INTERNSHIP TRAINING

AT

DELL INTERNATIONAL SERVICES, BANGALORE

HIPAA KNOWLEDGE & AWARENESS IN AN EMR SUPPORT PROJECT

BY

SHIVANG SHARMA

PG/14/055

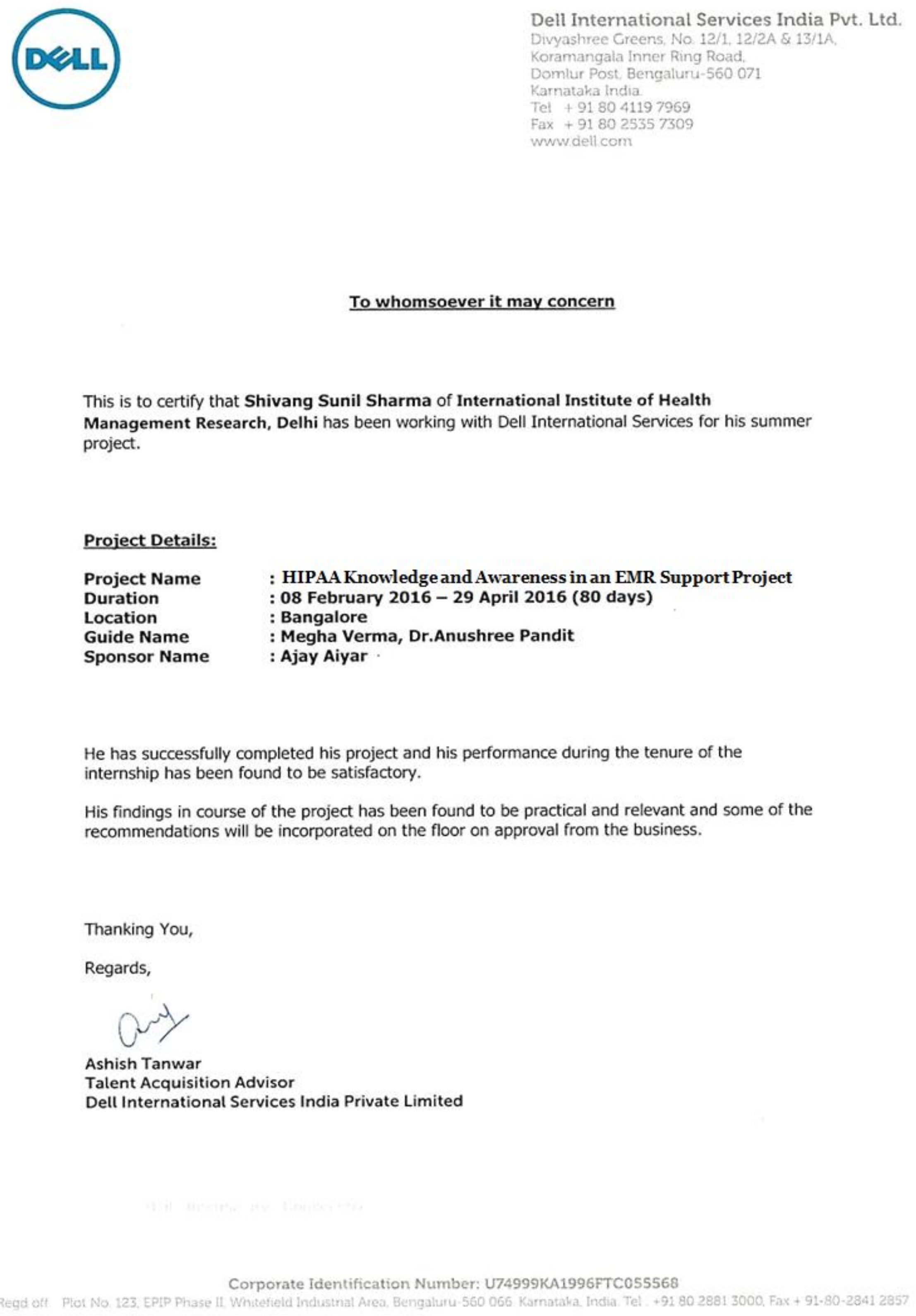
UNDER THE GUIDANCE OF

PROF.SURENDRA TYAGI

POST GRADUATE DIPLOMA IN HOSPITAL AND HEALTH MANAGEMENT

2014-16

INTERNATIONAL INSTITUTE OF HEALTH MANAGEMENT RESEARCH, NEW DELHI



Dell International Services India Pvt. Ltd.
Divyashree Greens, No. 12/1, 12/2A & 13/1A,
Koramangala Inner Ring Road,
Domlur Post, Bengaluru-560 071
Karnataka India.
Tel +91 80 4119 7969
Fax +91 80 2535 7309
www.dell.com

To whomsoever it may concern

This is to certify that **Shivang Sunil Sharma** of **International Institute of Health Management Research, Delhi** has been working with Dell International Services for his summer project.

Project Details:

Project Name	**: HIPAA Knowledge and Awareness in an EMR Support Project**
Duration	**: 08 February 2016 – 29 April 2016 (80 days)**
Location	**: Bangalore**
Guide Name	**: Megha Verma, Dr.Anushree Pandit**
Sponsor Name	**: Ajay Aiyar**

He has successfully completed his project and his performance during the tenure of the internship has been found to be satisfactory.

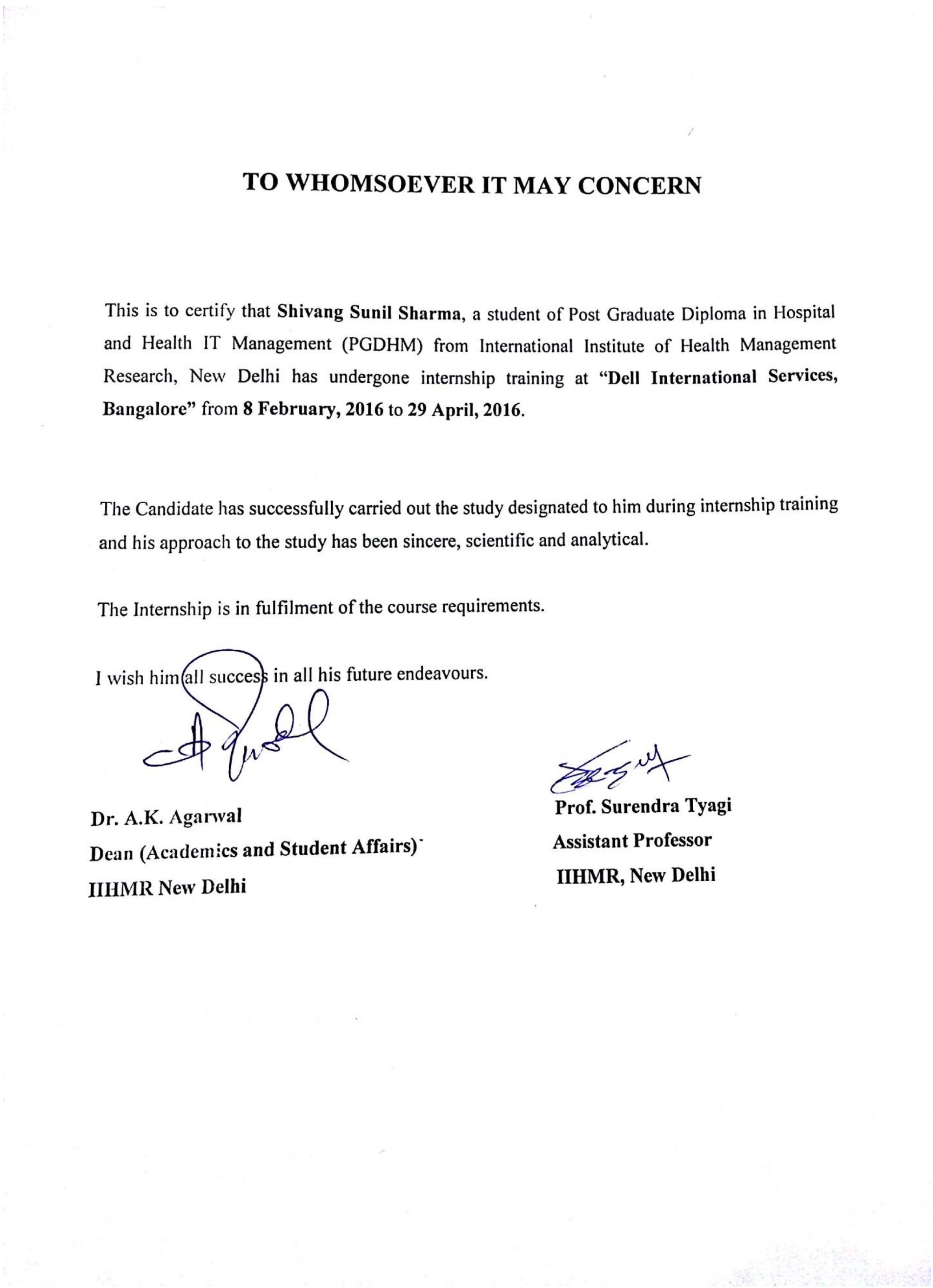
His findings in course of the project has been found to be practical and relevant and some of the recommendations will be incorporated on the floor on approval from the business.

Thanking You,

Regards,

Ashish Tanwar
Talent Acquisition Advisor
Dell International Services India Private Limited

Corporate Identification Number: U74999KA1996FTC055568
Regd off: Plot No. 123, EPIP Phase II, Whitefield Industrial Area, Bengaluru-560 066. Karnataka, India. Tel : +91 80 2881 3000, Fax + 91-80-2841 2857



TO WHOMSOEVER IT MAY CONCERN

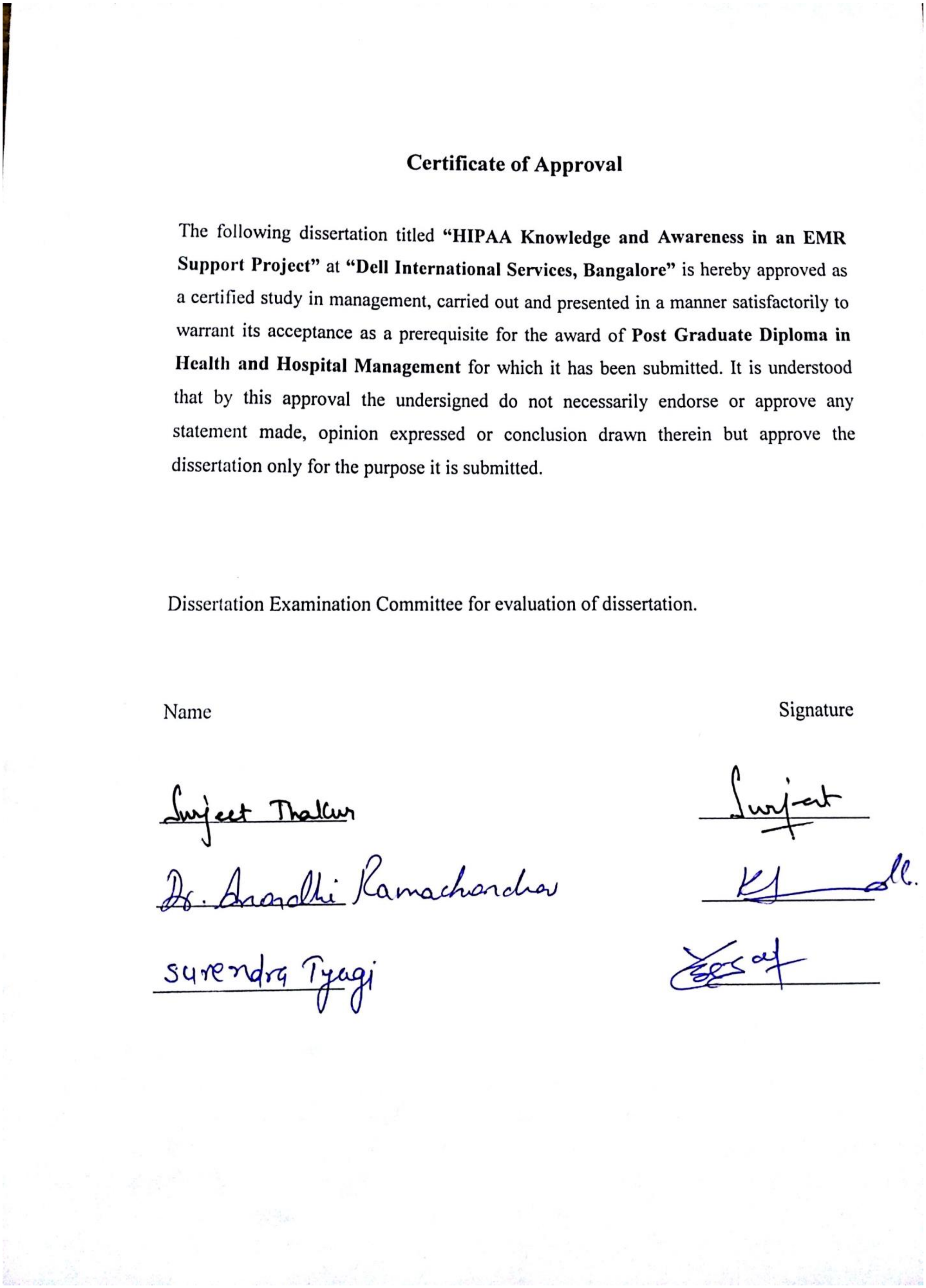
This is to certify that **Shivang Sunil Sharma**, a student of Post Graduate Diploma in Hospital and Health IT Management (PGDHM) from International Institute of Health Management Research, New Delhi has undergone internship training at **"Dell International Services, Bangalore"** from **8 February, 2016** to **29 April, 2016**.

The Candidate has successfully carried out the study designated to him during internship training and his approach to the study has been sincere, scientific and analytical.

The Internship is in fulfilment of the course requirements.

I wish him all success in all his future endeavours.

Dr. A.K. Agarwal	**Prof. Surendra Tyagi**
Dean (Academics and Student Affairs)	**Assistant Professor**
IIHMR New Delhi	**IIHMR, New Delhi**

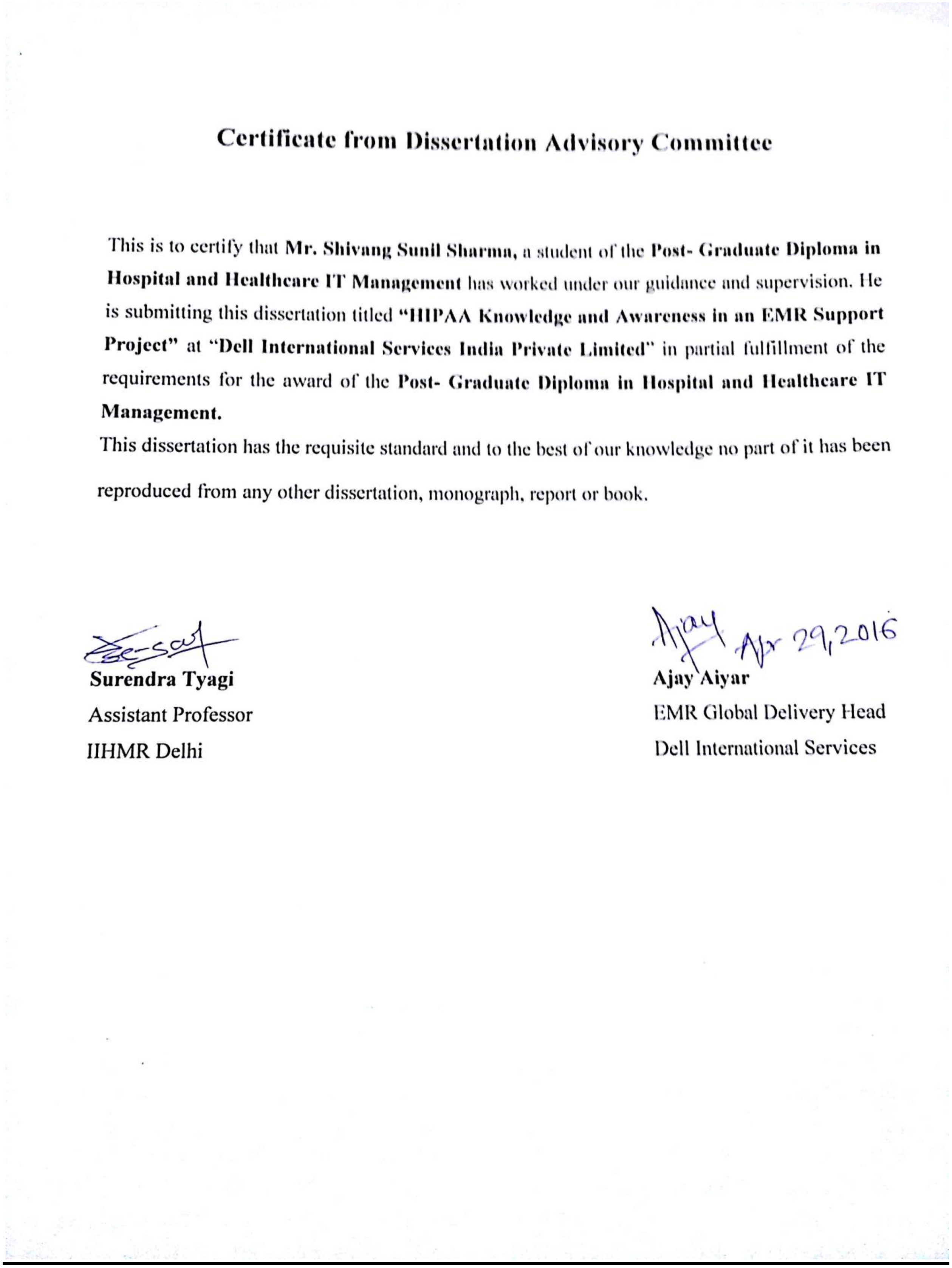


Certificate of Approval

The following dissertation titled **"HIPAA Knowledge and Awareness in an EMR Support Project"** at **"Dell International Services, Bangalore"** is hereby approved as a certified study in management, carried out and presented in a manner satisfactorily 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
Surjeet Thakur	Surjeet
Dr. Anandhi Ramachandran	
surendra Tyagi	

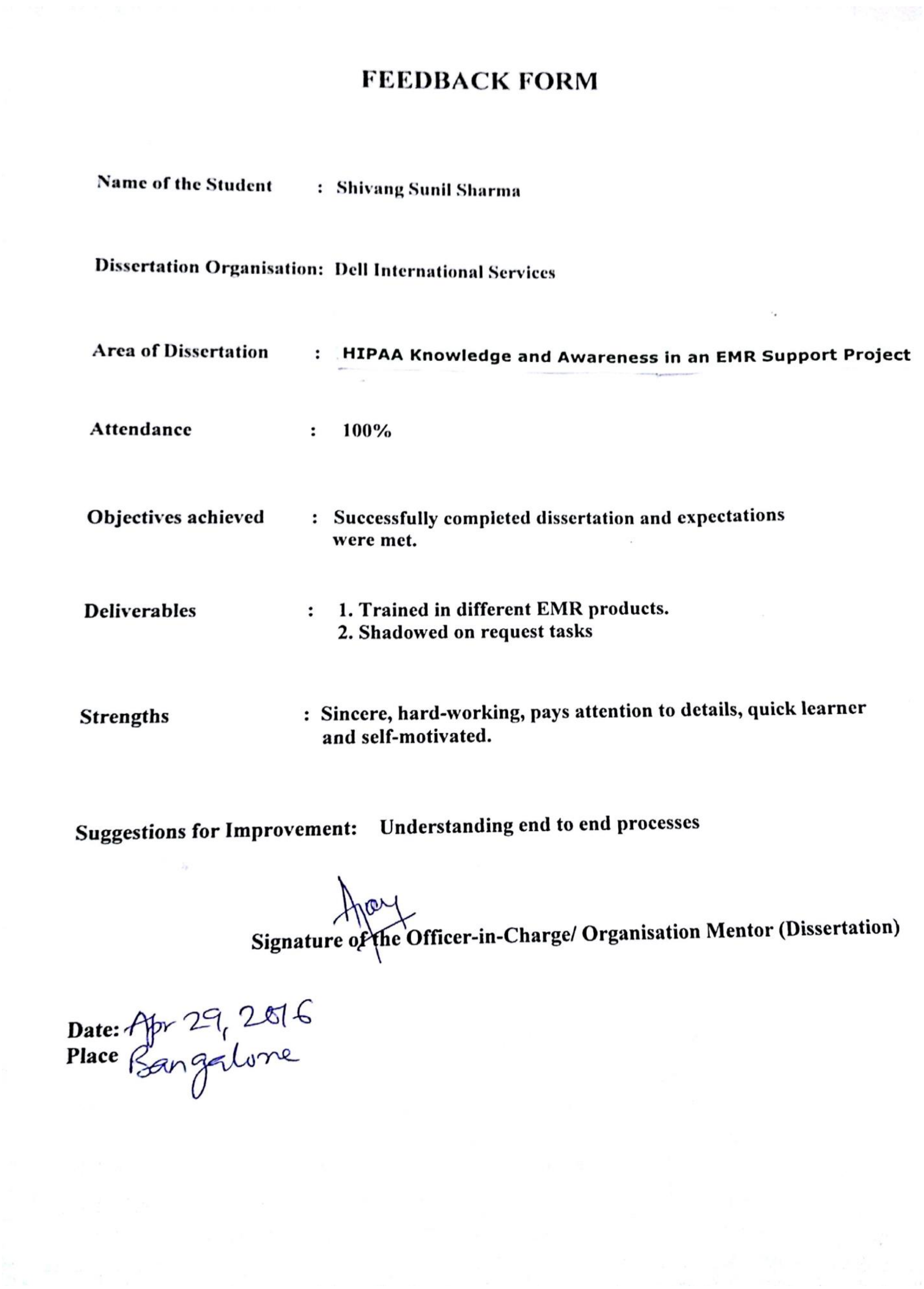


Certificate from Dissertation Advisory Committee

This is to certify that **Mr. Shivang Sunil Sharma,** a student of the **Post- Graduate Diploma in Hospital and Healthcare IT Management** has worked under our guidance and supervision. He is submitting this dissertation titled **"HIPAA Knowledge and Awareness in an EMR Support Project"** at **"Dell International Services India Private Limited"** in partial fulfillment of the requirements for the award of the **Post- Graduate Diploma in Hospital and Healthcare IT 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.

	Ajay Apr 29, 2016
Surendra Tyagi	**Ajay Aiyar**
Assistant Professor	EMR Global Delivery Head
IIHMR Delhi	Dell International Services



FEEDBACK FORM

Name of the Student : **Shivang Sunil Sharma**

Dissertation Organisation: **Dell International Services**

Area of Dissertation : **HIPAA Knowledge and Awareness in an EMR Support Project**

Attendance : **100%**

Objectives achieved : **Successfully completed dissertation and expectations were met.**

Deliverables : **1. Trained in different EMR products.**
2. Shadowed on request tasks

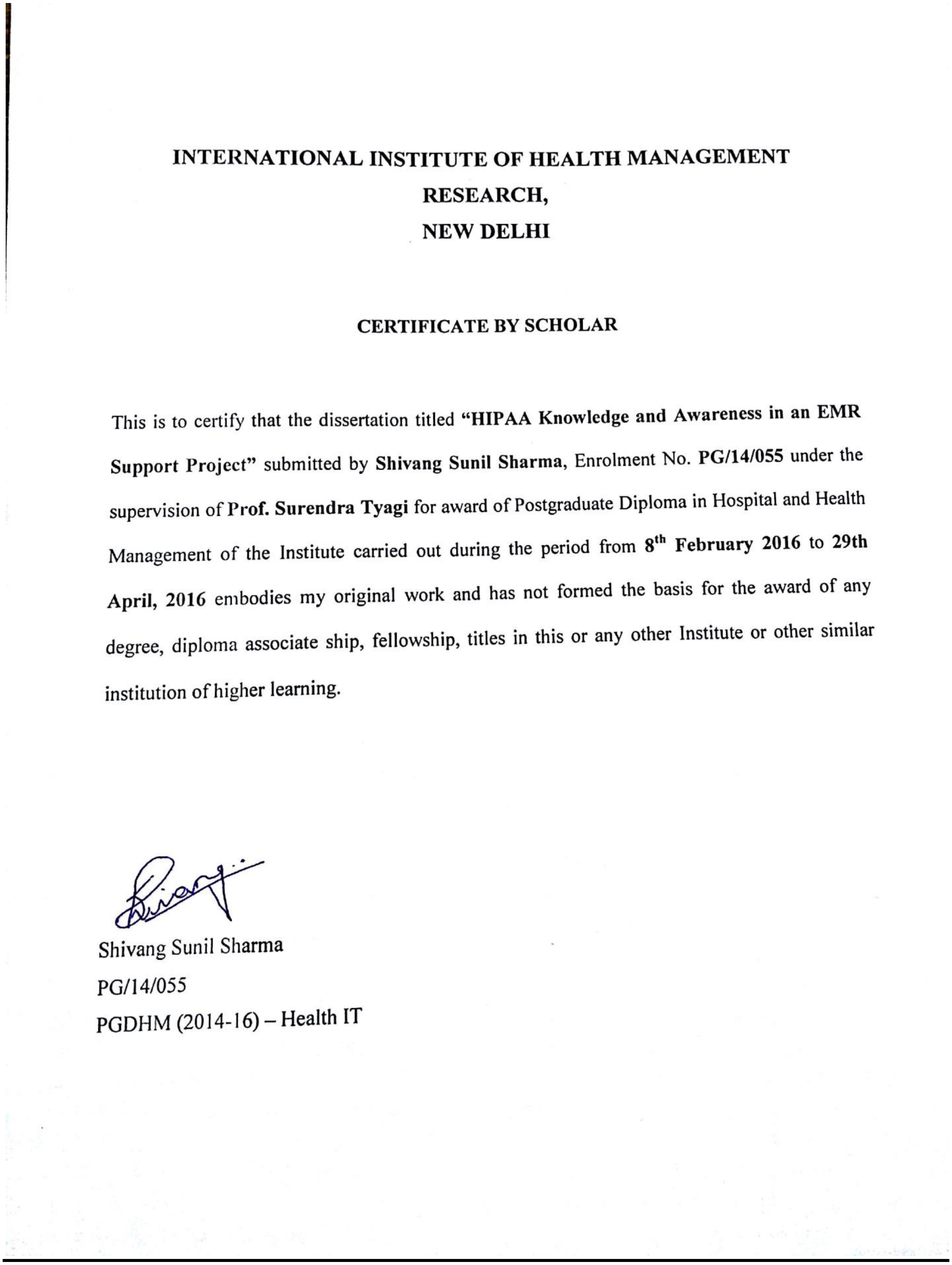
Strengths : **Sincere, hard-working, pays attention to details, quick learner and self-motivated.**

Suggestions for Improvement: **Understanding end to end processes**

Ajay

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

Date: Apr 29, 2016
Place Bangalore



INTERNATIONAL INSTITUTE OF HEALTH MANAGEMENT RESEARCH,
NEW DELHI

CERTIFICATE BY SCHOLAR

This is to certify that the dissertation titled **"HIPAA Knowledge and Awareness in an EMR Support Project"** submitted by **Shivang Sunil Sharma**, Enrolment No. **PG/14/055** under the supervision of **Prof. Surendra Tyagi** for award of Postgraduate Diploma in Hospital and Health Management of the Institute carried out during the period from **8th February 2016** to **29th April, 2016** embodies my original work and has not formed the basis for the award of any degree, diploma associate ship, fellowship, titles in this or any other Institute or other similar institution of higher learning.

Shivang Sunil Sharma
PG/14/055
PGDHM (2014-16) – Health IT

ACKNOWLEDGEMENT

Hard work, guidance and perseverance are the pre requisite for achieving success. Support from an enlightening source helps us to proceed on the path to it. I wish to thank first of all the almighty that provided me energy for the successful completion of summer training.

I am thankful and obliged to the EMR Global Delivery Head – Dell International Services Application Support - Mr. Ajay Aiyar and IT Services Managers- Ms. Archika Roy, Ms. Avishikta Sarkar and Mr. Rituraj Choudhary for giving me an opportunity to work on this project. I am also thankful to my mentors - Dr Anushree Pandit and Megha Verma for their continuous support, guidance and perseverance during the course of my project.

It has been my good fortune to be benefited by their knowledge, guidance and deep insight without which this project would not have taken the exact shape .To them, I tender my heartfelt regards.

I am highly indebted to my mentor Mr. Surendra Tyagi for his valuable guidance and motivation on various aspects of project.

Table of Content

List of Figures

Abbreviations

HIPAA	Health Insurance Portability and Accountability Act
EMR	Electronic Medical Record
EHR	Electronic Health Record
HITECH	Health Information Technology for Economic and Clinical Health Act
EDI	Electronic Data Interchange
HHS	Health and Human Services
PHI	Protected Health Information
e-PHI	Electronic Protected Health Record
CMS	Center for Medicaid & Medicare Services
ARRA	American Recovery & Reinvestment Act
ICD	International Classification of diseases
HIE	Health Information Exchange

1.0 Organization Profile

Dell is a leading provider of end-to-end scalable solutions for customers around the world delivering technology solutions that enable people everywhere to grow, thrive, and reach their full potential. Michael Dell founded the company more than 30 years ago in Austin, Texas, and since then we have been listening to and engaging our customers with their insight guiding everything we do. Dell's end-to-end solutions strategy and the innovations and investments it makes to enable that strategy are, as you would expect, truly customer-inspired.

Dell's industry focus

- Healthcare and life sciences
- Banking, financial services, securities and insurance
- Manufacturing, energy and utilities
- Consumer industries (retail, packaged goods and logistics)
- Education, state and local government
- Travel and hospitality
- Telecommunications, media and technology
- U.S. federal government

Dell in Healthcare

Dell has established four solutions groups to support customer segments—end-user computing, enterprise solutions, software and services and is committed to designing and delivering technologies that are practical, relevant, and customer-inspired. Dell's goal is to provide the best tools, products, and services for realizing hosting efficiencies, while improving service delivery. Through automation, standardization, and the right set of tools, IT works smarter to provide the "always-on and anywhere" service that end users expect.

As a leader in healthcare IT for more than 30 years, Dell is continuously chosen by customers to understand and identify the right solutions that help improve care, drive overall efficiency, and manage financial risks. The company offers end to end solutions for healthcare providers and health plans, including hardware, software, hosting, application implementation and support, systems integration, consulting, business process services, and services for Electronic

Health/Medical Records (EHRs/EMRs), Health Insurance Exchanges (HIXs), revenue cycle management, and policy administration.

Dell’s global reach encompasses operations in North America, Europe, the Middle East, and Asia. Dell currently manages IT projects for more than 1,000 hospitals worldwide. The team of experienced technologists within Dell has gained an in-depth understanding of the challenges inherent in integrating IT solutions within the most complex healthcare multi-vendor environments.

Dell’s secure end-to-end solutions and services enable healthcare organizations to solve critical problems and enhance patient care. The company’s goal is to build and support information-driven healthcare environments. This dynamic environment empowers caregivers and patients with technology, data, and processes to integrate new IT services into their daily routines for the betterment of care delivery.

Dell has successfully assisted customers with meeting their organizational goals through offering support from extremely qualified and experienced individuals who “know” healthcare organizations and workflow processes.

Industry Recognition

- Positioned by Gartner in the “Leaders” quadrant of the Gartner Magic Quadrant for Data Center Outsourcing and Infrastructure Utility Services, North America for the fifth consecutive year.
- Ranked “#1 IT Services Provider to Healthcare Providers,” by Gartner for the sixth straight year.
- Positioned as a leader in Everest Group’s “IT Outsourcing in the Healthcare Provider Industry—Service Provider Landscape with PEAK Matrix Assessment” for a third consecutive year.

1.1 Learning

During my internship in DELL International Services, Bengaluru,I learnt about various things given below:

- Various processes followed in the organization
- Workflow of the support team
- How the ticketing system works
- Daily monitoring tasks
- Trainings related to healthcare IT industry

2. Introduction

HIPAA is the federal law that requires certain entities to protect health information. HIPAA is divided into two sections - the Privacy Rule & the Security Rule.

- The Privacy Rule includes requirements on how entities can use or disclose health information, and
- Security Rule has requirements on how entities must secure and protect health information.

HIPAA only applies to the covered entities; a “covered entity” is defined as the healthcare provider, health plan, or healthcare clearinghouse. The adoption of the electronic medical records (EMR) by the healthcare Industry has made it mandatory for all the Organizations to ensure the safe handling of the sensitive data.

The importance of maintaining the highly sensitive information of patients is highly essential, as this is the data that can be used against the individuals in case of the database is getting hacked, corrupted or stolen. Any organization that have access to the patient health information is considered as covered entity and thus is required by law to comply with the HIPAA provisions or face civil and/or criminal penalties.

HIPAA Privacy Rule establishes the privacy requirement for the patients, HIPAA Security Rule also has an eye on the protections contained in Privacy Rule by addressing the technical & non-technical safeguards that the organizations called as the "covered entities" must put in place to secure the individuals' "protected health information" (PHI).

HIPAA Security Rule mainly focuses on the safeguard of "electronic protected health information" (e-PHI) that is created, received, transmitted, or maintained by a covered entity. HIPAA compliance is one of the necessity in today’s environment as the non-compliance brings the risks of penalties, prison, & lawsuits that can have an impact either on the individuals or the corporate entities.

2.1 Regulatory Overview

The Health Insurance Portability and Accountability Act (HIPAA) was passed by the US Congress in the year 1996 to safeguard the patient identities, medical records, health insurance activities & other protected health information (PHI).HIPAA is the federal law which wants some entities to protect the health information. The regulation makes it compulsory that healthcare plans, clearinghouses and the providers take essential steps to make sure that there is standardization of the electronic patient data, assign unique health identifiers to the patients and other people, and also implement security standards regarding the overall confidentiality and integrity of the patient data. It is required by the HIPAA Security Standard and Implementation specification that the access control rules and unique user identifiers should be addressed in a combination of encryption, port & the application controls.

2.2 HIPAA Components

1. **Title I: Health Care Access, Portability, and Renewability**

   "Health care access, portability and renewability," employers and health plans must allow a new employee's medical insurance coverage to remain continuous without regard to pre-existing conditions. [1]

2. **Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform**

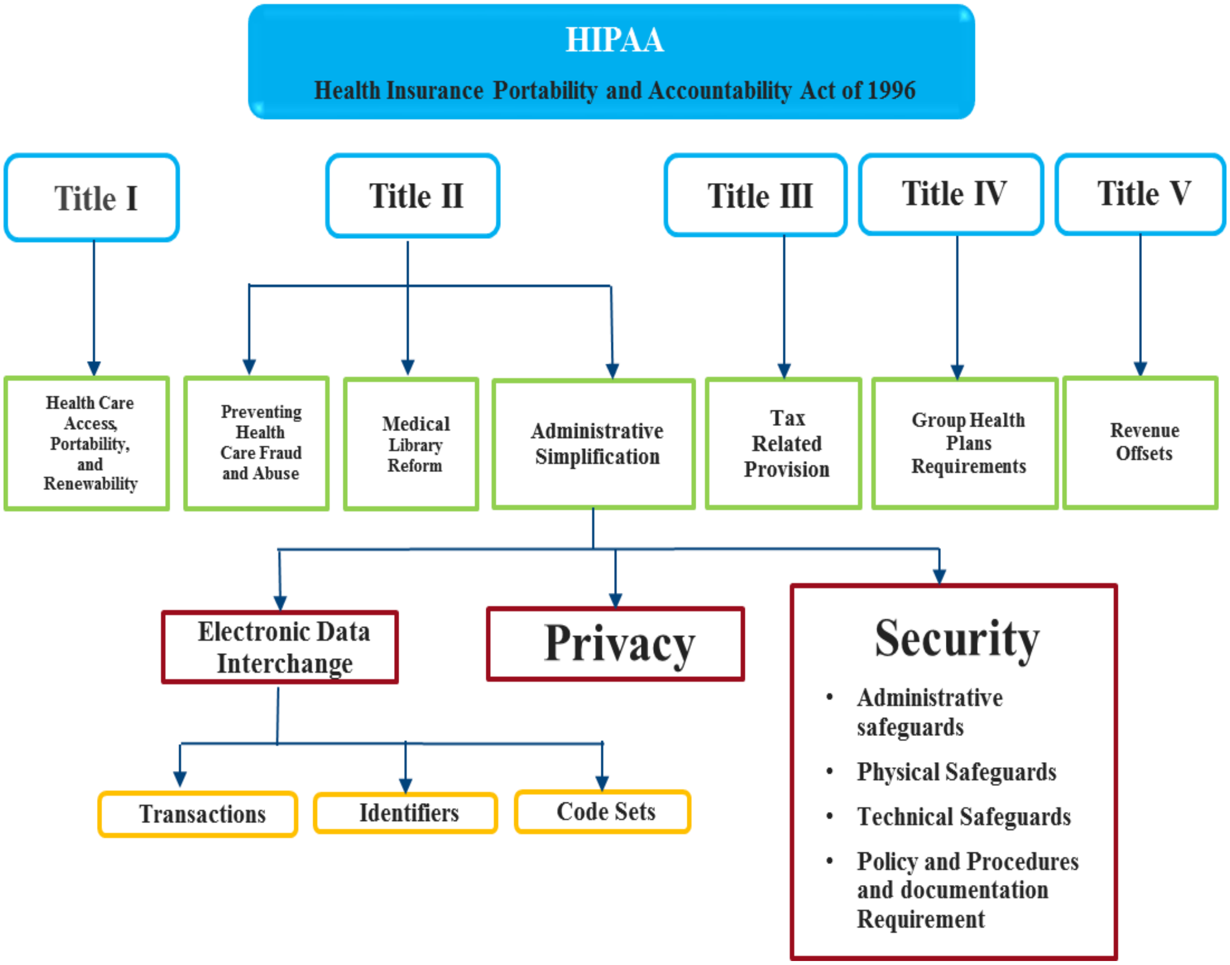
   "Preventing health care fraud and abuse; administrative simplification; medical liability reform" defines new requirements for privacy and security of individually identifiable patient information."Administrative simplification," **Subtitle F** reduces the administrative component of health care costs through the implementation of electronic data interchange (EDI) standards primarily by embracing ASC X12N transaction formats. [1]

3. **Title III: Tax-related health provisions governing medical savings accounts**

   "Tax-related health provisions" standardizes the amount you can save per person in a pre-tax medical savings account. [1]

4. **Title IV: Application and enforcement of group health insurance requirements**" Application and enforcement of group health plan requirements" broadened information on insurance reform provisions and provide detailed explanations.[1]
5. **Title V: Revenue offset governing tax deductions for employers** "Revenue offsets" are regulations on how employers can deduct company-owned life insurance premiums for income tax purposes. [1]

Figure 1.HIPAA Components


HIPAA
Health Insurance Portability and Accountability Act of 1996
Title I
Title II
Title III
Title IV
Title V
Health Care Access, Portability, and Renewability
Preventing Health Care Fraud and Abuse
Medical Library Reform
Administrative Simplification
Tax Related Provision
Group Health Plans Requirements
Revenue Offsets
Electronic Data Interchange
Privacy
Security
Administrative safeguards
Physical Safeguards
Technical Safeguards
Policy and Procedures and documentation Requirement
Transactions
Identifiers
Code Sets

2.3 Protected Heath Information

Personal health information (PHI), also referred to as protected health information, generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and revisions to HIPAA made in 2009's Health Information Technology for Economic and Clinical Health (HITECH) Act, covered entities which include healthcare providers, insurers and their business associates are limited in the types of PHI they can collect from individuals, share with other organizations or use in marketing. In addition, organizations must provide protected health information to patients if requested preferably in an electronic PHI format. Organizations cannot sell PHI unless it is for public health activities, research, treatment, services rendered or the merger or acquisition of a HIPAA covered entity. HIPAA also gives individuals the right to make written requests to amend PHI that a covered entity maintains. Partners or business associates of healthcare providers that sign HIPAA business associate agreements are legally bound to handle patient data in a way that satisfies the HIPAA Privacy and Security Rules. Business associates, as well as covered entities, are subject to HIPAA audits, conducted by the U.S. Department of Health and Human Services Office for Civil Rights (OCR). [2]

HIPAA's rules for protected health information were initially mostly applied to paper records. Since the passage of the HITECH Act and healthcare providers' subsequent implementations of electronic health records (EHRs) and other modern health IT systems, HIPAA has increasingly governed electronically-stored patient data because providers transitioned PHI from paper to electronic formats. While the HIPAA rules regulate paper and electronic data equally, there are differences between the two formats. First, patients that submit a request for access to their data can be answered by a covered entity within the 30-day period, a timeframe that was created to accommodate the transmission of paper records. The disposal methods of PHI also vary between electronic and paper records. Paper files can be shredded or otherwise made unreadable and unable to be reconstructed. Electronic PHI should be cleared or purged from the system in which it was previously held. [2]

2.4 HIPAA Privacy Rule

- The HIPAA Privacy Rule sets rules and regulations for the use and disclosure of Protected Health Information (PHI) which is being used and held by the "covered entities" which are the health care clearinghouses, employer sponsored health plans, healthcare insurers, and the medical service providers which are engage in some of the certain transactions.[3]
- As per the regulations governed, the Department of Health and Human Services had extended the HIPAA privacy rule to all the independent contractors of covered entities which will fit in the definition of the "business associates." [3]
- Protected Health Information which is termed as PHI by the privacy rule is the unique information in medical record which can be used to identify the person, and which was created or/used or disclosed in the process of providing healthcare service. PHI is personally identifiable information in medical records which can also include the medical treatment conversation between a patient and a doctor. The billing information and any information in health insurance company's records than can identify a patient is also included in the PHI.[3]

2.5Privacy Rule: Establishing Minimum Standards

The privacy rule has established certain minimum requirements and standards in order to safeguard the patients' privacy and confidentiality. It requires "covered entities" i.e. health care providers, health plans, health care clearinghouses in order to protect the privacy and the confidentiality of patients' medical information. As per the Privacy Rule the covered entities are required to take reasonable steps so as to limit the use or disclosure of, and requests for, PHI to the minimum necessary to achieve the intended purpose.[4]

The minimum necessary standard is not applicable to the following:

- Disclosures to or requests by a health care provider for the purpose of treatment.
- Disclosures of the information to the individual who is the subject.
- Uses or disclosures done pursuant to an individual's authorization.
- Uses or disclosures that are being required for the compliance with the HIPAA Administrative Simplification Rules.(Title II)

- Disclosures to Department of Health and Human Services (HHS) under the Privacy Rule for enforcement purposes when the disclosure of information is required by HHS.
- Uses or disclosures that are being required by some other law.

The main purpose is to direct all the covered entities so that they should control the ways in which they disclose and use patients' PHI and also to offer the patients certain amount of rights with respect to their personal information which includes the right to inspect as well as copy, the right to make request for amendments including the right to request an accounting. [4]

Also the covered entities under HIPAA must have certain amount of administrative protections accordingly so as to assure the privacy as well as confidentiality of patients' information which can be done as appointing privacy officers, implementation of appropriate policies and procedures and staff training sessions. Where the privacy rule looks after to restrict who all may have the access to the health information and the way in which it may be distributed, the rule knows the necessity and the need of medical practitioners and physicians to access patients' records during the course of treatment. Most importantly, the rule creates an exception for treatment activities such as:

- A covered entity may disclose PHI for the purpose of treatment activities of a health care provider. The privacy rule make measures to protects information that is in concern with the health care treatment or may be the payment that can be potentially identify and reveal the identity a particular patient i.e. "individually identifiable health information" also known as IIHI, which is being defined as "any information, including demographic information collected from an individual that" -
    - Is being created or is received by a health care provider or/ health plan or/ employer or/ a health care clearinghouse
    - Information that may relate to past, present, or future physical or mental health or it may be a condition of an individual or/ the provision of health care to an individual or/ the past, present, or future payment for the purpose of provision of the health care to an individual

2.6The Final Omnibus Rule Update- 2013

- In January 2013, HIPAA law was updated via the Final Omnibus Rule. The new update in the law included changes that were related to the updates to the Security Rule and to the Breach Notification portions of the HITECH Act. The greatest changes were related to the expansion of the requirements that mentioned to include the business associates, where till now only the covered entities were supposed to originally been held to uphold all these sections of the law.[5]
- In addition to that definition of 'significant harm' to an individual in the case of a breach was now updated to provide more scrutiny to the covered entities having the intention of disclosing more number of breaches which might be previously gone unreported. Before this an organization needed proof to prove that the harm had occurred whereas now they need to just prove that the counter that harm had not occurred.[5]

The only drawback of HIPAA is that the hospitals will not be able to reveal any information to relatives over the phone for individual that may have been be admitted under the emergency conditions or else even if that individual is a patient in that hospital.[5]

2.7Transaction and Code Set Standards under the Privacy Rule

- Transactions are electronic exchanges that may involve the transfer of information between two parties so that the administrative and financial activities can be carried out related to the health care activities. HIPAA has adopted specific standard transactions for the purpose of electronic data interchange of administrative health care data. Under HIPAA, it is clearly stated that if a covered entity performs any of the adopted transactions in an electronic format, then they must use adopted standard as specifies. [6]
- HIPAA also specifies to adopt the specific code sets for diagnoses purpose and for the procedures to be used in all the transactions process, which may include the Current Procedural Terminology known as the CPT codes for the outpatient services/procedures, the Health Care Procedure Coding System known as HCPCS which are the ancillary services/procedures, International Classification of Diseases i.e. ICD-9 and ICD-10 [6]

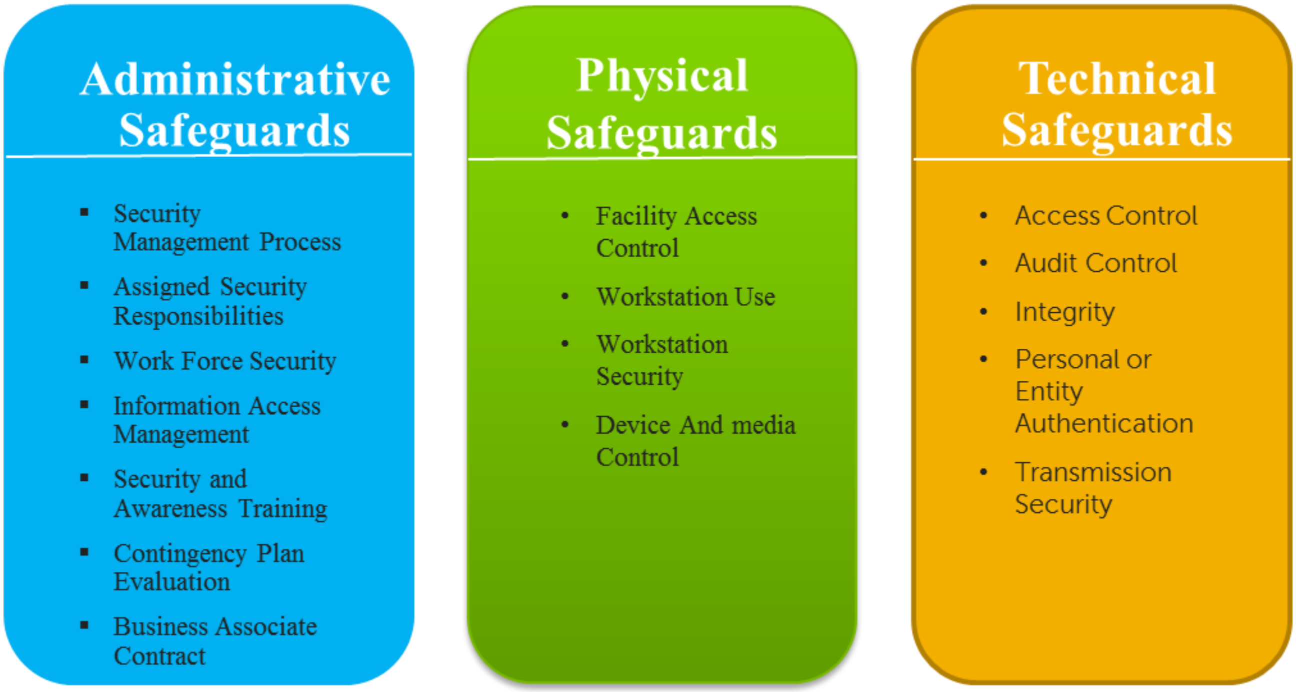
2.8 HIPAA Security Rule

Objectives

As per the Security Standards Rule of HIPPA each covered entity or its business associate must follow and comply with following set of rules -

- Ensure the confidentiality, integrity and availability of e-PHI that it creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats and hazards to the security or integrity of e-PHI.
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.
- Confidentiality is "the property that data or information is not made available or disclosed to unauthorized persons or processes."
- Integrity is "the property that data or information have not been altered or destroyed in an unauthorized manner."
- Availability is "the property that data or information is accessible and usable upon demand by an authorized person."

Figure2. HIPAA Security Rule Components:



Administrative Safeguards

- Security Management Process
- Assigned Security Responsibilities
- Work Force Security
- Information Access Management
- Security and Awareness Training
- Contingency Plan Evaluation
- Business Associate Contract

Physical Safeguards

- Facility Access Control
- Workstation Use
- Workstation Security
- Device And media Control

Technical Safeguards

- Access Control
- Audit Control
- Integrity
- Personal or Entity Authentication
- Transmission Security

Security standards and specifications are as follows:

Administrative Safeguards

The Security Rule defines administrative safeguards as, “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.” The Administrative Safeguards comprise over half of the HIPAA Security requirements. As with all the standards in this rule, compliance with the Administrative Safeguards standards will require an evaluation of the security controls already in place, an accurate and thorough risk analysis, and a series of documented solutions derived from a number of factors unique to each covered entity.[7]

Physical Safeguards

The Security Rule defines physical safeguards as “physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.” The standards are another line of defense (adding to the Security Rule’s administrative and technical safeguards) for protecting e-PHI. When evaluating and implementing these standards, a covered entity must consider all physical access to e-PHI. This may extend outside of an actual office, and could include workforce members’ homes or other physical locations where they access e-PHI. [8]

Technical Safeguards

The Security Rule defines technical safeguards as “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.” The Security Rule is based on the fundamental concepts of flexibility, scalability and technology neutrality. Therefore, no specific requirements for types of technology to implement are identified. The Rule allows a covered entity to use any security measures that allows it reasonably and appropriately to implement the standards and implementation specifications. A covered entity must determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization. The Security Rule does not require specific technology solutions. There are many technical security tools, products, and solutions that a covered entity may select. Determining which security measure to implement is a decision that covered entities must make based on what is reasonable and appropriate for their specific organization [9]

3. Review of Literature

HIPAA provides portability of health insurance from employer to employer; standards for transmitting health information in writing, orally, and electronically; and methods for assuring the security, confidentiality, and privacy of personal health information. The legislation, originally passed in 1996, and amended several times over the intervening years, was finally implemented in 2003, according to Swartz (2003). In the years of its development and since its implementation, HIPAA has raised deeply fundamental issues for healthcare providers, insurers, employers, policy makers, researchers, and, most prominently, for patients and consumers of healthcare services and their families. The goal of HIPAA is to ensure the protection of confidential health information through having appropriate security systems to guard against unintentional disclosure of that information (Erlen, 2007).[10]

Swartz, N. A. (2003) in his study on **What every business needs to know about HIPAA** states that the reason that business stakeholders are so interested in the HIPAA legislation is that healthcare organizations share information with a variety of business associates ("any entity working in partnership with the covered entity and receiving health information from the covered entity or working for or on behalf of the covered entity" who are also subject to HIPAA legislation, such as "vendors, consultants, lawyers, auditors, clearinghouses, billing firms, and record storage"[11]

In a study by *Maddox P. J.* on **HIPAA: Update on Rule Revisions and Compliance Requirements** regulatory framework of HIPAA is described. The Department of Health and Human Services (DHHS) was charged with implementing HIPAA and establishing regulations for accessing, transmitting, and storing health information. The regulations mandated "that electronically stored personal health information be kept confidential and protected against unauthorized users and any threats to its security or integrity".[3] DHHS estimated that $29.9 billion would be saved over 10 years due to the efficiency that would be gained in administrative processes and procedures.[12]

A study by Smith, *Harry E.* on “**The HIPAA Final Security Rule-More Than a New Security Standard**, states that one of the biggest challenges presented by the security rule of HIPAA is how to codify information security standards and implementation specifications that could be understood and imposed fairly on a group of organizations that differed greatly in scale. The solution was to incorporate a set of “required,” mandatory security standards and a set of specifications that were “addressable.” Addressable standards were not required to be implemented by organizations for which, in view of the organization's size and available resources, the standards were either “inappropriate” or “unreasonable.” According to Smith, the required implementation specifications include safeguards related to risk analysis, risk management, sanctions policies, information system activity review, isolation of clearinghouse functions, incident response, backup, disaster recovery, emergency modes of operation, business associate contracts, disposal, media reuse, unique user identification, emergency access procedures, and documentation. These were categorized into three groups of safeguards to establish a minimum level of protection- administrative safeguards, physical safeguards, and technical safeguards.[13]

A study by *Amatayakul, Margret* on “**Putting the Finishing Touches to Security**,” states that with the development of policies and procedures to achieve HIPAA security compliance firmly established in most facilities, a number of issues remain to be resolved. Because many hospital personnel are involved in the total care of a patient, it is no surprise that above the fears of natural disaster, equipment compromise, or even terrorist attack, the greatest threat to security of EPHI was perceived to be employee error, with the employee group most named as a concern being “support staff.” This finding supports the statement by Amatayakul that “a large percentage of security incidents are the result of human error, not machine error.[14]

A study by *F. Caoa,*, H.K. Huanga , X.Q. Zhoub***Medical image security in a HIPAA mandated PACS environment** describes that medical image security is an important issue when digital images and their pertinent patient information are transmitted across public networks. Mandates for ensuring health data security have been issued by the federal government such as Health Insurance Portability and Accountability Act (HIPAA), where healthcare institutions are obliged to take appropriate measures to ensure that patient information is only provided to people who have a professional need. Guidelines, such as digital imaging and communication in medicine (DICOM) standards that deal with security issues, continue to be published by organizing bodies in healthcare. However, there are many differences in implementation especially for an integrated system like picture archiving and communication system (PACS), and the infrastructure to deploy these security standards is often lacking. Over the past 6 years, members in the Image Processing and Informatics Laboratory, Children's Hospital, Los Angeles/University of Southern California, have actively researched image security issues related to PACS and tele-radiology. The paper summarizes our previous work and presents an approach to further research on the digital envelope (DE) concept that provides image integrity and security assurance in addition to conventional network security protection. The DE, including the digital signature (DS) of the image as well as encrypted patient information from the DICOM image header, can be embedded in the background area of the image as an invisible permanent watermark. The paper outlines the systematic development, evaluation and deployment of the DE method in a PACS environment. We have also proposed a dedicated PACS security server that will act as an image authority to check and certify the image origin and integrity upon request by a user, and meanwhile act also as a secure DICOM gateway to the outside connections and a PACS operation monitor for HIPAA supporting information. q 2002 Elsevier Science Ltd. All rights reserved.[15]

A study by Joy L. Pritts, JD***The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research** describes that the privacy of personal information, and of health information in particular, continues to be a vexing issue in the United States. As more and more health information is computerized, individuals express concern about their privacy and that they are losing control over their personal health information. To help allay public concerns, federal rules governing the use and disclosure of health information were promulgated under the Health Insurance Portability and Accountability Act (known as the HIPAA Privacy Rule). While the HIPAA Privacy Rule does not directly regulate researchers, it does restrict the manner in which health care providers may use and disclose health information for health research. Health researchers have been critical of the HIPAA Privacy Rule since its inception, concerned that it would interfere with valuable research. Various research organizations and others have requested that the Rule be revised to lessen its effect on research. Most recently, an Institute of Medicine (IOM) committee was formed and charged with reviewing the impact of the Privacy Rule on health research. This paper was commissioned by that committee, the IOM Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule. Because there were a number of other studies presented to the Committee on the impact of research, this paper does not focus on researchers. Rather, it is intended to provide background information on the importance of protecting privacy in general and, more specifically, in the context of research, from the perspective of the individual. To set the stage, Part I of his paper first gives a very general overview of the various concepts of privacy and its value. Part II focuses specifically on the importance of protecting the privacy of health information. It reviews public attitudes toward the privacy of health information and discusses the value that privacy serves in the health care context. Because the HIPAA Privacy Rule and the "Common Rule," the regulations that directly govern most research, evolved in different contexts and, therefore, take different approaches to protecting privacy, Part III of this paper describes the historical development of the legal protections for health information in the United States.[16]

In an article named **HITECH's Challenge to the Health Care Industry,** it is explained that the Health Information Technology for Economic and Clinical Health Act (HITECH) forces health care providers and their business associates to bring a sense of urgency to the security of protected health information (PHI). The act brings both pressures and incentives into play in its mandate to convert PHI to electronic health records (EHR), and puts teeth into the enforcement of the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA). Although the HIPAA Security and Privacy rules have been in effect since 2003, auditing has been, at best, spotty, enforcement and imposition of penalties rare, and they did not apply directly to business associates. Under these conditions, it's not surprising that healthcare has lagged behind most other industries in their security programs. More than one fifth of the respondents in the 2009 survey conducted by the Healthcare Information and Management Systems Society (HIMSS) reported that security accounted for less than 1% of their budget, with almost no change from the previous year. Forrester Research's annual security survey showed that healthcare trails financial services, retail and government sectors in the percentage of overall IT budget spent on security. Information security has not been a high-priority issue for hospitals, which naturally evaluate commitment of energy, spending and allocation of resources in terms of their impact on the quality of patient care. Before HITECH, there were no incentives and little concern about enforcement. Conversion to EHR will result in explosive growth in digital information sharing among health information exchanges, hospitals, medical practices and business associates. Under HITECH, all recipients of PHI contained in EHR are now subject to the same requirements for protecting PHI. The risk of inadvertent or malicious disclosure of health information increases dramatically, and there is evidence that attackers are taking note and targeting healthcare institutions in growing numbers. In this environment, healthcare providers should assess their security programs and ensure that they have the policies, processes and supporting automated tools in place to protect patient information.[17]

In the article issued by **Cerner Corporation: Health Insurance Portability and Accountability Act of 1996 (HIPAA): Positioning of Support for EDI, Privacy and Security Requirements by Solution Updated for Key Provisions of the American Recovery and Reinvestment Act of 2009 (ARRA HITECH),** mentions that the Health Insurance Portability and Accountability Act (HIPAA) of 1996 presents great challenges and requirements for healthcare providers as covered entities to meet compliance requirements of the major rules that comprise the Administrative Simplification provisions of the Act. In reviewing the requirements of the rules that can be taken as having import for information systems, Cerner has attempted to identify the most significant areas where Cerner’s Millennium application suite can assist Cerner’s clients in achieving their organizational compliance objectives for HIPAA. Additionally, with the signing into law of the American Recovery and Reinvestment Act (ARRA) of 2009, a number of new provisions were enacted under the HITECH portion of the Act that extend the HIPAA Security and Privacy Rule requirements for certain patient rights such as the patient right of access to an electronic copy of their record, the right to receive an accounting of disclosures when made from an electronic health record for treatment, payment or healthcare operations and to restrict disclosures of patient information to a health plan for services the patient paid for out of pocket. ARRA HITECH also instituted breach notification requirements for breaches involving electronic health records and personal health records, and some new requirements were introduced connected to safe harbor requirements under the breach notification rules issued by the federal government in 2009 that involve use of encryption. The purpose of this whitepaper is to review the major areas of compliance requirement and the role in compliance played by each major Cerner solution type based upon current capability as Millennium 2007.19 and 2010.01 [18

In an article named **Privacy and security in the implementation of health information technology (Electronic Health Record): U.S. & EU compared** the importance of the adoption of Electronic Health Records (EHRs) and the associated cost savings cannot be ignored as an element in the changing delivery of health care. However, the potential cost savings predicted in the use of EHR are accompanied by potential risks, either technical or legal, to privacy and security. The U.S. legal framework for healthcare privacy is a combination of constitutional, statutory, and regulatory law at the federal and state levels. In contrast, it is generally believed that EU protection of privacy, including personally identifiable medical information, is more comprehensive than that of U.S. privacy laws. Direct comparisons of U.S. and EU medical privacy laws can be made with reference to the five Fair Information Practices Principles (FIPs) adopted by the Federal Trade Commission and other international bodies. The analysis reveals that while the federal response to the privacy of health records in the U.S. seems to be a gain over conflicting state law, in contrast to EU law, U.S. patients currently have little choice in the electronic recording of sensitive medical information if they want to be treated, and minimal control over the sharing of that information. A combination of technical and legal improvements in EHRs could make the loss of privacy associated with EHRs de Minimis. The EU has come closer to this position, encouraging the adoption of EHRs and confirming the application of privacy protections at the same time. It can be argued that the EU is proactive in its approach; whereas because of a different viewpoint toward an individual's right to privacy, the U.S. system lacks a strong framework for healthcare privacy, which will affect the implementation of EHRs. If the U.S. is going to implement EHRs effectively, technical and policy aspects of privacy must be central to the discussion. [19]

In **Information Security Policies and Governance to Safeguard Protected Health Information** it was explained about how the healthcare organizations must comply with the Health Insurance Portability and Accountability Act of 1996 and develops information security policies that ensure the confidentiality, integrity, and accessibility of sensitive information; however guidelines are vague. This bibliography identifies policies and describes information security governance strategies designed to ensure compliance. Organizations must create a leadership committee to (a) assess current policies, (b) oversee policy enforcement, (c) note the effects of internal and external influences, and (d) maintain currency. [20]

The use of technology in counseling is expanding. Ethical use of technology in counseling practice is now a stand-alone section in the 2014 American Counseling Association Code of Ethics. The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act provide a framework for best practices that counselor educators can utilize when incorporating the use of technology into counselor education programs. This article discusses recommended guidelines, standards, and regulations of HIPAA and HITECH that can provide a framework through which counselor educators can work to design policies and procedures to guide the ethical use of technology in programs that prepare and train future counselors. [21]

4.0 Scope of Study and Study Objectives

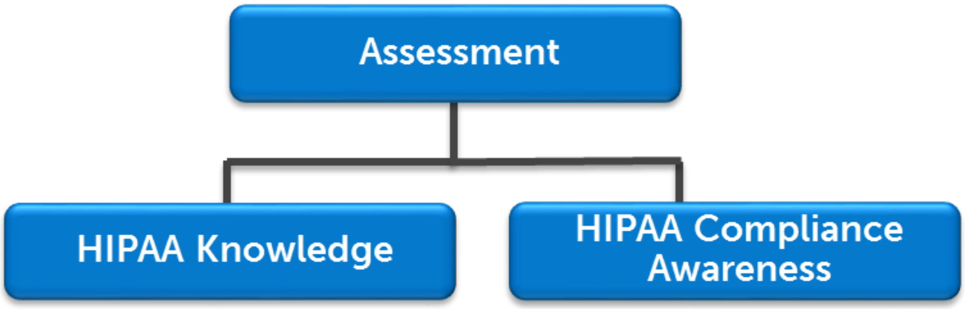
Scope of the Study

The study aims to assess the knowledge about HIPAA as a concept amongst Support Employees of Healthcare IT Project. The study also intends to measure the awareness of the Support Employees of Healthcare IT Project about the existing measures being taken by the organization in order to abide by HIPAA rule.

The study does not intend to measure/audit HIPAA rule compliance with in the organization. It only intends to measure the knowledge and awareness of the Study group on HIPAA.

Study Objective

To measure the extent of HIPPA knowledge and compliance awareness within Support Employees in a Healthcare project.



5.0 Methodology

- **Study Type:** Cross sectional and descriptive
- **Study Organization:** Healthcare IT Organization, Bangalore
- **Target Population:** Support Employees
- **Sample Size:**112 support employees
- **Sampling:** Convenient Sampling – based on availability and voluntary participation
- **Duration of the Study:** 8th February, 2016 to 29th April, 2016
- **Data Collection Method & Tools:** Primary Data (quantitative) through structured questionnaires. The tool includes items for
  - HIPAA Knowledge Assessment
  - Compliance Awareness Assessment

- **Ethical Considerations**
  - Security of Organization’s Data
  - Privacy and Confidentiality shall be maintained
  - Data/findings will not be shared with any other organization/person

6.0 Study Findings

HIPAA Knowledge Assessment Result Findings for Support Employees

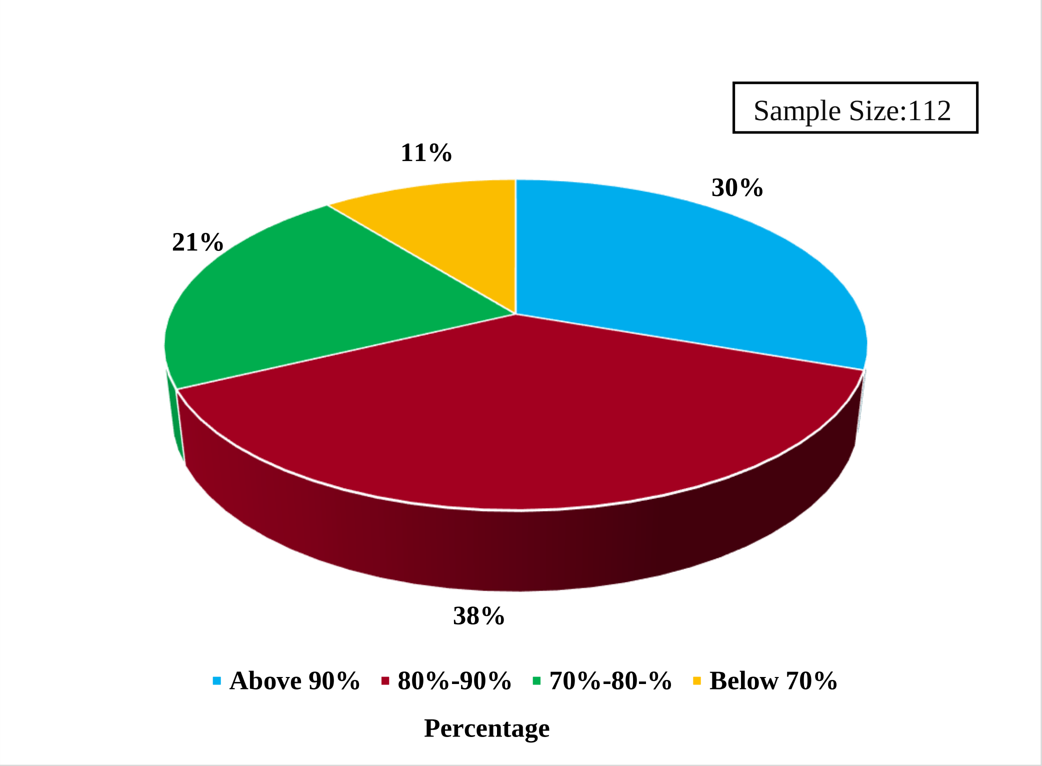
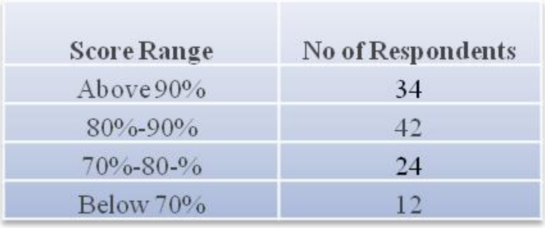


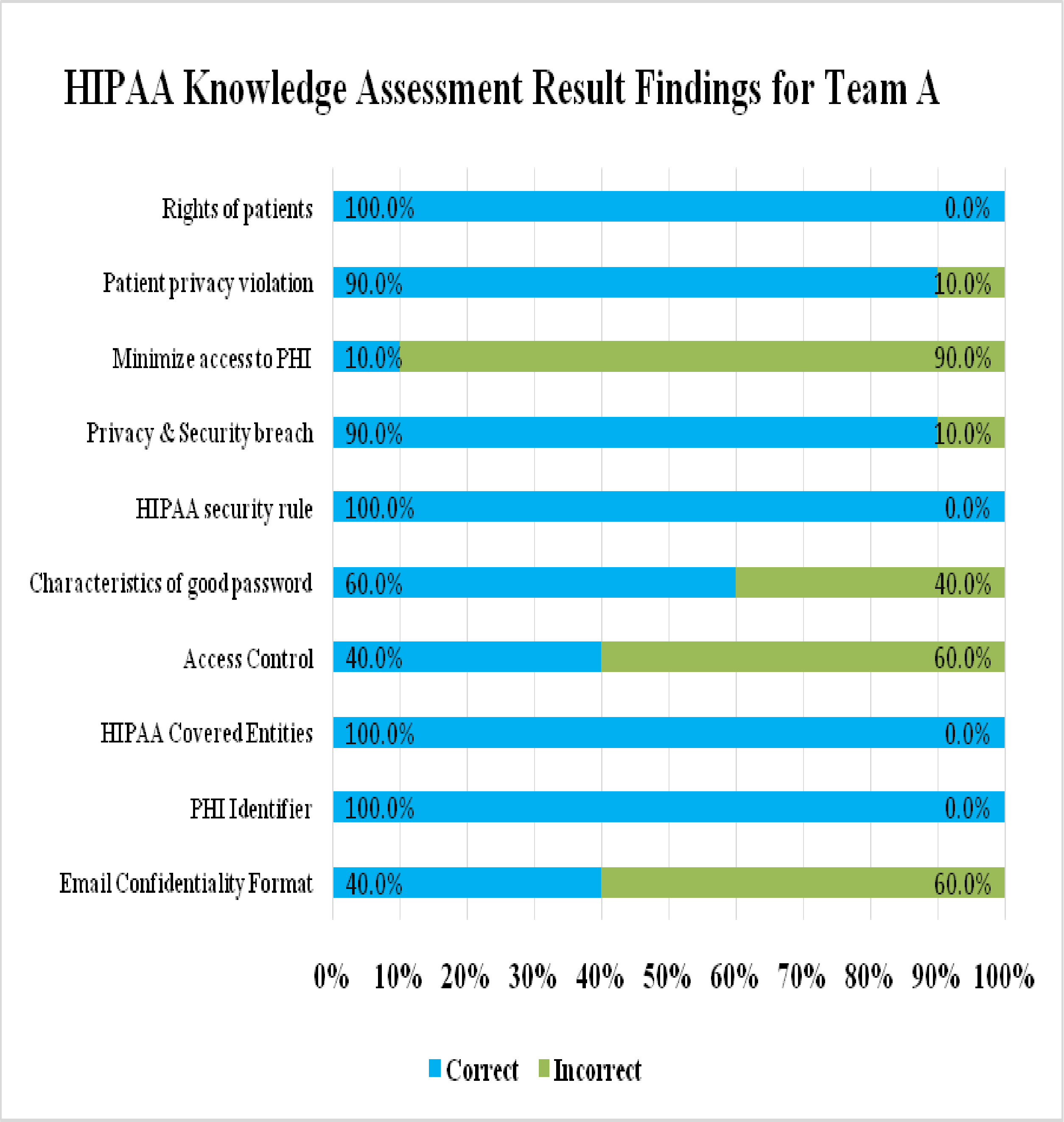
Figure No.3

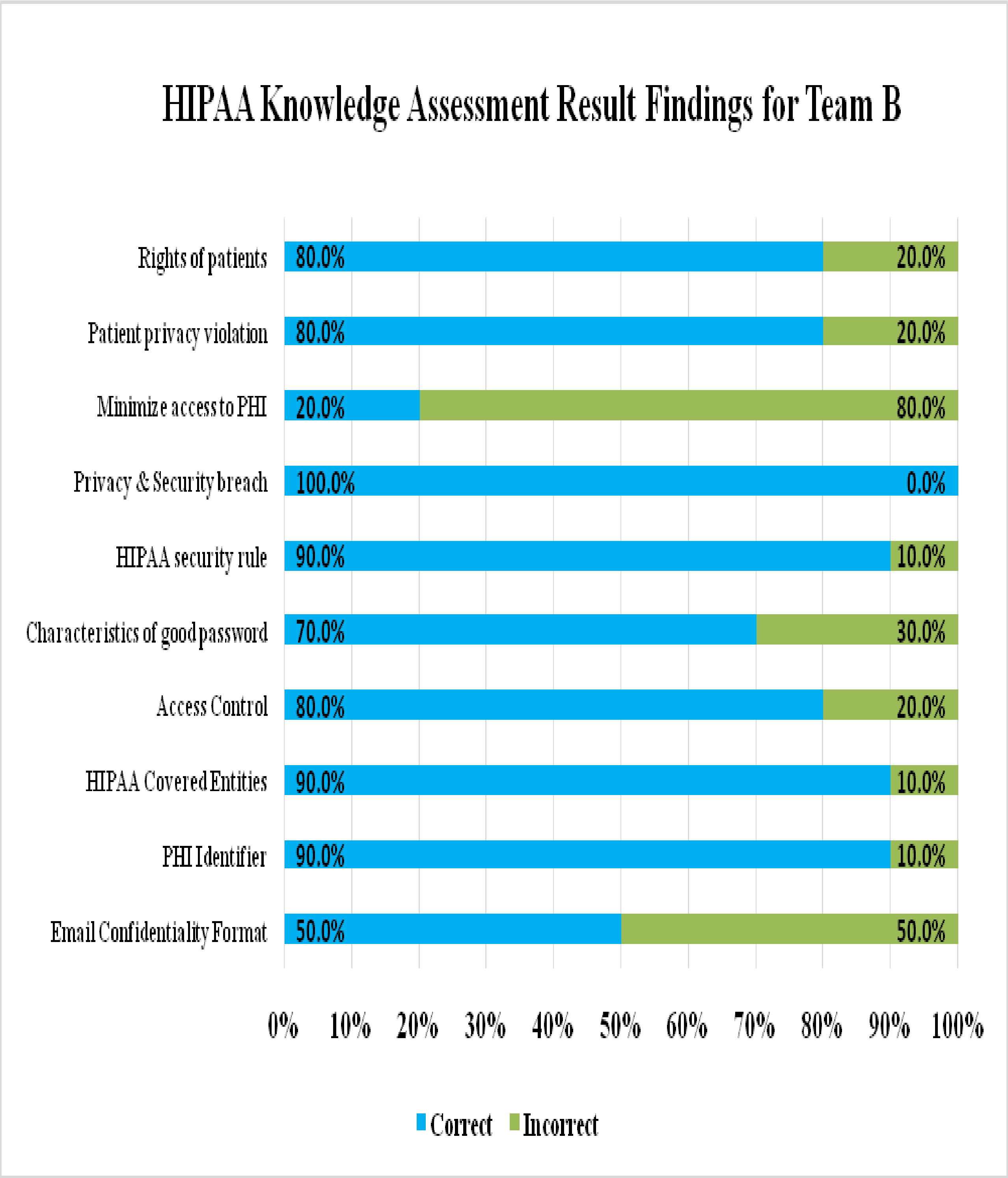


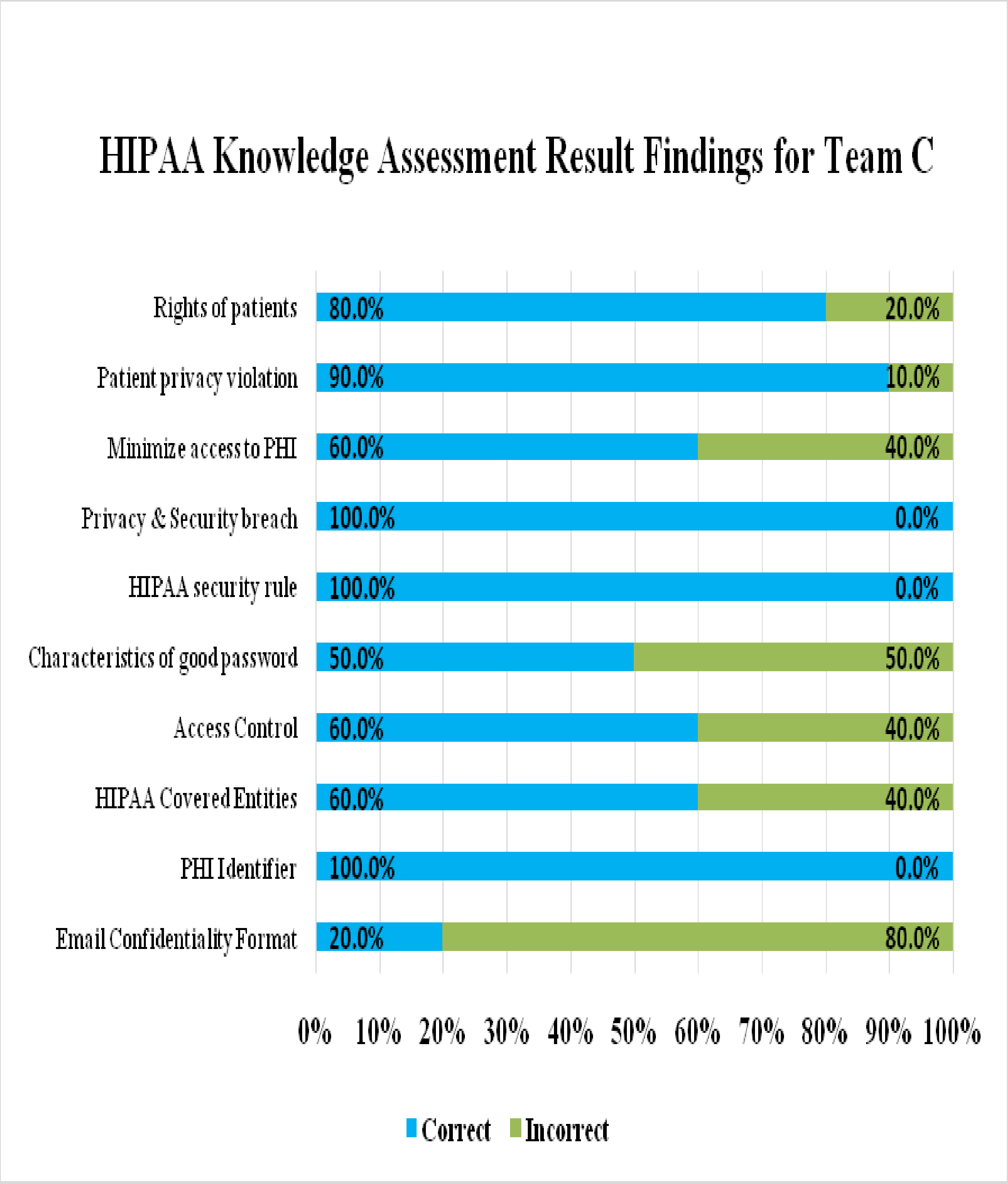
Score Range	No of Respondents
Above 90%	34
80%-90%	42
70%-80-%	24
Below 70%	12

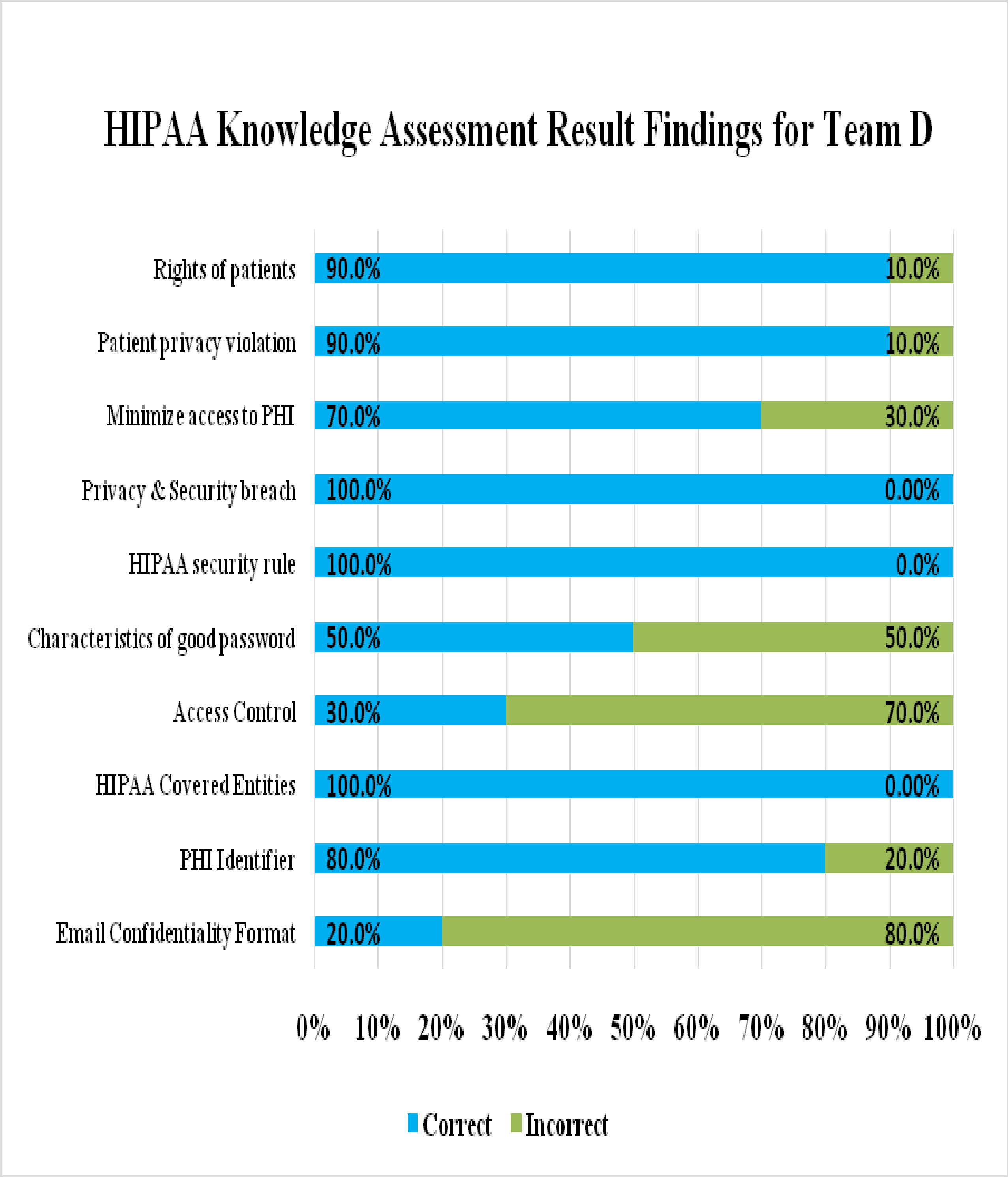
The result of the study group was grouped into four sections based upon the respondents score. The study shows that 68% of the respondents have scored more than 80% in HIPAA knowledge assessment. About 30% of the respondents have scored more than 90%.

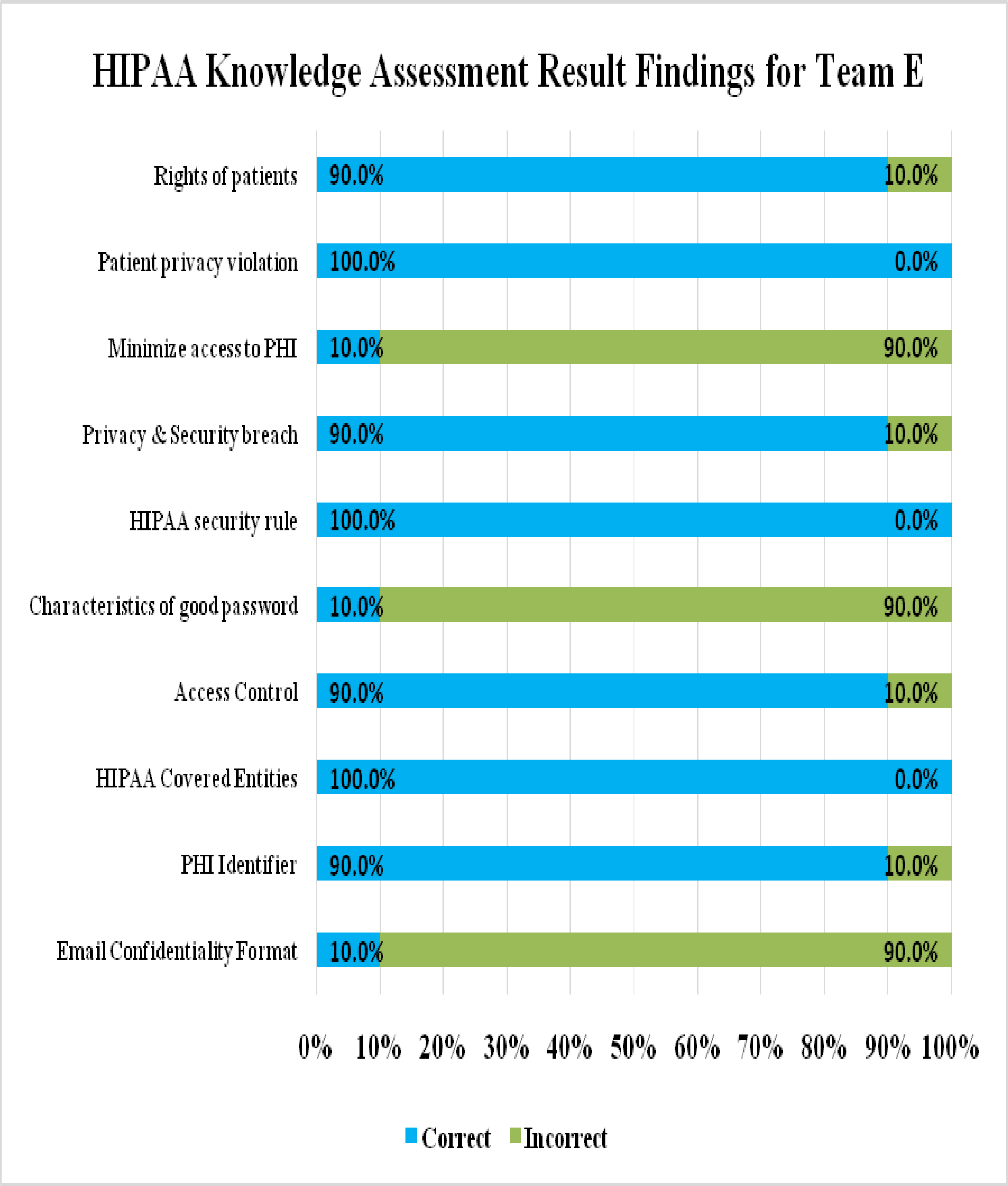
HIPAA Knowledge Assessment Result Findings for Support Employees




HIPAA Knowledge Assessment Result Findings for Team B

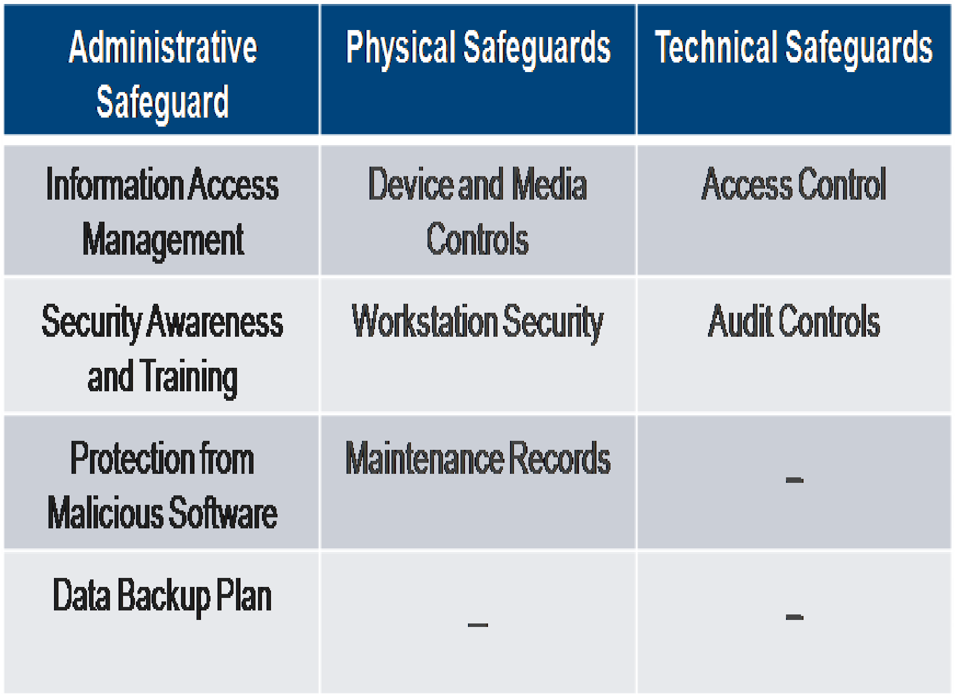
HIPAA Knowledge Assessment Result Findings for Team C
Rights of patients
80.0%
20.0%
Patient privacy violation
90.0%
10.0%
Minimize access to PHI
60.0%
40.0%
Privacy & Security breach
100.0%
0.0%
HIPAA security rule
100.0%
0.0%
Characteristics of good password
50.0%
50.0%
Access Control
60.0%
40.0%
HIPAA Covered Entities
60.0%
40.0%
PHI Identifier
100.0%
0.0%
Email Confidentiality Format
20.0%
80.0%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Correct
Incorrect


HIPAA Knowledge Assessment Result Findings for Team D
Rights of patients
90.0%
10.0%
Patient privacy violation
90.0%
10.0%
Minimize access to PHI
70.0%
30.0%
Privacy & Security breach
100.0%
0.00%
HIPAA security rule
100.0%
0.0%
Characteristics of good password
50.0%
50.0%
Access Control
30.0%
70.0%
HIPAA Covered Entities
100.0%
0.00%
PHI Identifier
80.0%
20.0%
Email Confidentiality Format
20.0%
80.0%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Correct
Incorrect


HIPAA Knowledge Assessment Result Findings for Team E
Rights of patients
90.0%
10.0%
Patient privacy violation
100.0%
0.0%
Minimize access to PHI
10.0%
90.0%
Privacy & Security breach
90.0%
10.0%
HIPAA security rule
100.0%
0.0%
Characteristics of good password
10.0%
90.0%
Access Control
90.0%
10.0%
HIPAA Covered Entities
100.0%
0.0%
PHI Identifier
90.0%
10.0%
Email Confidentiality Format
10.0%
90.0%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Correct
Incorrect

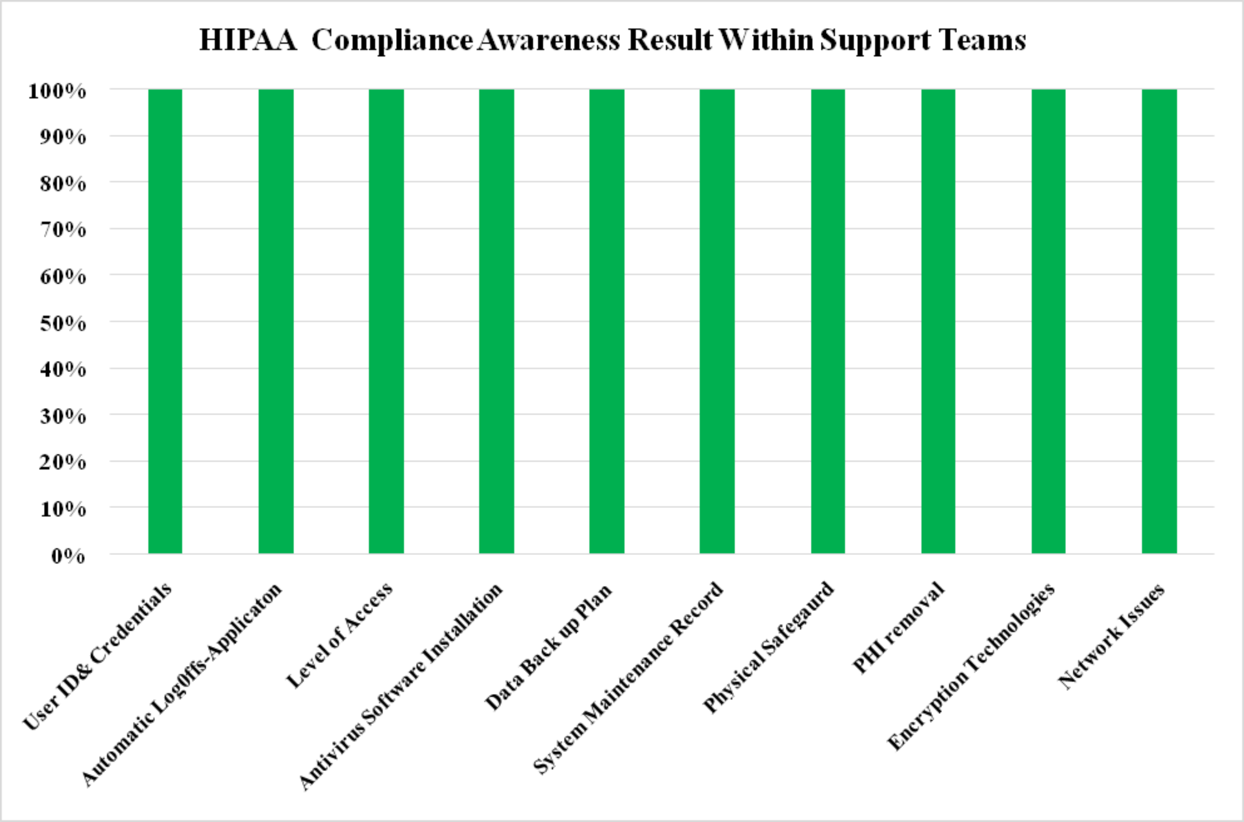
HIPAA Compliance Awareness Assessment for Support Employees

The Questionnaire for compliance awareness assessment is prepared on the standards of Physical Safeguard, Administrative Safeguards and Technical Safeguards and assessment has been done as per these standards only:



Administrative Safeguard	Physical Safeguards	Technical Safeguards
Information Access Management	Device and Media Controls	Access Control
Security Awareness and Training	Workstation Security	Audit Controls
Protection from Malicious Software	Maintenance Records	–
Data Backup Plan	–	–

HIPAA Compliance Awareness Assessment Result Findings for Support Employees



The Analysis is based as per the following observations:

- **User Id & Credentials:** To login into any system, application and network the user has to use his own credentials and password. (Technical Safeguard: Access Control)
- **Automatic Logoffs Configuration –Application:** If the application is kept idle for 30 minutes the user automatically gets logged off from the application. (Technical Safeguard: Access Control)
- **Level of Access:** Based on the level of delegation/position there all level of access to the application. (Administrative Safeguard: Information Access Management)

- **Antivirus Software Installation:** Automatic system updates are scheduled periodically to ensure the safety of workstation from threats and malware. (Administrative Safeguard: Protection from Malicious Software)
- **Data Back Up Plan:** Disaster recovery plans are implemented and followed as a quality document so that even if any disaster happens there is no interruption in the work due to data loss. A complete guideline is followed for the data backup plan. (Administrative Safeguard: Data Back Up Plan)
- **System Maintenance Record:** Audit trails are there in place which monitors and keep records of each & every activity. It is available for application, entry and exit in organization etc. (Physical Safeguard: Maintenance Record)
- **Physical Safeguard:** No pen drives and other storage devices can be used. No paper policy for patient information and data safety is being followed. (Physical Safeguard: Workstation Security)
- **PHI Removal:** PHI is not available easily. Its available only on client’s site and it can be accessed only if the support employees are getting incidents. At the point also only specific information is being displayed and if that information is being used all the details reviling patient information is being hidden or made blurred. Also no PHI is being stored on the system. (Physical Safeguard: Device and Media Control)
- **Encryption Technologies:** HL7, end to end encryption technologies are being used. (Technical Safeguard: Access Control)
- **Network Issues:** The network administrator gets notification about any abnormal activities in the network like hacking or other threats. (Technical Safeguard: Access Control)

HIPAA Compliance Awareness Assessment Result Findings for the Support Employees

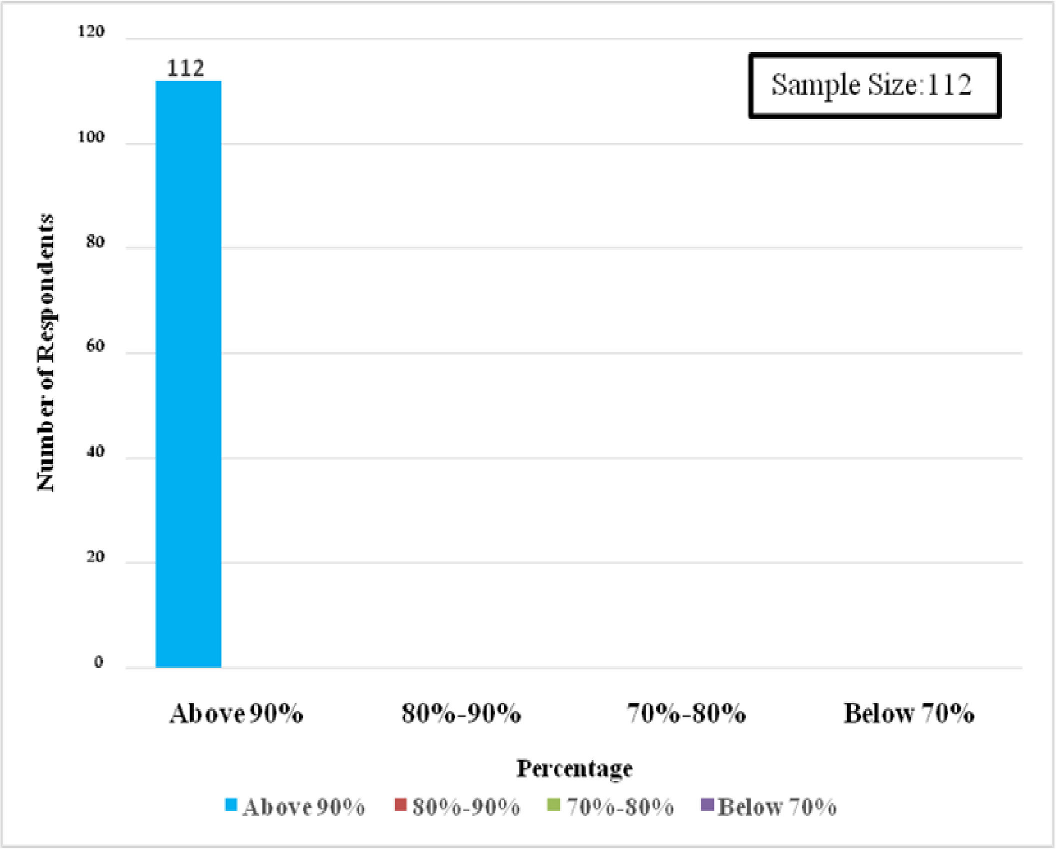
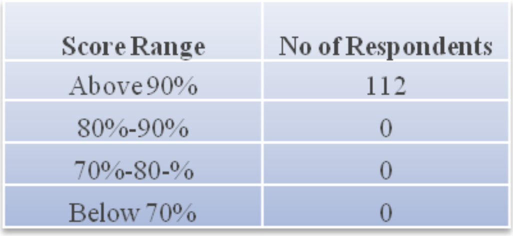


Figure No.4



Score Range	No of Respondents
Above 90%	112
80%-90%	0
70%-80-%	0
Below 70%	0

The result of the study group was grouped into four sections based upon the respondents score. The study shows that all the respondents have scored above 90% in HIPAA Compliance awareness assessment. This clearly indicates that the study group is very well aware of the measures that the organization is taking to abide by HIPAA privacy and security rules

7.0 Security Measures at the Organization

- Clear Desk And Clear Screen Policy

  - No critical information should be left lying in the work areas or left displayed on the screen when not in use
  - Desk space should be as uncluttered as possible.
  - Information when printed or transmitted through paper media must be cleared from the printers and fax machines immediately
  - Confidential and valuable information (soft and paper media) must be locked away in cabinets at the end of the day, or when desks are unoccupied
  - Clear the white board in a discussion/meeting room once the discussion is complete, don't allow un-authorized people to see the content scribbled on the board
  - The password protected screensaver will automatically engage after 15 minutes of inactivity

- User id and password dependent system authorization
- User id and password dependent VPN and application authorization
- Access management- No tail gaiting only authorized entry in work areas
- Audit trails for network/application access
- Secured work system, LAN cables, CPU cables.
- Unlicensed or unrequited software installation on machines is blocked
- Social Networking from secured network is blocked
- Use of removable storage disks/PD's is prohibited
- Secured laptops use with laptop locks, secured workstations
- Designated HIPAA compliance officer in the organization
- Security X-ray scanners at organization entrance to identify any unauthorized movement of systems, LAN's, storage devices etc.
- Security cameras at every entrance/exit

- No support staff is allowed access to production systems without successful completion of the HIPAA course. In addition this course has to be taken every year to maintain access to production systems.

8.0 Conclusion

Every Healthcare organization must address HIPAA compliance Requirements in terms of their unique business goals and technical environment. The organization offers the highest security standards to meet the stringent demands of all types of healthcare data interfaces and data transmissions. Every project resource should go for Induction program on Awareness of HIPAA and periodically knowledge check on same. Every organization must conduct annual HIPAA compliance audit should be done and if any gaps are found, remedial measures should be taken to ensure that these gaps are not repeated. This may also involve periodic process changes across the entire organization. Audit should also be conducted for the various business associates of the organization to ensure compliance.

9. References:

1) https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-implification/HIPAAGenInfo/downloads/HIPAAlaw.pdf

2) http://searchhealthit.techtarget.com/definition/personal-health-information

3) http://www.hhs.gov/sites/default/files/privacysummary.pdf

4) http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.pdf

5) http://www.hhs.gov/about/news/2013/01/17/new-rule-protects-patient-privacy-secures-health-information.html#

6) http://www.asha.org/practice/reimbursement/hipaa/electronic.pdf

7) http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

8) http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

9) http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

10) Erlen, J. (2007, March). HIPAA—Clinical and ethical considerations for nurses. Orthopaedic Nursing, 23(6) , 410–413

11) Swartz, N. A. (2003). What every business needs to know about HIPAA. The Information Management Journal, 37(2), 26–34.

12) Maddox P. J. HIPAA: Update on Rule Revisions and Compliance Requirements. MEDSURG Nursing.2003;12(1):59–63. [PubMed]

13) Smith, Harry E. “The HIPAA Final Security Rule-More Than a New Security Standard.” ISSA Journal (October 2003): 16-19.

14) Smith, Harry E. “The HIPAA Final Security Rule-More Than a New Security Standard.” ISSA Journal(October 2003): 16-19

15) http://www.cs.jhu.edu/~sdoshi/jhuisi650/papers/hipaapacsmedimage03.pdf

16) http://www.nationalacademies.org/hmd/~/media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftweb.ashx

17) http://www.oracle.com/technetwork/database/security/owp-security-hipaa-hitech-522515.pdf

18) http://www.cerner.com/solutions/White_Papers/HIPAA/

19) http://www.bu.edu/jostl/files/2015/02/Hiller_Web_171.pdf

20) https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/11399/Noyes-2011.pdf?sequence=1

21) http://tpcjournal.nbcc.org/wpcontent/uploads/2015/06/Pages_407%E2%80%93418.pdf

10. Annexure

Questionnaire for HIPAA Knowledge Assessment

NAME:

BADGE ID:

1. **How should an email containing confidential information be transmitted over the Internet to a destination that is external to the computer network?**
   a) Encrypt it first by putting the word [secure] in the subject line, using square brackets.
   b) Encrypt it first by putting the word {secure} in the subject line, using curly brackets.
   c) Place the words "private and confidential" in the subject line.

(Email confidentiality format)

2. **Which of the following can be termed as PHI Identifiers: Choose all that apply.**
   a) Health plan beneficiary number
   b) Biometric identifiers, including fingers and voice prints
   c) Medical Record Number (MRN)
   d) Social Security Number

(PHI Identifiers)

3. **Who is covered under HIPAA**?
   a) Clearinghouses
   b) Healthcare providers that transmit standard transactions electronically
   c) Health plans
   d) All of the above

(HIPAA covered entities)

4. **One of the required specifications of the access control standard is to**
    a) Use voice and eye recognition software
    b) Use encryption software
    c) Assign unique names and numbers to system users.
    d) Implement automatic logoff for computers

(Access Control)

5. **What makes a good password?**
    a) Using a wide range of characters
    b) Using mixed case in words
    c) Using mnemonics to help you remember passwords
    d) None of the above
    e) All of the above

(Characteristics of good password)

6. **Which of the following is true regarding a healthcare company complying with the HIPAA security rule?**
    a. The company has to disclose healthcare information when the media requests it in writing.
    b. The company doesn't have to train its workforce in security procedures.
    c. The only data that's actually protected in e-PHI are the patient names.
    d. The company has to protect its e-PHI against all reasonable threats.

(HIPAA security rule)

7. **How should an employee report a suspected privacy or security breach?**
    a) Tell your supervisor or privacy officer
    b) Fill out an occurrence report.
    c) Keep it to yourself so as not to make waves.
    d) Take it upon yourself to tell the patient that his/her privacy was breached.

(Privacy & Security breach)

8. What should be done to minimize access to PHI &/or personal identifying information on our computers?

a) Use passwords that have at least 10-12 characters, upper/lower case, alphanumeric and special characters

b) Never use dictionary words, birthdates or other easily obtained information

c) Always use the same password for all accounts

d) Use pass phrases rather than passwords

e) All of the above

f) a & b

g) a, b & d

(Minimize access to PHI)

9. What can happen to a person who knowingly violates patient privacy for personal gain or malicious harm?

a) Disciplinary action

b) Loss of access privileges

c) Fines and penalties

d) Imprisonment

e) All of the above

(Patient privacy violation)

10. True or False?

Under HIPAA, a patient has the following rights:

a) To receive a Notice of Privacy Practices.

b) To see or receive a copy of his/her protected health information (PHI).

c) To request that his/her PHI be corrected.

d) To ask for PHI to be sent to him/her at a different address or a different way.

e) To request limits on how his/her PHI is used and disclosed.

f) To receive a list of disclosures.

(Rights of patients)

Questionnaire for HIPAA Compliance Awareness Assessment

Name:

Badge ID:

Team:

1. **Are unique user id(s) in place/use (network and application)? Do you allow others to use your credentials?**
   - ○ Yes
   - ○ No

(User Id & Use of Credentials)

2. **Are controls in place and configured to allow for automatic logoffs in application?(Name the application)**
   - ○ Yes
   - ○ No

(Automatic Logoffs Configuration -Application)

3. **Are there rules established to determine the level of access an individual may have based on the delegation/roles?**
   - ○ Yes
   - ○ No

(Level of Access)

4. **Are procedures in place to make sure virus checking software is installed and running on all computer systems within the organization?**
   - ○ Yes
   - ○ No

(Antivirus Software Installation)

5. **Has a Disaster Recovery Plan been implemented and followed within your project team?**
   - ○ Yes
   - ○ No

(Data Back Up Plan)

6. **Does the organization retain system maintenance records?**
   - ○ Yes
   - ○ No

(System Maintenance Record)

7. **Has the project team implemented physical safeguards to eliminate or minimize unauthorized access/viewing of health information on workstations?**
   - ○ Yes
   - ○ No

(Physical Safeguard)

8. **Does the Project team takes care for the final disposition of electronic data (including PHI) if it resides on the hardware?**
   - ○ Yes
   - ○ No

(PHI Removal)

9. **Are access controls or encryption technologies used to secure transmission of sensitive information?**
   - ○ Yes
   - ○ No

(Encryption Technologies)

10. **Are software or hardware solutions in place that will provide notification of abnormal conditions that may occur in a networked system**
    - ○ Yes
    - ○ No

(Network Issues)