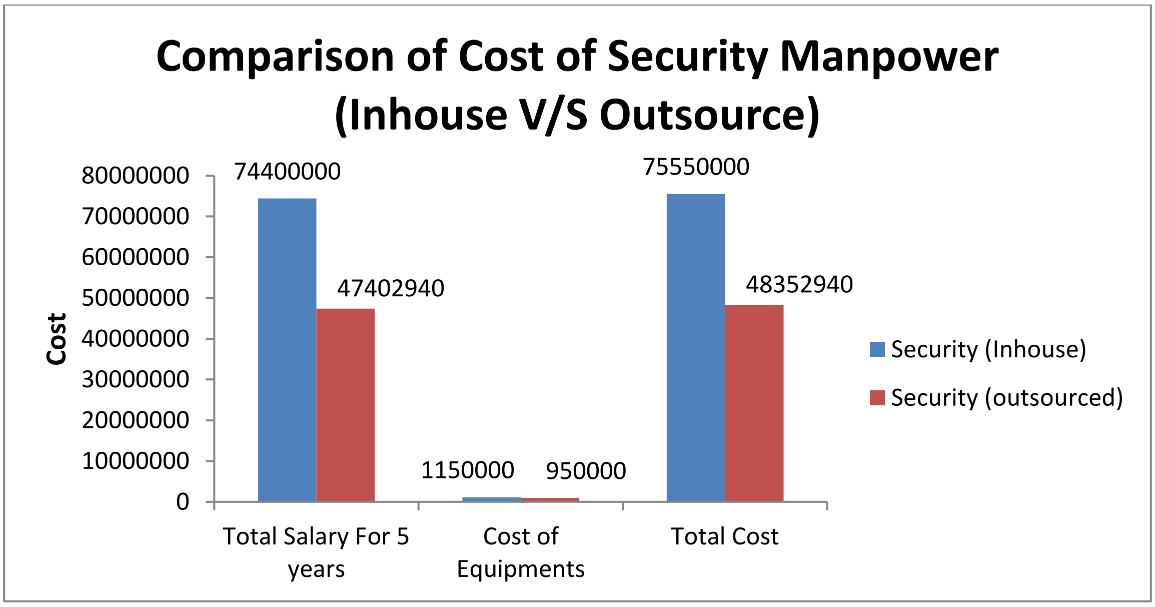


Chart 2 - Chart showing Total Cost of Manpower - Salary & Equipments (In house V/S Outsource)

Chart no 2 shows the cost comparison of security man power and security equipments when system is in house and when system is out sourced. We can see from the chart that when system is outsourced than cost bearing is less. But it is always advisable to have equipments in house.

C. Need of Camera and Access Control Points (Same for Outsource and In house)

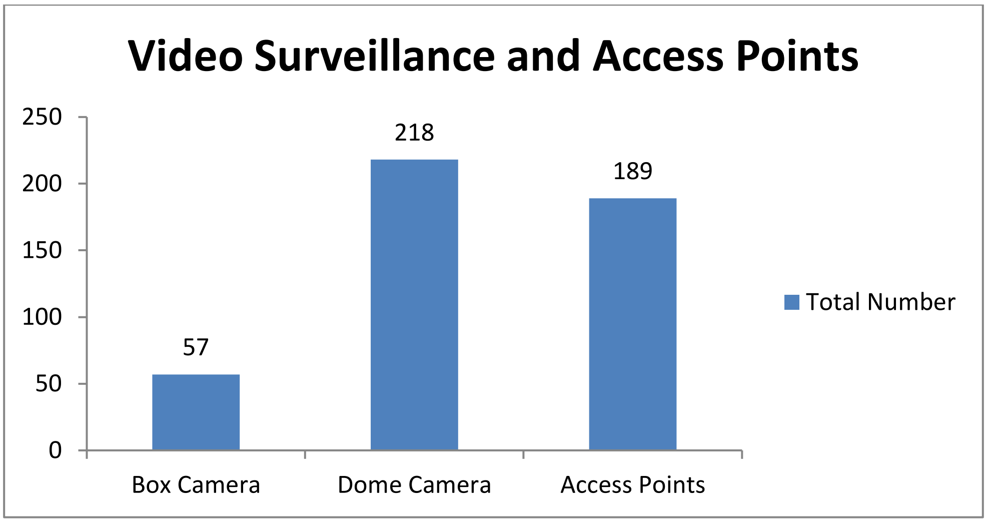


Chart 3 - Chart showing Need of Camera and Access Control Points

On analyzing the need we found out that 57 dome cameras, 218 box cameras and 189 access points are required for hospital building

D. Combined Cost of Video Surveillance and Access Control System (In house & Outsourced)

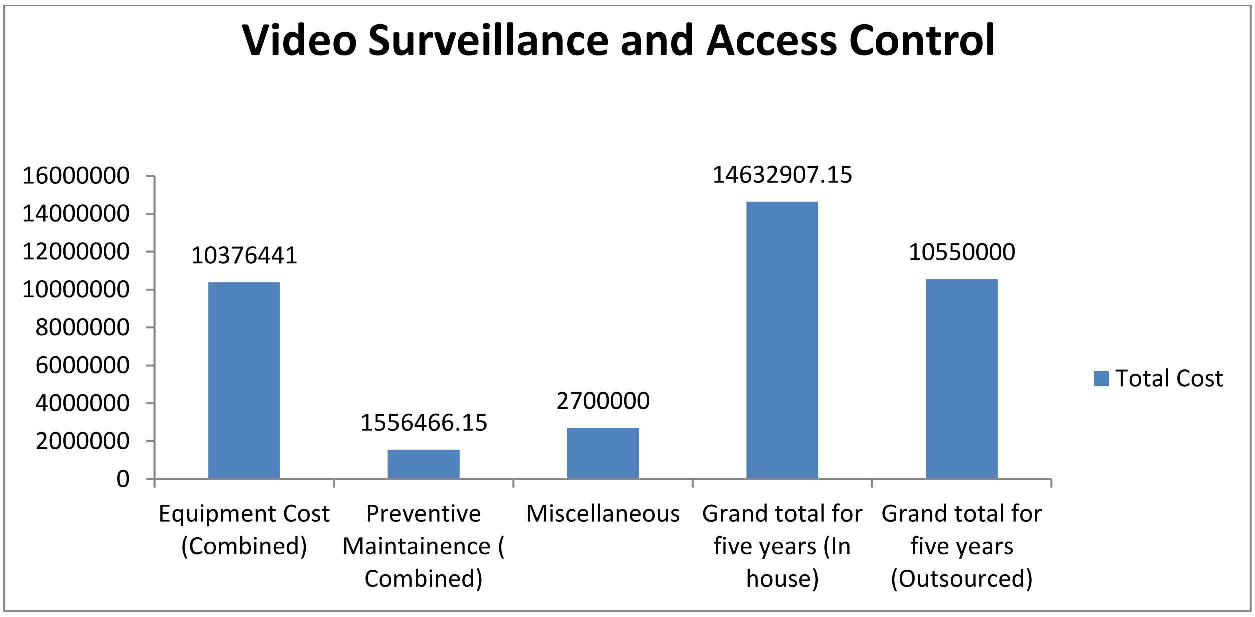


Chart 4 - Chart showing Combined Cost of Video Surveillance and Access Control System (In house & Outsourced)

From the chart no 4 we can analyze that cost incurred in outsourced is much less than in-house system. The major factor it that vendor is supplying equipment at cheaper rates than market. This is because vendor has a contract with Cisco Company which gives 10% off on Cisco equipments.

E. Combined Cost of Security, Video Surveillance and Access Control System (In house V/s Outsource)

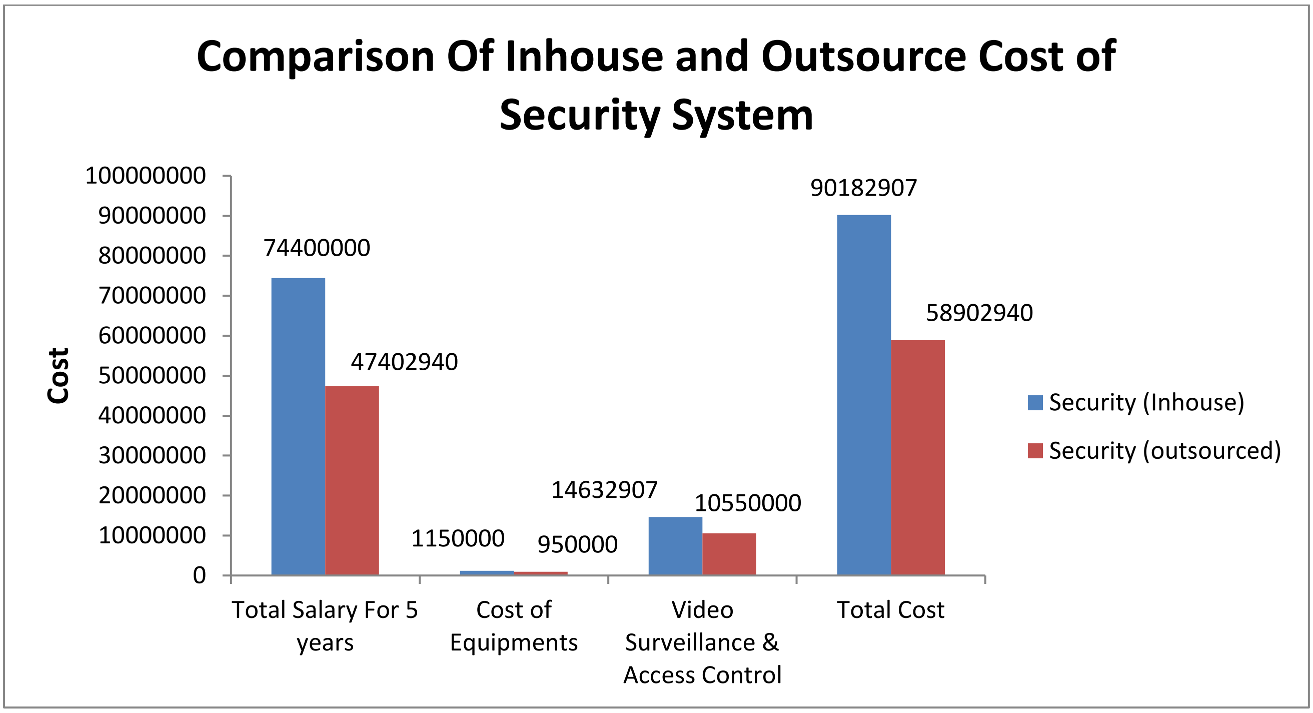


Chart 5 - Chart showing Combined Cost of Security, Video Surveillance and Access Control System (In house V/s Outsource)

The above chart shows comparison of cost when system is out sourced and when system is in house.

F. Different Combinations of Manpower, Equipments, Video Surveillance & Access Control System

Table No. 12 – Different Combinations of Manpower, Equipments, Video Surveillance & Access Control System

No.	Man power	Equipment	Video Surveillance & Access Control	Total Cost
1	**74400000**	**1150000**	**14632907**	**90182907**
2	**74400000**	**1150000**	**10550000**	**86100000**
3	**47402940**	**1150000**	**14632907**	**63185847**
4	**74400000**	**950000**	**14632907**	**89982907**
5	**47402940**	**950000**	**14632907**	**62985847**
6	**74400000**	**950000**	**10550000**	**85900000**
7	**47402940**	**1150000**	**10550000**	**59102940**
8	**47402940**	**950000**	**10550000**	**58902940**

- **Red** indicates – Outsourced
- **Blue** indicates – In house

Combination no 1. shows highest cost amongst all which is **INR 90182907** when all the services are In house. When services are in house than the responsibility of leave reserve, preventive maintenance and back up is of hospital.

Combination no 2. shows 3rd highest cost amongst all which is **INR 86100000** when two services (manpower and equipment) are in house and Video Surveillance and Access Control are Outsourced.

Combination no. 3 shows medium cost as compared with other combinations which is **INR 63185847** where only manpower is outsourced.

Combination no 4. shows 2nd higher cost which is **INR 89982907** when compared with other combinations where only equipments are outsourced.

Combination no 5. shows medium cost which is **INR 62985847** where both Manpower and equipments are outsourced.

Combination no. 6 shows high cost which is **INR 85900000** as manpower and equipments are inhouse.

Combination no. 7 shows low cost which is **INR 59102940** as manpower and Video Surveillance and Access control are outsourced.

Combination no. 8 shows lowest cost which is **INR 58902940** where all the services are outsourced.

In the combinations mentioned above **Combination No. 7** is best as Manpower, Video Surveillance and Access control which is main cost center over here is outsourced and equipments is in house which is very important. This relieves an organization from the headache of preventive maintenance and leave reserve.

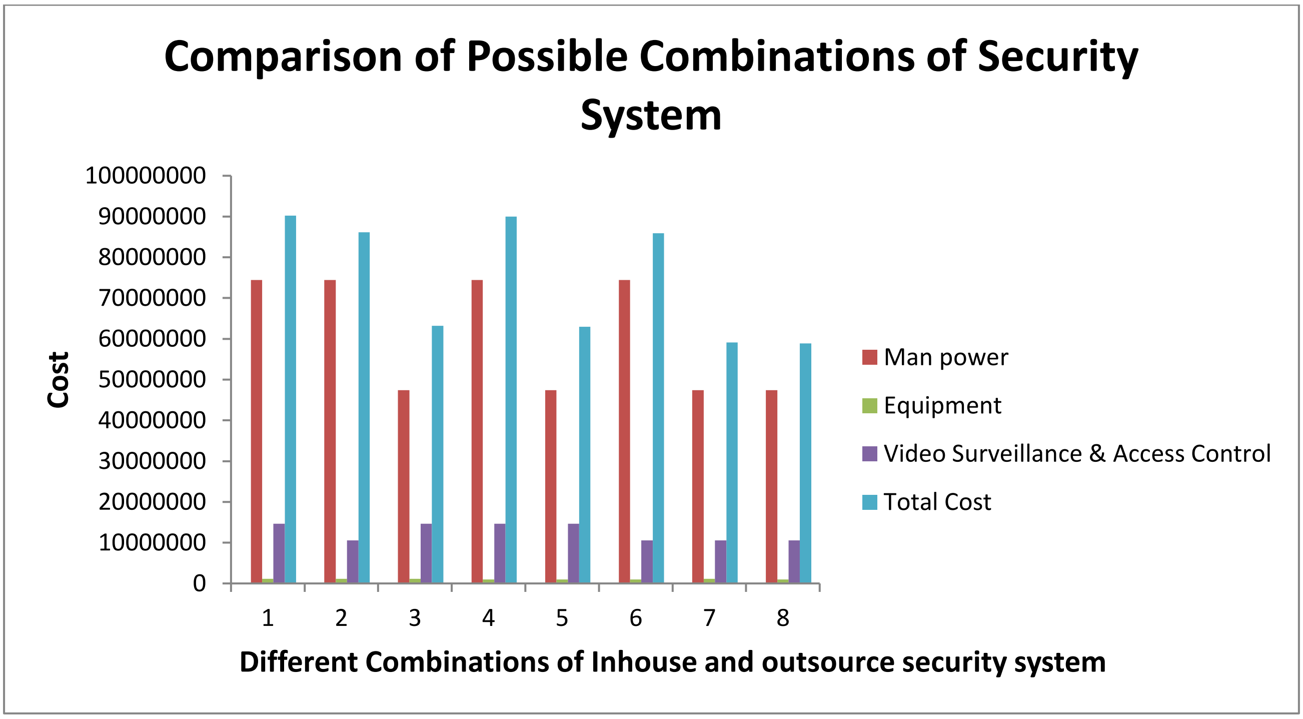


Chart 6 - Chart showing comparison of possible combinations of Security System

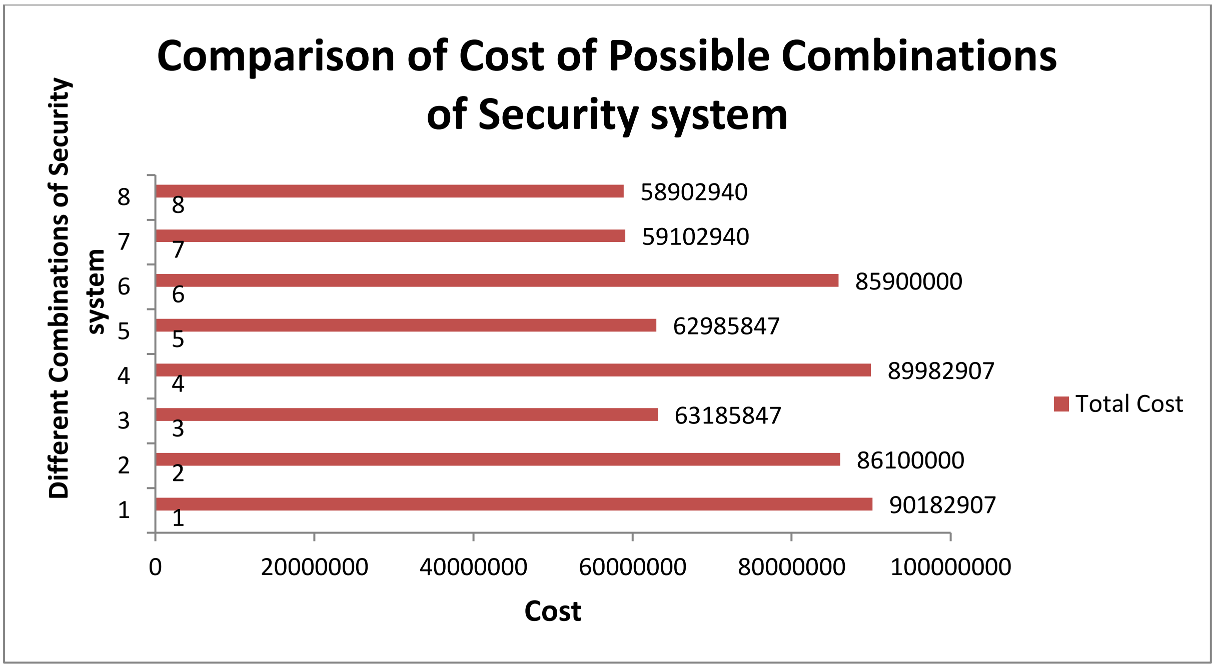


Chart 7 - Chart showing comparison of cost of possible combinations of Security System

Discussion

Constraints faced by the organization in its delivery of healthcare services are:

- Non availability of adequate skilled manpower
- Unionization of the labour manpower
- Staff absenteeism
- Inadequate monitoring and operational efficiencies
- Inadequate maintenance of related equipments leading to larger down time and fewer operational hours.

Purpose of Outsourcing

- Increased patient and staff satisfaction
- Facility up gradation leading to NABH / ISO accreditation
- Establish good reputation of healthcare facilities

Experience at private hospitals reveals that outsourcing these facilities to professional facilities management companies proves to be more economical in the long run. Since the services are provided based on the contract, the hospital has more authority and can decide on the terms & conditions and lay them out clearly based on the requirements of each property. This ensures consistent quality of services.

Fulfilling the needs of increasing patient population and ensuring that all the ancillary services are in good condition in the limited financial resources is a huge challenge. Offloading the facility / infrastructural maintenance to an external private agency and monitoring the services relieves their administrative burden and saves them considerable time & energy.

Improvement in care services requires mechanization, trained manpower, and better supervision by professionals; this necessitates capital investment in non-core areas. Outsourcing minimizes this cost of capital for the hospital and this can be used to enhance the clinical services. Proved efficacy, better cost management, avoidance of additional expenses, sharing and managing risks, overcoming red tape and negative attitudes are some of the other associated benefits

Key Issues with Outsourcing

The key issues in outsourcing of facility management services are:

1. Finding and choosing the right outsourcing agency
2. Cultural differences between the principal employer and outsourced agency
3. Lack of emotional attachment and accountability of the employee to the organization lead to poor quality of services
4. Sometimes maintaining discipline becomes challenging
5. Managing adherence to internal processes and protocols by people deployed in 'outsourced' positions becomes difficult
6. Dependency, lack of control, unpredictability, occasionally higher costs, lack of alignment with overall strategy and culture are few of the challenges comes with outsourcing

Table No. 13 Comparison In-house Vs Outsource

	In house	**Outsource**
Quality of services	Unable to scale up and match NABH standards	Strict adherence to ensure they match NABH standards
24X7 Availability of on-ground manpower	Not ensured	Ensured
Mechanization of service delivery	Low	High
24X7 Availability of supplies & consumables	Not ensured	Ensured
Down time of used machinery	High	Low
Need to train manpower	Required	Manpower with requisite skill sets will be deployed
Reliability	Availability of manpower not assured due to absenteeism and inadequate numbers	Availability of manpower in requisite strength assured
Administrative burden	High	Low

Operational control of hospital administration	Low	High
Patient and staff satisfaction	Low	High
Operational efficiencies and effectiveness	Low	High
Image of the hospital	Low	High

Taking in consideration all points the **Combination no 7** full fill major requirements. This combination is cost effective and will be very helpful staff and patient satisfaction. As major burden is on outsourcing agency the hospital staff can focus more on patient care services and upliftment of hospital.

Conclusion

Security department is not a revenue generating department but a cost centre for the hospital. Thus it becomes utmost important to do proper planning for it. Inadequate in-house staff provides ancillary services at a reduced cost; however, it results in poor quality of services due to constrained number of quality manpower. Outsourcing will bring in skilled personnel and expertise required to provide good services that will allow hospitals to focus on their core strengths. Hence, it is observed that the hospital will enjoy better services and facilities when the non-clinical services are outsourced to an efficient service provider.

But at the same time there are some issues with outsourcing like dependency, lack of control, unpredictability, occasionally higher costs, lack of alignment with overall strategy and culture which must be taken care of for proper functioning of hospital. So a proposal of integrated system of Outsourced Manpower , Video Surveillance and Access Control System and In house Equipments was given in order to have better accountability and efficiency in the system.

It is not correct to directly compare the cost of services and judge the best case for the hospital, better management of service results in cost savings in the fronts like better maintenance of the equipments and premises extends the performance life of the same which directly converts into visible savings Thus it is observed that the benefits of outsourcing bundled contract outweigh the costs it incurs and provides quantum leap in quality of service and efficiency of service.

.

Limitations

- Planning was mostly based on experiences and discussion made by security officials.
- Data of other hospitals were not compared in the study.
- All type of security equipments were not taken into account like RFID, Cones etc.
- Vendor selection was mainly dependent upon cost factor.
- Planning for extra team like intelligence team was not done.
- Back up was not prepared if contract with vendor is cancelled at any point of time.

References

1. http://www.jaypeehealthcare.com/ accessed on 2nd april 2013
2. Jeff Aldridge in an article *"Hospital Security: The Past, The Present, and The Future – Part 1 & 2"* addresses today's and tomorrow's needs from healthcare security available from http://www.saione.com/articles/HSPPF_Part1.pdf, page1,2 and http://www.saione.com/articles/HSPPF_Part2.pdf, page1,2
3. Schneider electric (2008) in paper ***"Hospital meet security challenges with integrated solutions"*** available from http://www.schneider-electric.us/documents/customers/healthcare/resource-library/hospitals-meet-security-challenges-wp.pdf accessed on 5th april 2013
4. Jeff Aldridge in an article *"Hospital Security: The Past, The Present, and The Future – Part 1 & 2"* addresses today's and tomorrow's needs from healthcare security available from http://www.saione.com/articles/HSPPF_Part1.pdf page1,2 and http://www.saione.com/articles/HSPPF_Part2.pdf page 1,2
5. **ISIO – International Security Industry Organization** (2005)***''New Generation of Access Control''* available on** http://www.intsi.org/access_control_latest.html accessed on 7th april 2013
6. Matrix Security System a case study on **"Providence Hospitals Security upgrade offers high tech functions that cut costs "** available from http://www.matrixsys.com/case-studies/providence-hospitals-case-study.html accessed on 7th april 2013
7. Matrix Security system a case study on **"Promedica health system a perview of 21st century Hospital security / Access control"** available on http://www.matrixsys.com/news/promedica-hospital-security.html accessed on 8th april 2013
8. Fred Miehl (03/08/2012) wrote an article titled, **"Hospital Security Strategies"** available from http://www.securityinfowatch.com/article/10523110/hospital-security-strategies. accessed on 8th april 2013