Arab American University – Palestine
Faculty of Graduate Studies

‘‘Assessment of Health Information Security and Privacy Protection in the Palestinian Ministry of Health’’

By

Mohammad Ahmad Salaheddeen

Supervisor
Dr. Rami Hodrob

Co-Supervisor
Prof. Mohammed Awad

This Thesis was Submitted in Partial Fulfillment of the Requirements for the Master’s Degree in Health Informatics

October/ 2021

Thesis Approval

"Assessment of Health Information Security and Privacy Protection in the Palestinian Ministry of Health"

By

Mohammad Salaheddeen

This thesis was successfully defended and approved on 02/10/2021 by the committee members:

Committee Members	Signature
Supervisor: Dr. Rami Hodrob	.....
Co-Supervisor: Prof. Mohammed Awad	....
Internal Examiner: Dr.Yosef almimi	....
External Examiner: Dr.Yosef daraghmeh	.....

Declaration

I hereby declare that I am the sole author of this thesis.

I acknowledge that what was included in this thesis is the product of my effort, except for what has been referred to, wherever it is mentioned, and that this letter as a whole, or any part of any other educational or research institution to whom it has not been submitted before for a degree or scientific or research title.

I am the undersigned submitter of the thesis with the title:

Assessment of Health Information Security and Privacy Protection in the Palestinian Ministry of Health.

Mohammad A. Salaheddeen

Signature: .....

Date: 02/ 10 /2021

Dedication

To my beloved parents; the reason for what I became today; they gave me lessons in otherworldly things,

To my cherished sisters and brother,

To the computer engineering members at the Ministry of Health,

To my supervisors and all who bolstered me in finalizing this work,

To those who made my thesis happen.

And most especially to our Almighty Lord our God.

This research is dedicated to you.

Acknowledgments

I would like to express my thankfulness to Almighty God who remains to give me his benedictions for studying.

I would like to express my deep gratitude to the Arab American University and to the Department of Health Sciences for providing me such a great opportunity.

I would like to thank my supervisors Professor Mohammad Awad and Dr. Rami Hodrob for their guidance and supervision on this thesis. I'm very grateful for their time and suggestions throughout the duration of this thesis.

My thanks go also to the Ministry of Health for funding my study.

I'm very grateful to my family, and co-workers for their encouragement, inspiration, love, and continuous support throughout the entire duration of my study.

Abstract

Background: Information systems have a significant role in healthcare organizations which deal with patients private and sensitive information, and as a result of the rapid widespread use of computers and the internet, information security has become one of the most considerable issues in the field of health information systems due to the increasing threats and the risks it causes.

Aim and objectives: The study aimed at assessing the level of health information security and privacy protection in the Palestinian Ministry of Health and Palestine Medical Complex (PMC) as a case study that may reflect the certainty of information security in the governmental hospitals, and the availability of the necessary administrative, physical and technical safeguards for the protection of health information systems, as well as evaluating the extent of application of information security and privacy protection of the health information system domains in MoH and PMC.

Methods: The researcher used the descriptive-analytical method, where the researcher developed two questionnaires; to investigate the administrative, physical, and technical safeguards in the Ministry of Health, and, likewise, the perceptions of the staff in the Palestine Medical Complex, where the researcher investigated seven (7) health security domains. The study was carried out between March 2020 and May 2021. Employees who work in the (MoH and PMC) were invited to participate in this study. Using the questionnaires, the MoH staff of the computer and engineering department sample consisted of 20 employees with a (100%) response rate, while (142) employees who have been working in the PMC were recruited using the random stratified method to select (142) out of (950) employees. The tool was a questionnaire derived from the previous literature. Furthermore, analyses were executed employing the statistical package for social sciences (SPSS).

Results and conclusions: The study displayed that the females were more representative than males (*n*=93; 57%) vs. (*n*=69; 43%) in both sites. In addition, the vast majority of the staff declared bachelors' degrees (*n*=104; 64.2%) vs. (*n*=30; 18.5%) higher than bachelors' degree level. Furthermore, (*n*=72; 44.4%) of the staff had up to 10 - 20 years of work experience. Computer and

engineering department staff specified that MoH applies security safeguards to maintain the security and privacy protection of health information at a high level (71.4%), with the physical security (75.5%), technical (73.8%), and administrative security (67.6%). Nonetheless, staff of PMC identified that the level of information security application to maintain the security and privacy protection of health information was at a moderate level (66.6%), with the business continuity planning 75.8%, development and maintenance of systems 70.2%, organizational policy 69.2%, security policy 68.8%, system access control 68.6%, personal security 58%, and data disclosure 61%. Moreover, the study revealed that there are positive significant statistical correlations at level ($\alpha \leq 0.05$) between all the fields of information security and the security and privacy protection of health information in MoH and PMC.

The study concluded a rate ranging from medium to high in the application of system security domains, in addition to security safeguards of security and privacy of health information in the Palestinian MoH and PMC.

Recommendations: Unify efforts between the computer and engineering department and all hospitals and to establish a unified information security unit to formulate, implement, update and monitor implementation of Health information security policy, and it is also necessary for health sector employees to constantly receive adequate training and education to reach a high level of information security awareness in the healthcare field. Furthermore, Designation chief information officer would help in managing and organizing all the security techniques and initiatives in health information systems.

Keywords: information security, privacy, health information system, hospital.

Table of Contents

List of Tables

List of Figures

Acronyms and Abbreviations

BCP	Business Continuity Planning
CIA	Confidentiality, Integrity, Availability
CT	Computed Tomography
DPA	Data Protection Act
GHI	Governmental Health Insurance
HI	Health Informatics
HIE	Health Information Exchanges
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIS	Health Information System
HR	Human Recourses
ISMS	Information Security Management System
IT	Information Technology
JICA	Japan International Cooperation Agency
MoH	Ministry of Health
MRI	Magnetic Resonance Imaging
PACS	Picture Archiving and Communication System
PECDAR	Palestinian Economic Counsel for Development and Reconstruction
PHI	Protected Health Information
PMC	Palestine Medical Complex
PNIPH	Palestinian National Institute of Public Health
PSQIA	Patient Safety and Quality Improvement Act
SEHR	Shared Electronic Health Record
SPU	Service Purchase Unit
UK	United Kingdom
USA	United States of America
USAID	U.S. Agency for International Development

CHAPTER ONE
INTRODUCTION

1.1 Overview

Health information system (HIS) is judged a key part of the healthcare system, on which all the processes of care delivery depend. It can provide substantial benefits to healthcare professionals, patients, and healthcare organizations (Khalifa, 2017). The health information system is "*the system in which collection, utilization, processing, storing, analysis, and transmission of information is done for performing health services, training, and research*" (Feyzabadi et al., 2015). It reinforces doctors, patients, nurses, and paramedical healthcare providers in diagnosing, treating, and subsidizing patients (Clark and McGhee, 2008). Information system plays the role in data processing in healthcare for the profit of hospitals (Shoniregun et al., 2010). It has many benefits, such as quicker access, effortless packing, and data viewing besides cost-effectiveness, user-friendliness, and more secure (Tezera, 2013).

Healthcare is a theme of life and death concerns. In such a considerable issue, patients have to confide in healthcare providers, and both patients and healthcare providers relying on the credibility of the information systems used. Inelegantly, privacy and security requirements are recurrently expressed in ambiguous, opposing, and complex laws and regulations (Clark and McGhee, 2008). It is a major concern that requires new approaches in systems design. Adopted HIS provides actual, high-quality sponsorship for providing the best care for patients but without conceding their privacy and security (Clark and McGhee, 2008).

Security and privacy have become a principal disquiet of diverse stakeholders, governments, users, systems managers, and service providers. These affairs are even escalating more in health information systems (Tan, 2005). Studies reveal that numerous healthcare associations are

susceptible to security outbreaks; since they encompass subtle and receptive patient information (Filkins et al., 2016). While patients trust their health providers if their information is kept private and secure, they are compelled to disclose information with their doctors to enable precise medical treatment, particularly to evade adverse drug interfaces. Nonetheless, this guides them to be more willing to discuss their feelings, illnesses, and risk comportments (Filkins et al., 2016). Nevertheless, patient data can be hacked, deployed, or devastated by users (external or internal) and cause inappropriate alteration of diagnosis results that can jeopardize patients' health or even life (Asress, 2014). Health information performs a chief task in piloting medical research for bettering healthcare quality. On the other hand, the revelation of health information for several reasons inflates disquiets about security and privacy (Tezera, 2013). The application of technological advances in information, telecommunication, and network have directed to the advent of an innovative new pattern for health care which is denoted as E-health (Van de Castle et al., 2004). Safeguarding the privacy and security of health information is the basic element to creating the trust prerequisite to apprehend the likely benefits of electronic health information interchange (Davidson, 2002). Moreover, concerns of the sensitivity of information security and privacy are increased annually as a result of several rising developments in healthcare, such as clinician mobility and wireless networking, health information exchange, and cloud computing (Abouelmehdi et al., 2017).

Health care organizations managed to safeguard personal information with strict protection regulations and policies. Based on web security standards, the USA, UK, and numerous countries had introduced data protection technical solutions such as; HIPAA Act and Patient Safety and Quality Improvement Act (PSQIA) HITECH Act in the USA, Data Protection Act (DPA) in the UK, Data Protection Directive (DPD) in the European Union (EU), Personal Information Protection and Electronic Documents Act (PIPEDA), the 09-08 Act, dated on

February 2009, and Russian Federal Law on Personal Data in Russia (Rodrigues et al., 2013). However, to prevent breaches of sensitive information and other types of security incidents, a proactive, preventive approach has to be taken by the healthcare organization (Abouelmehdi et al., 2017).

With the development of technology and the increase in security risks, new technologies may used to increase the protection of patient's medical files, reduce the opportunity for penetration, and enhance trust between the patient and the health service provider. Blockchain, a new technology that helps health care providers to ensure the integrity and safety of the patient's medical data by storing a single, immutable and decentralized copy of patient medical record. In addition to assign a key role to the patient in its development, updating,and modify it, and the responsibility for allowing its participation among health care providers, while keeping anonymized of patient's identity[El-Gazzar and Stendal, 2020; Tandon et al., 2020].

A massive quantity of data is recorded by individuals such as the registrars, physicians, and nurses, while other data are recorded by devices for instance laboratory and radiology machines, warehoused in one place, managed by one team, and can be easily accessed by any authorized by a member of staff. Health information data are precisely critical, private, and sensitive comprising personal information "names, addresses, telephone numbers" and other medical information for instance mental illnesses, substance abuse, genetic tests, and sexual diseases. Patients' data are viewed and edited by authorized personnel to provide the best health services, but in the ministry of health; educational hospitals, students, university researchers, outside medical consultations, and social relations contribute to improper use, leakage, or disclose of the medical data. Adopting such a large system with a sophisticated network and an enormous

number of employees dealing with very sensitive data necessities further effort and determination by decision-makers to safeguard the patient's data from unauthorized access or any type of breaches or hacking.

In Palestine, and since 2011, MoH has adopted –with USAID funding- an all-inclusive health information system to develop appropriate health informatics standards and an architectural framework for interoperability and scalability of the various eHealth initiatives in the country. This is being achieved to serve the patients in all the government hospitals to attain an integrated patient medical record that is shareable, flexible, and accessible in a timely way, considering all processes of daily health services workflow into a computerized system. The project has a well-placed international consortium that merges strong academic and industrial expertise in both computing and health to develop innovatively, integrated HI prospectuses, which serve hundreds of thousands of patients. Furthermore, HI saves and allocates resources, reduces costs, allows for the implementation of clinical decision support, and promotes health care quality (Palestinian Health Capacity Project, 2018).

The concern and responsibility of creating a general security policy are on the Palestinian Ministry of Telecom and Information Technology, which initiated a security policy based on the International Information Security Management System ISO 27001, and disseminated this policy to various ministries which should offer the human resources and financial needs to customize and implement this policy[1].

In this study, the level of security and privacy of health information in the MoH are assessed by gauging to which extent the personnel in the health sector are compelled to implementing security controls or their knowledge. In addition to their view of the role of the administration

[1] *https://www.mtit.pna.ps/ 2021*

and its interest in the security theme, the personnel involved in the application and dissemination of security policies and considering appropriate measures to ensure the availability of the optimum security level are assessed, as well as to measure the various security safeguards utilized by the Ministry's engineers and technicians who are in charge for developing, implementing and maintaining the various electronic systems in the ministry.

1.2 Justification and Significance of The Study

This study is considered a solitary study in this field. Hitherto, such a study -to the knowledge of the researcher- has not been formally or informally investigated in Palestine in the Health information security and privacy protection and its impact on the effective implementation of protection.

The rationale of this topic arises from the importance of the medical information of the health information system, which encompasses patient information, examinations, medications, sexual and genetic diseases, demographics, places of residence, and phone numbers. Any penetration, misuse, or disclosure of this information would jeopardize the patient's life, as it comes along with the efficiency and the correctness of the information entered, techniques, and procedures that provide the right and accurate information at any time it is needed. The top most justification for protecting personal privacy is to protect the interests of individuals. Moreover, the utilization of study conclusions and recommendations is important to identify the priorities and to recognize the gap between the real situation and the prospects in the field of information security, Data and its ability to deal with information security threats to which the security and privacy are exposed in Ministry of Health, in addition to identifying the types of threats, and contribute to overcoming and conquering them. The researcher is motivated to explore the fields of information security and privacy protection as one of these fields. Moreover, enriching the

Palestinian library, as this study sheds the light on an imperative aspect represented in the significance of the use of health information security and privacy protection, and their contribution to achieving information security.

Thus, the findings of this study, hopefully, will be advantageous for many categories in MoH including hospitals, medical teams, and policy makers. It will be used as a reference and a review to engineers and technicians, and researchers in the future. This study recommendation might be the basis for future planning and might assist in developing a policy or protocol for the MoH team and hospitals about health information security and privacy protection.

1.3 Problem Statement and Research Questions

This study tries to reveal the severe flaws in health information security and privacy protection in MoH. Moreover, the researcher has noticed -over years of practice in MoH and hospitals in Palestine- that medical information is valuable and accurate, and along with the work environment and day-to-day observations, it may be straightforward to obtain information by people who should not have access, as there may be a flaw in the policies and laws that would shelter this data in addition to a shortage of teams and a lack of awareness curriculums. It is also true that medical information is shared among physicians and other users. For instance, in some cases, end-users of medical information may need medical information with a clear identity of the patients. Nevertheless, physicians may take an overall conclusion on shielding the privacy of the patients. Consequently, they may encode the names of all the patients before providing the information to the end-users. Such conflicts of interest continuously occur.

Another concern is that the security and privacy regulations were not fully adopted by the ministry of health or not followed or recognized by the staff, which could lead the patient's data to be breached or disclosed. This necessitates the development and implementation of privacy

laws and regulations, and confidentiality, and security framework for safeguarding personal health information.

Accordingly, privacy and security in health data and information security and privacy protection is the crucial point, where the main study question comes ahead: **What is the level of security and privacy protection of health information in MoH and PMC?**

This thesis aims to assess the level of health information security and privacy protection in the Palestinian MoH and PMC.

To this end, this study endeavors to survey and address the following research questions.

1. How far is the availability of administrative security for health information protection in the MoH from the point of view of the computer and engineering department staff?
2. How far is the availability of physical security for health information protection in the MoH from the point of view of the computer and engineering department staff?
3. How far is the availability of technical security for health information protection in the MoH from the point of view of the computer and engineering department staff?
4. What are the aspects of security and privacy protection of health information in the MoH from the viewpoint of the Palestine Medical Complex staff?

1.4 Aim and Objectives of the Study

1.4.1 Aim of the Study

This thesis aims to assess the level of health information security and privacy protection in the Palestinian Ministry of Health.

1.4.2 Specific Objectives

- To assess the adopted policies and regulations from MoH to protect health information systems.
- To assess the availability of the necessary administrative, physical, and technical safeguards for the protection of health information systems.

- To evaluate the extent of application of security domains in MoH and PMC.

1.5 Hypotheses of the Study

Hypothesis (H01): MoH applies security safeguards to enhance the level of health information security and privacy protection in MoH.

However, the following sub-hypotheses were derived from the first main hypothesis:

(**H01-1**)**:** Administrative safeguards are applied in MoH.

(**H01-2):** Technical safeguards are applied in MoH.

(**H01-3):** physical safeguards are applied in MoH.

Hypothesis (H02): Important security and privacy domains of health information are applied in MoH from the viewpoint of Palestine Medical Complex staff.

Moreover, the following sub-hypotheses were derived from the second main hypothesis:

(**H02-1):** There are policies applied for the security and privacy protection of health information in the MoH from the viewpoints of Palestine Medical Complex staff.

(**H02-2):** The organizational security for the security and privacy protection of health information is applied in the MoH from the viewpoint of Palestine Medical Complex staff.

(**H02-3):** The employees are qualified to maintain the security and privacy protection of health information in the MoH from the viewpoint of Palestine Medical Complex staff.

(**H02-4):** There is control over access to systems to maintain the security of the privacy of health information protection in the MoH from the viewpoint of Palestine Medical Complex staff.

(**H02-5):** Systems are developed and maintained to have the security and privacy protection of health information in the MoH from the viewpoint of Palestine Medical Complex staff.

(**H02-6):** There is a business continuity planning (BCP) to maintain the security and privacy protection of health information in the MoH from the viewpoint of Palestine Medical Complex staff.

(**H02-7):** The patient data are not disclosed from the viewpoint of Palestine Medical Complex staff.

1.6 Thesis Outline

This thesis structure has been systematized as follows; Chapter 1 dealt with an introduction, background, and how the researcher considers the concepts in this current study as a term of reference, problem description, objectives, and hypotheses to answer. Chapter 2 the clinical research as literature review covered patient privacy and data security and related works in this area. Then, the methodology chapter presented the methodology and methods describing how the expedition was undertaken to do this research, as well as the framework used for this research chapter 3. Next, in chapter 4, an analysis of the findings and results are outlined, while finally, chapter 5 is displaying the discussion, limitations, and strengths of the study, conclusions, and recommendations.

1.7 Summary

This introductory chapter provided an overview of the importance of the health information system (HIS) providing substantial benefits to healthcare professionals, patients, and healthcare organizations. Moreover, an overview of the study aims and objectives is; to assess the level of health information security and privacy protection in the Palestinian Ministry of Health, to assess the adopted policies and regulations from MoH to protect health information systems, and the availability of the necessary administrative, physical and technical safeguards for the protection of health information systems. Furthermore, this chapter included the rationale of

this topic, as well as the security and privacy that have become a principal disquiet of diverse stakeholders, governments, users, systems managers, and service providers which were all collectively encompassed within the study problem.

CHAPTER TWO
THEORETICAL FRAMEWORK

2.1 Overview

In this chapter, the concept of information security is defined in conjunction with the concepts of the security triad. The interrelated terms of information security are then described and important standards in this area are discussed. Moreover, the most important electronic schemes in the MoH are reviewed, along with government institutions responsible for drafting laws, legislation, and security policies.

2.2 Health Information

Information is defined as any meaningful data, where assets are anything that has value to the organization including the information, the importance of the information comes from the sensitivity of it which increases the value it and enlarge the dangerous of breaching it (Kaospilot, 2005). Personal health data are included in the category of "sensitive" or "special nature" within the personal data category. Protecting this confidentiality is necessary in terms of protecting the right to privacy of persons who have medical data. Clearly 'health information' is a particularly sensitive subset of personal information, thus justifying the privacy concerns relating to the emergence of SEHR systems (Sahma et al., 2013).

PHI stands for Protected Health Information. is a term given to health data generated, obtained, stowed, or conducted by HIPAA-covered entities and their business associates with regard to the delivery of healthcare, healthcare operations, and disbursement for healthcare services. Secure health information is often abbreviated to PHI, or in the case of electronic health information, ePHI. It narrates to an individual's health conditions, medical services, or payments and the information is sufficient to identify someone, identifiable means. There's an

unbiased root to believe the information can be used to detect the individual e.g., name, address, birth date, and social security number. PHI includes electronic media and other forms of media including paper, audio recordings, and digital images (CMS, 2016).

In line with ISO, 27799 presents steps for organizations to perform an information security standards and practices counting the assortment, application, and application of controls depending to the information security risk. health information to be protected comes in different types like personal health information, research and statistical data, public health surveillance data, health staff data, medical knowledge, and health information system security data (Hamidovic and Kabil, 2011).

2.3 Information Security and Privacy

Numerous definitions of the privacy concept are applied in the literature; the right to be alone, or the right of the individual to avoid others (individuals, organizations, or the government) having access to personal information (Rognehaugh, 1999). 'Information privacy' refers to the capability of a person to exert discipline over their data controlled by others. Information privacy involves the use, maintenance, collection, and disclosure of 'personal information': in the case of medical information, any item of information that may reveal a person's identity should not be viewed, published, or shared without the patient's consent and authorization or with the consent of a legal representative in case of young age or mental disorders (Ozair et al., 2015). Privacy protection is the framework within which security and confidentiality are maintained (Rinehart-Thompson and Harman, 2006).

Information security is not only about the protection from unauthorized access, information security is "*basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information*" (Alhassan &

Adjei-quaye, 2017), taking into consideration the protection of data from inadvertent or improper use, and data unavailability due to system failure and user errors (UNAIDS, 2007).

The information security code [ISO / IEC 27001] defines the term as follows: Information security "*is the protection of information from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities*" (Ormandjieva et al., 2012).

Security and privacy of patient health information are decisive to improving systems and configurations that reinforce the interchange of information among healthcare providers, payers, and consumers using Health Information Exchanges (HIE), and to assure concealment and confidence of the physician-patient relationship. The E-Healthcare information proposes exceptional security, privacy, and confidentiality approaches that necessitate an active examination of the conventional perceptions and methods to information security. If patients did not have the equitable security safety measures primed to defend their information, or the confidence that their privacy will be preserved, they would care for their privacy on their own, such as repudiate to permit to use of personal health information for research purposes, or not pursue treatment, or Refrain from disclosing dangerous information (McGhee, 2008).

2.4 Information Security Risks, Threats, and Vulnerabilities

The information facilities are constantly exposed to and susceptible to many different threats.

A threat is a process or event that has the potential to disrupt the reliability of an object like breaches, disclosures, unauthorized access, errors, misuse, and system failure. The extent to which the information provided is sensitive to threats depends on the vulnerability of the information provided to a specific threat, the vulnerability defined weakness in assets, which can be exploited through the threat to harm like unprotected network, poor password

management, lack of monitoring, lack of security awareness, and unstable power source. The sensitivity arises because one or more objects of the information provision make it possible that one or more threats lead to a negative influence on one of the reliability aspects “availability, integrity, and confidentiality”. (eHealth Ontario, 2010)

2.5 Information Security Elements (CIA)

Information security is the process of protecting information from unauthorized access, use, disclosure, destruction, alteration, or damage. The basic elements of information security are: confidentiality, integrity, and availability, this trio is briefly called CIA (Figure 2.1).

Figure 2.1: The Confidentiality, Integrity, and Availability (CIA) triad (Oza, 2019).

These elements are basically as follows:

2.5.1 Confidentiality: It aims to prevent unauthorized access to information. The information must be protected from unauthorized access, both when processing in computer systems (process), when stored in storage media (storage), and when moving between the sender and

receiver (transport) on the network. The point to be considered in this principle is not to ensure that the information is completely hidden, but in an unauthorized way to prevent it from being obtained and to be informed when it can be accessed (Popescul, 2011).

2.5.2 Integrity: The aim is to keep and preserve the information as it should be. It aims to prevent the distortion of the information, its modification, the addition of new data, and the deletion partially or completely. For this purpose, the realization of access control for critical information and backup periodically must be realized (Popescul, 2011).

2.5.3 Availability: It is the principle that aims to make the information (data, source, system,) accessible and usable during the determined, expected, targeted, needed time and to make it complete. It aims to protect information systems against performance threats that may come from within and outside the organization (Popescul, 2011)**.**

2.6 Risk Management

Generally, the risk is considered a negative situation or danger. It is defined as the probability of an event occurring and the possibility of being affected by the event. Risk management covers three processes: risk assessment, risk mitigation, and risk evaluation. Risk management is the procedure that permits IT managers to equalize the operational and economic costs of defensive actions and accomplish gains in mission capability by protecting the IT systems and data that support their organizations' missions (Stoneburner et al., 2002). Therefore, harm from the negative effects of risks taking into account the possibilities for not seeing, a discipline that is called risk management has emerged which includes taking measures, working and planning activities. Risk management has an essential role in protecting healthcare information assets as healthcare facilities using digitalize information systems to process information to improve the services (NIST, 2012).

On the other hand, risk management is the process of determining, measuring, and reducing the risk factors that can affect the profitability of an institution or organization and primarily for business organizations. In risk management, it is not possible to eliminate the risk. It is aimed to prevent unnecessary losses through a systematic and careful approach to the problems and careful management of the risks decided to take. For efficacious risk management, it is imperative to identify and analyze the risks regarding the information assets and targets of the organizations, and to monitor the classified risks under control, while the most accurate approach of managing the risk is to conceive an information technology risk management process that will lessen the risks with the highest opportunity of realization and the highest damage it will instigate (Ranong and Phuenngam, 2009).

2.7 Health Information Security Policy and Standards

The health care organizations must manage and safeguard personal information with policies and regulations, the Countries have shown great interest in the security and privacy of medical information by adopting regulations and enacting legislation and aspects that will strengthen the security and privacy of medical information:

There are various standards and frameworks in the field of information security. In this section, there will be a depiction of the most commonly used standards and frameworks in the context of the research.

1-**The Health Insurance Portability and Accountability Act (HIPAA).**

HIPAA "*Health Insurance Portability and Accountability Act*", Health Insurance Portability and Responsibility Instruction; It sets rules on the conditions under which health information can be accessed by healthcare professionals and other organizations to ensure the security of personal health information (James, 2007).

HIPAA, which has been in force in the USA since 1996, includes the necessary sanctions (such as fines and imprisonment) for the unauthorized use and disclosure of personal health information, including procedures and protocols restricting access to health records. It includes some administrative, physical, and technical standards that increase the security of personal health information. Confidentiality, integrity, and availability of personal health information should be guaranteed according to HIPAA security rules. Measures should be taken against any unauthorized access that may threaten the integrity of personal health information and/or endanger its confidentiality and privacy. Security rules were developed to deal specifically with electronically protected health information and working on three types of security warranties: administrative, physical, and technical (James, 2007)

Each person is concerned about their health confidentiality and wants to keep up with them as a secret. trustworthiness must apply to the doctor and patient's relationship. However, some professionals are delegated with the most personal patient information like health information and interpretation distinctiveness. These data contraventions will enlarge substantial significances not only for the patient but for the healthcare industry as well. Therefore, guarding health information is both important and difficult. As well as quality, healthcare organizations use information technology to amend effectiveness (Takura and Jomin, 2019).

Administrative Measures: Supervision of health institutions (health plans, health clearing offices, organizations operating in the health sector), classification of accessibility, regulations; management of selection, development, implementation procedures. It includes the maintenance of security measures necessary for the protection of personal health information and the management of the necessary workforce to ensure security (Hoffman et al., 2015).

Physical Measures: It defines the physical precautions; the procedures required to protect and control the relevant structures in case of natural and environmental hazards and/or unauthorized access (Hoffman et al., 2015).

Technical Measures: It defines the technical precautions It includes procedures, technologies, regulations,it Control access to computer systems and enable covered entities to protect communications containing PHI transmitted electronically over open networks (Hoffman et al., 2015).

2-The ISO/IEC 27000-series (also known as the Information Security Management System ISMS Family of Standards.

The ISO 27000 series ('ISO27K' for short) foresees very comprehensive processes regarding "information security", which can be expressed as ensuring the confidentiality, integrity, and availability of information. In this series; while ISO / IEC 27001 sets the specifications for an Information Security Management System, ISO / IEC 27002 is the application code for Information Security Management which represents the guidelines for information security standards and management practices considering the organization's information security risk environment (Win and Susilo, 2015). The ISO 27799 standard is related to health informatics and regulates how to perform information security management in the health sector using ISO / IEC 27002. It integrates quite a few informal rules that empower to decrease the expanding number of threats, resolves existing security issues, and improve the security targets in general [Fenz et al., 2016; Kovalenko et al., 2018].

ISO 27001 consists of 114 controls organized in 14 sections covering the breadth of information security management including:

"*Information security policies, Organization of information security, Human resource security, Asset management, Access control, Cryptography, Physical and environmental security,*

Operations security, Communications security, Supplier relationships, Information security incident management, Information security aspects of business continuity management, Compliance, and System acquisition, development, and maintenance".

The standard requires organizations to compare the measures they have implemented with the standard controls, then expected to implement the missing controls

ISO 27799 also includes detailed standards for taking all necessary precautions and keeping them under security in the stages of shaping, storing, and sharing health information. At the same time, applying relevant international standards can provide the necessary security requirements for healthcare organizations and health information protectors, depending on their size and situation (Flaumenhaft and Ben-Assuli, 2018).

The ISO 27799 standard, which is related to the health system, regulates how it integrates into the health system by taking physical security measures to safeguard the information, access, unauthorized access, theft, and damage. The operation of standard procedure, processes, exceptional situations, delays, interruptions, failures is determined and documented. Moreover, technical or organizational changes are checked. Before the potential effects on the operations of information technology systems are applied, security events are analyzed, evaluated and imperative developments for the security systems are determined. In conclusion, by taking appropriate measures to fulfill, data security requirements are arranged in a verified manner, specified in the data protection standard, and information is secured. Irrespective of the form of information (spoken, sound recordings, drawings, video images, medical analysis results, etc.), whatever medium found in (printed or electronic media), or whatever tools are used for the transfer of information (fax, computer networks, mail, etc.), they all have to be well protected (Farn et al., 2007).

2.8 MoH Information Systems

In 2011 with cooperation between USAID and MoH, the idea of computerizing Patient medical files has begun in all governmental hospitals affiliated with the MoH, the first phase started in three main hospitals, which are Rafidia, Alia and PMC , which required the establishment of a main datacenter in the PMC and the disaster recovery site in Rafidia hospital, in addition to providing data connection lines, Internet lines, creating computer networks in all hospitals, as well as distributing computers in all hospitals departments and wards, to be followed by the process of installing and operating the health information system, training health care staff , creating employees accounts and giving them the necessary privileges, along with providing 24/7 technical support

Upon completion of the project, The Engineering and Computer Unit at the MoH abides to improve the configuration of health information system in the Ministry, throughout the development of existing systems, or the construction of new computerized ones. Moreover, MoH IT staff is assured to the provision of technical support essential for the work immovability of these systems, as well as working on the preparation of numerous types of infrastructure needed to confirm the stability of the operational services in the different facilities of the ministry, and empowering citizens for these services as well, to reach 13 fully computerized hospitals, serve hundreds of thousands annually “253,000 patients PMC alone”, as well as more than 2.5 million computerized medical record in the health information system database as a whole by the end of 2020(Alhelou, personal communication, 2021).

In this part, the researcher will investigate the MoH information systems hosted in the main data center in PMC which is managed by the MoH team and serves almost all MoH facilities.

2.8.1 Avicenna: The health information system which was funded by the United States Agency for International Development (USAID) in 2011 was developed by a Turkish company and deployed by a local one. The system is a desktop application connected to an application server settled in the main data center in the PMC. It is a three-phase deployed system, functions in thirteen (13) governmental hospitals and 4 public health care centers. Furthermore, the system epitomizes the main data source of health information in MoH and encompasses almost all patient medical records. These records include diagnoses, visits, doctors' and nurses' notes, lab tests, radiology tests, drugs, pathology, physiotherapy, and financial issues, in addition to managing the kitchen, laundry, maintenance, stores, transportation, purchasing, and sterilization. Further, the system provides MoH departments with looked-for reports about the activities and procedures of the hospitals and centers. Besides, it is integrated with the referral, PACS, and Qlik systems.

The Ministry team is entirely in charge of the day-to-day operations (Alhelou, personal communication, 2021).

2.8.2 Stradus: represents the PACS" Picture Archiving and Communication System", is a web-based system funded by JICA in 2018, installed in thirteen (13) MoH hospitals, archives all X-Rays, CT, Ultrasound, and MRI pictures for five years. It is integrated with Avicenna and could be accessed at anytime, anywhere, and from any authorized persons from the link[2]. The system is installed locally in each hospital while pictures are saved locally, synced to the main storage in the main data center as well as to the Microsoft cloud. However, the system is developed, installed, maintained by a local company, and can be accessed from the link:[3] (Alhelou, personal communication, 2021).

[2] *https://view.stradus.com/*
[3] *https://view.stradus.com/*

2.8.3 HR: Human resources system is a web-based system, funded by USAID in 2011, developed by an international company, installed by a local one, and managed by the MoH team. However, the system's objective is to organize the human resources-related works such as employees' profiles, their vacations, leaves, and their timesheets. It can be accessed from the link[4]:

2.8.4 Pharmacy: a web-based system developed, installed, and maintained by the MoH team, with the purpose to enhance the performance of the General Administration of Pharmacy. It comprehends the related laws and regulations, essential drug lists and prices, reports, and warnings. It can be accessed from the link[5]:

2.8.5 Moodle System: it is an E-learning system installed in the main datacenter by Al-Quds Open University developers, maintained and supported by the MoH team, with the purpose to activate electronic learning. It offers online courses, training, and exams for medical students in the ministry. It can be accessed from the link[6]:

2.8.6 GHI: Government Health Insurance is a web-based system funded by the Palestinian Economic Council for the Development and Reconstruction (PECDAR), with the purpose to create an insurance system to serve the people. The Government Health Insurance (GHI) project was established in 1994 to provide the Palestinian population with health insurance coverage. It is linked with the Ministry of Interior, Ministry of Social Affairs and any related ministry to facilitate the flow of information between ministries. The system is still under testing by a local firm, while the servers are installed and configured by the MoH team.

---

[4] *http://me.moh.ps/MenaITech/application/hrms/mename/index.php*
http://hr.moh.ps/MenaITech/application/hrms/menahr/index.php
[5] *http://pharmacy.moh.ps*
[6] *http://moodle.moh.ps/*

2.8.7 E-Referral: electronic medical referral is a web-based system that was funded by the United States Agency for International Development (USAID) in 2016, to ease the communication between the Service Purchase Unit "SPU" in the ministry, and the public hospitals "referring hospitals" from one side and between the private hospitals" referred hospitals" and SPU from the other side, moreover, it seeks to facilitate the provision of services for Palestinian patients outside the public health system on time. The system can be accessed from the link[7]: The Service Purchase Unit (SPU) at the Ministry of Health (MoH) has received technical support from the USAID-funded Palestinian Health Capacity Project (PHCP) since 2014 to streamline referral services and improve communications with all referral facilities, with specific highlighting on referrals to hospitals. The SPU developed the first version of the referral guidelines document in 2014 (MoH, 2016). These guidelines have served as an important tool for the SPU and other PMOH staff throughout the referral workflow process. More in recent times, the PMOH and SPU implemented further refinements to the referral process that required documentation. Unfortunately, the link is not functioning[8]:

2.8.8 Qlik: is a web-based system, funded by Intra-Heath in 2016, the system was installed in the main data center by a local firm, and managed by the MoH team, with the purpose to supply the needed reports about the HIS system automatically and send them periodically to pre-defined emails to the hospital Administrative and Financial Affairs and diverse departments in the ministry. The system can be accessed from the link[9]:

[7] *http://ereferral.moh.ps/*
[8] *https://spu.moh.ps/.*
[9] *https://qlik.moh.ps/.*

2.8.9 Covid19 results is a web-based system developed, installed, and managed by the MoH team. The system was initiated post COVID19 pandemic and aims to display the results of COVID19 tests. It can be accessed from the link[10]:

2.8.10 PNIPH E-Registries: PNIPH Established in 2012 by the corporation between Palestinian Ministry of Health (MoH), the World Health Organization (WHO), and the Norwegian Institute of Public Health (NIPH), it focused on the development of health systems and e-registries in order to improve the public health functions which translated in funding, developing, and managing the following registries:
Cause of death e-registry, Cancer e-registry, Mammography e-Registry, Road Traffic Accidents & Injury Prevention e-Registry, and Family Practice, which are all installed in the MoH datacenter (PNIPH, 2021).

2.9 Information Security in Palestine

The Palestinian Basic Law presented a clear interest in information security, as its enacted laws and legislations that would preserve information from any penetration, sabotage, confusion, disclosure, or wrong use, through the so-called Cybercrime Law (Decree-Law No. (16) of 2017 regarding electronic crimes, 2017). This Decree-Law was issued in 61 clause clarifying articles for:

1-Anyone who intentionally and unlawfully penetrated any means of a website, system, or electronic network, or bypassed the authorized access.
2-Anyone who hindered or disrupted access to the service, or access to equipment, software, data resources, or information, by any way, through the electronic network or any of the information technology tools.
3-Any person who introduced or produced by the electronic network, or by using any means of information technology, that would stop it from working, or disrupt, or destroy programs, delete them, destroy them or modify them.

[10] *https://result.moh.ps/.*

4-Whoever captures, records, intercepts, or intentionally wiretaps what is sent through the networks or any means of information technology.

5-Anyone who intentionally decodes encrypted data in circumstances other than those authorized by law.

6-Every employee who perform any of the crimes defined in this Law, by taking advantage of his powers and authority during the performance of his work, or because of it, or facilitating that for others.

The Ministry of Telecom. & Information Technology is the second body in the Palestinian National Authority which is concerned about information security. The Council of Ministers initiates the basics for the general policies of information security to all ministries and governmental institutions. It consists of eight domains (Ministry of Telecommunications and Information Technology, 2017):

- Administrative responsibilities: which cover the administration responsible for information security policies, standards, circulars, procedures and their applications, reviewing and monitoring.
- Physical security: which deals with environmental security, equipment security, and physical access to the Data Center, and securing backup media.
- Access control security: which covers access control security, data access control, personality verification, privacy, identification, manage user privileges, manage passwords, network access, and documenting events.
- Information security: it includes data privacy and how to protect the data from disclosure, and it ensures the encryption mechanism and covers the backup procedure.
- Application security: includes the policies of developing and maintaining applications, managing and controlling settings.
- Communication and network security: it covers protection of networks, internet and email security, deal with sever computer viruses and malicious codes, management of software and patch files, and wireless network security.
- Security risk assessment and auditing: it relates to scheduling and implementing periodic risk assessments, as well as arranging for third-party information systems evaluation.
- Security incident management: where the security events are monitored and the security incidents are resolved.

2.10 Summary

In this chapter, the basic concepts regarding to the domain of the study were presented in terms of health information and the security and privacy of medical information. The risks, threats, vulnerabilities, and basic elements of information security were defined, in addition to the most popular international regulations and standards.

The researcher also reviewed the most important electronic systems in the Palestinian Ministry of Health, in addition to the laws and initiatives established by the Palestinian government to preserve all electronic information.

CHAPTER THREE
LITERATURE REVIEW

3.1 Overview

The present review displays an upsurge in the number of research studies completed on health information security and privacy protection in the healthcare system. Nevertheless, an extensive literature review did not reveal so many studies, which focused on health information security and privacy protection such as our study. Local, regional, and international studies related to information security are reviewed.

3.2 literature Review

3.2.1 Local Studies

1. A study conducted by Tayeh (2008) in Gaza, Palestine, aimed at "*identifying the extent of the effectiveness of information security management in forty-one Palestinian information technology companies*" (Jerusalem, West Bank, and Gaza) by investigating ten domains. The researcher explored the differentiation in implementing the information security management and concluded that all the fields except organizational security affect the effectiveness of information security management in those companies. Furthermore, there were no differences between the information security management attributable to the history company in the fields of IT, yearly security budget, company main working field, years of staff experience, operating systems, and staff qualifications. The study recommended advising the information security IT companies to improve incident management plans to deal with developed security incidents with compliance to legal requirements and enhance employees' training as well as to develop a procedure to measure the incidents costs and volume.

2. Another study was carried out in Gaza by Hassan (2013) to investigate "*the impact of information security management on the effectiveness of applying e-management in the governmental organizations in the Gaza Strip*". Using a questionnaire as a tool to collect data, eight (8) governmental organizations were allocated to this purpose using ten (10) domains with a (91%) response rate. However, the study concluded that the effectiveness of information security management in the Gaza governmental organizations was rated about (65%), while the effectiveness rate of applying e-management in these governmental organizations assayed about (74.5%). Moreover, there was a noticeable weakness in the fields of organizational and personnel security, compliance with legal requirements, and the classification of assets.

In addition, there was a significant correlation between the fields of information security management and the effectiveness of applying e-management in Gaza governmental organizations. The study recommended establishing a cross-functional forum of management representatives from pertinent portions of the situation to match up the implementation of information security controls, directing the government to wield more efforts headed for the feeble information security fields, as well as informing all employees about the latest updates of the procedures and policies of the institutional information security.

3. Al-Danaf (2013) fulfilled a study in the Gaza Strip aimed at identifying the actual situation of information systems security management in six (6) Technical Colleges and how to improve it. Using the analytical descriptive method, the researcher used questionnaires and interviews as tools with a (79%) response rate. The study concluded that the entire technical colleges did not have any written IS policy, while few colleges knew about this issue. More than 92% of the studied sample had declared that colleges use computerized health information systems at a relatively high level. Moreover, information system IS infrastructures are available at an intermediate level in these colleges, as well as there were significant differences between

technical colleges in the application of information security management due to the age, the experience of staff, training levels, and rate of the security budget. The researcher recommended creating and improving an information security policy in the technical colleges, as well as increasing the financial information security budget and the training capabilities of employees in the security fields. Moreover, the study recommended improving the contract conditions with IT-Outsourcing vendors.

3.2.2 Regional Studies

1. A study was conducted by Abd Aljaber (2013) aimed at "*investigating the degree of effectiveness of internal control procedures in providing electrical information security in Jordanian manufacturing companies using electronic accounting information systems in reducing security risks*". Besides, the study exposed the likely obstacles that restrict the efficiency of internal control in these companies. Three groups of risks were classified (hacking, social engineering, and malware), besides, the study highlighted the efficacy of internal controls in preventing and identifying these risks and improving the situation in case of their manifestation. Using questionnaires, the study population consisted of information technology staff, internal auditors, and accountants who were recruited in thirty random sample manufacturing companies functioning in Jordan managing electronic accounting information systems. The researcher distributed (145) questionnaires and recovered (72) questionnaires with a (50%) response rate. The study results showed that internal control procedures used by the companies were commonly operational in preventing and identifying risks related to hacking, social engineering and malware, and in rectifying their effects in case of their incidence. Furthermore, the findings showed statistically significant differences in views of the study sample that may be due to the respondent's job nature, professional experience, and possession

of a professional certificate, and to the company's size and affiliation with an international company. Moreover, the results displayed the presence of impediments and challenges facing the application of effective internal control procedures, including the quick development of electronic fraud methods and the lack of management support for the activities of internal controls related to information security. The study recommended including management support for the activities of internal control over information security through the provision of qualified staff and encouraging them to attain related professional certificates.

2. The study of Mishnah et al. (2019), was carried out in Saudi Arabia with the objectives to assess the state of electronic security and cyber-security level in Saudi hospitals, and to determine the extent to which hospitals are prepared for any potential threats that may affect patient privacy, health data confidentiality, and EHR availability and integrity. The researchers Mentioned that Saudi Arabia has a widespread of adaption different EHR systems which could expose the health facilities to high-risk threat. In addition, they mentioned that Saudi Health institutions have begun to develop security settings and update policies and procedures to prepare and prevent any electronic attacks, leaks, sabotages, or disruptions of computerized health systems. The researchers have developed and distributed a questionnaire to hospitals located in seven different Saudi regions, it covers the network, servers and storage, policies and procedure, computer department, power supply, backup plan, policies, and procedures. The study concluded that a few hospitals have a high and moderate e-security measure, tools, and procedures to achieve the best level of security and the vast majority have poor security level which needs a very fast intervention.

3. The study of Al-Gharbi et al., (2015) was conducted to review health information systems in Oman and to assesses the axes of the used system in terms of security, performance and

effectiveness. The study discussed the security features of the Al-shifaa health information system. They mentioned in their literature that almost all major health institutions in Oman adopted a computerized health system, and the MoH is the main provider of health service in Oman and has a comprehensive health system called Al-Shifaa. Al-Shifaa system is characterized by being comprehensive of all elements of the medical file in one screen, where privileges are given according to the tasks assigned to the employees. The system protects patient information from improper use by setting limitations and controls to read, write and delete. The system is designed to comply with the basic principles of safety, namely CIA, as the system is isolated from the Internet and does not allow the use of a USB or cd. Moreover, the system is protected from unauthorized access by using a complex and powerful username and password and the employee does not have access to un allowed privileges. To achieve high availability, redundancy was used for the important elements in the system. The record of changes to the patient's file is maintained by time and date.

4. Karasneh and colleagues (2019) piloted a descriptive, cross-sectional study about “Patient data sharing and confidentiality practices of researchers in Jordan”. The researchers explored to assess the knowledge and practices of healthcare workers regarding medical information security and data sharing, about the medical data retrieved for research purposes, Targeting all medical field researchers in academic institutions in Jordan, a questionnaire-based survey was used, and included three (3) sections which are: personal information, "experience, age and affiliations", knowledge of research ethics, and security techniques and practices "access to information, storage and delivery". The results showed substandard performance due to information security between researchers from various health sectors. They found that researcher team could have a medical data more than the study needs. More than a third of the respondents claimed that managers do not know about the protection techniques or do not

adhere to them, as well. They are allowed to store this information on their personal computers in addition to using their USB to transfer the information. The researchers claimed that the medical information is not encrypted. Accordingly, the study concluded that such practices endanger health information and reduce confidence between the patient and the health institution. The study recommended that healthcare providers and lawmakers must work hard and fast to issue regulations to protect electronic health information by controlling data sharing, access, and transfer.

3.2.3 International Studies

1. Yarmohammadian and coworkers (2010) conducted a descriptive and comparative study in Iran, aiming to compare the laws and security policies for medical information between Iran from first side and some developed countries from the other side; "The United States, Australia, Malaysia, and England", and worked to identify the points of convergence and differences between them. The researchers used the description and comparison method, where the data were collected through extensive searches in the Internet and libraries, in addition to communication from experts in the field of information security. The study concluded that the aforementioned countries are responsible for enacting legislation and laws related to information security, and based on these laws comes the role of hospitals in developing policies and procedures to translates these laws in protecting medical information. In comparison with the state of Iran, there are no specific written policies or procedures regarding the leakage of medical information, although there are few laws and policies that come in the form of letters and bylaws. The researchers concluded that the legal authorities should enact the laws and legislation necessary for the use of medical information, and more studies should be done regarding the disclosure of medical information.

2. Eroglu and Cakmak (2016) performed a study in Turkey aimed at assessing the information system in health organizations by measuring the security and risks and determining the gaps in the used assessment tools and information security applications to improve the health organization. The researchers employed an international Information Security Assessment Tool for State Agencies and the data were collected by interviewing health information security and information system managers. The tool consisted of questions that covered five domains: organizational reliance, risk management, staff, processes, and applications. The researchers found that the threats resulting from the system bugs had adverse effects on the processes, identity, and culture. In addition, bugs may cause loss of the values and quality of services provided. They also found that there was a shortage of security policies and procedures, and staff vulnerability who use the system which needs training and support from the organization. To conclude, post analyzing the results, they assessed that the health institutions is in a good security level, where the infrastructure and the technical side rose to a strong level, but they still need to enhance the regulations and decisions.

3. Mehraeen and colleagues (2016) executed a survey study aimed at assessing many Iranian university hospitals regarding the information security safeguards " administrative, technical, and physical". The study targeted (36) IT managers in these hospitals using a four-section questionnaire. The result showed a strong level of technical and physical security and a moderate level of security regarding administrative safeguards. The respondents agreed that the access policies to data could be changed over time, However, the patient right to access to their medical data weren't identified clearly, besides the lack of the sanction over illegal data access. Regarding access control, furthermost of the IT managers noted that IT staff could easily determine the user's identity. However, the system access sessions have no time limit. The

researchers recommended increasing the staff training, developing security policies, applying access control rules, and Implement appropriate penalties against unauthorized access to data.

3.2.4 Comment on Previous Studies

The preceding studies that have been reviewed in this topic have focused on the issuance of health information security in particular, because of its significant role in the efficiency and quality of the performance of health institutions and the strengthening trust between patients and service providers. The researcher has educed from the previous literature in forming a clear depiction of the health information security setting in the Arab and foreign countries in general, in addition to enriching the theoretical and conceptual framework in developing the study tool. Furthermore, in the explanation of the current study results throughout analysis and comparison with the previous studies' results. Previous literature fluctuated in terms of objectives, some of which focused on reviewing the laws and procedures followed, others aimed at comparison with developed countries, while some converged-on threats and risks. Nevertheless, all of them were to improve health information security, consequently, a variety of methods were used to accumulate information, including questionnaires, interviews, research, previous literature, description, and comparison methods. This study was in concordance with some previous studies' results, nonetheless, was inconsistent with some others. The researcher justifies this as a result of the dissimilarities in the societies, and the variance in the time period in which these studies were conducted.

3.3 Summary

In this chapter, the researcher presented some important local, global, and regional studies related to the topic of research, which served as a road map in identifying the study tools, and also helped him in analyzing the results and linking them with each other.

In addition to evaluating the information security situation in the Palestinian Ministry of Health with other countries and health institutions.

CHAPTER FOUR
METHODOLOGY

4.1 Introduction

The methodology and procedures of the study are considered the principal part through which the applied aspect of the study is achieved. The data required to perform the statistical analysis are obtained to achieve the results that are interpreted, and thus, to attain the goals that the study pursues to accomplish. This chapter explore the approach used in the development of the study tool, the community and the sample of the study, as well as the development of the questionnaire, and the extent of its validity and reliability. Lastly, the statistical management that the researcher relied upon analyzing the study.

4.2 Study Design

Based on the nature of the study and the goals it seeks to achieve, the researcher used the descriptive-analytical method, which depends on the study of the phenomenon as it exists in reality and is interested in describing it as an accurate description and expresses it in a quantitative expression. Also, this approach is not satisfied when collecting information related to the phenomenon to investigate its various manifestations and relationships, but goes beyond it to analysis, linking, and interpretation to reach conclusions on which the proposed vision builds to increase the balance of knowledge about the topic.

This approach was chosen because the study aimed at quantifying the opinions about the assessment of health information security and privacy protection for employees working in Palestine Medical Complex, and employees in the computer and engineering department at the MoH.

4.3 Sources of Information

However, two main sources of information been used:

4.3.1 Primary Sources: the researcher used a well prepared questionnaire designed specially to the topic of the study as a best way to collect the primary data to reflect the analytical aspect of the study.

4.3.2 Secondary Sources: To address the theoretical aspects, the researcher has used the related Arabic and English books, articles, magazine, websites, reports, other studies and researches which represents the secondary data sources.

4.4 Study Population

The researcher had recruited all the employees of the two sites; the entire staff members totaling twenty (20) employees constituted the computer and engineering department at the Ministry of Health, and nine hundred and fifty (950) employees in the Palestine Medical Complex in Ramallah.

4.5 The Study Sample

The researcher used the random stratified method to select (142) employees working in the Palestine Medical Complex in Ramallah from the year 2020, while all employees in the computer and engineering departments responded to participate in the study. Tables 5.1 and 5.2 show the characteristics of the demographic samples.

4.6 Study Period

The study was carried out between March 2020 and May 2021.

4.7 Study Tools

A two-page written questionnaire booklet was constructed for each facility (Palestine Medical Complex, and the computer and engineering department at the Ministry of Health) from

literature and other studies questionnaire designed consisting of short and direct questions, which requiring a tick answers. The questions were designed to assess the health information security and privacy protection for employees working in Palestine Medical Complex, and employees in the computer and engineering department at the MoH. The current study used the community survey method for computer and engineering department employees, and by sample for Palestine Medical Complex employees, and the questionnaires as tools to collect data and information about the study population. The study tool was developed due to literature, previous studies, books, scientific references, and thesis related to the current study site, to assess the health information security and privacy protection for employees in the MoH, where the researcher developed two questionnaires as follows:

4.7.1 Computer and Engineering Department Staff Questionnaire

As the computer and engineering department in the MoH manage responsible to install and develop every system in the ministry and provide day-to-day technical support for all the governmental hospitals, a questionnaire has been developed to cover -the-scenes security measures and techniques. Appendices (B, C).

The questionnaire enclosed three main parts. The first part consists of the consent form, which contains a brief explanation of the topic of the study, in addition to the participants' appreciation for allocating part of their precious time, emphasizing the need for credibility in answering the questions. The second part consists of socio-demographic questions in order to determine the characteristics of the sample in terms of age, gender, educational level, in addition to the job title. The third part aimed to investigate how much the assessment of the health information security and privacy protection the employees have, which consists of questions from 5-33 cover three safeguards which are: administrative, physical, and technical safeguards.

4.7.2 Palestine Medical Complex Questionnaire

As healthcare workers don't know much about the technical issues, the researcher developed another questionnaire after adequate literature review. The structured questionnaire was applied to ten (10) employees as a pilot assessment, which was used to identify problems and to evaluate the ease and level of the questionnaire.

It was observed that there was no problem in understanding the questionnaire which was distributed in both Arabic and English languages to the same sample, and the results were completely identical.

The questionnaire form consists of two parts. Questions 1-4 in the first part are about the personal characteristics of the participants. Questions numbered 5-34 in the second part are questions about information security. The questionnaire covers 7 domains which are: security policy, organizational security, access control, personnel security, business continuity planning (BCP), systems development and maintenance, and data disclosure. (Appendices D, E).

4.8 Validity of the Questionnaire

The truthfulness of the questionnaire is intended to measure the questionnaire questions of what they were designed to measure, and the researcher verified the validity of the questionnaire in two ways:

4.8.1 Arbitrators Validity "virtual honesty"

The researcher designed the questionnaire in its initial form, and then to verify the validity, he presented it to the supervisor and to a group of specialized arbitrators consists of six specialists in the field of information security and statistics to show their suggestions, and their names are listed in Appendix (A).

The researcher followed their suggestions and made all the required modifications to brought out the questionnaires in their final form.

4.8.2 Internal Validity (internal consistency)

The validity of the tool was also verified by calculating the Pearson correlation coefficient for the study items with the total score for each field of study

The validity of the tool was also verified by calculating the Pearson correlation coefficient for the study items with the total score for each field of study, where there is a direct relationship between the pearson correlation coefficient and the strength of the validity of the study tool,as the value of pearson correlation coefficient increase , the validity of the study tool increase to achieve what was set for it , as shown in table. (Table 4.1).

Table 4.1: Pearson correlation coefficient results for the study paragraphs.

The scale of PMC staff			**The scale of Computer and engineering department staff**		
No.	**Pearson correlation coefficient**	**P-value (sig.)**	**No.**	**Pearson correlation coefficient**	**P-value (sig.)**
1	0.873	0.000	1	0.562	0.010
2	0.920	0.000	2	0.556	0.011
3	0.854	0.000	3	0.609	0.004
4	0.868	0.000	4	0.610	0.004
5	0.887	0.000	5	0.585	0.007
6	0.648	0.000	6	0.740	0.000
7	0.535	0.000	7	0.506	0.023
8	0.652	0.000	8	0.616	0.004
9	0.822	0.000	9	0.545	0.013
10	0.780	0.000	10	0.550	0.012
11	0.793	0.000	11	0.315	0.176
12	0.760	0.000	12	0.284	0.225
13	0.455	0.000	13	0.747	0.000
14	0.700	0.000	14	0.460	0.041
15	0.762	0.000	15	0.709	0.000
16	0.782	0.000	16	0.642	0.002
17	0.498	0.000	17	0.562	0.010
18	0.627	0.000	18	0.795	0.000
19	0.457	0.000	19	0.811	0.000
20	0.648	0.000	20	0.843	0.000

21	0.692	0.000	21	0.689	0.001
22	0.595	0.000	22	0.661	0.002
23	0.475	0.000	23	0.843	0.000
24	0.531	0.000	24	0.756	0.000
25	0.278	0.000	25	0.717	0.000
26	0.632	0.000	26	0.680	0.001
27	0.750	0.000	27	0.532	0.016
28	0.570	0.000	28	0.748	0.000
29	0.648	0.000	29	0.576	0.008
30	0.492	0.000	30	0.721	0.000
31	0.263	0.002	31	0.612	0.004
32	0.620	0.000	32	0.568	0.009
33	0.565	0.000	33	0.456	0.043
34	0.293	0.000			

The data reported in Table 4.1 signify that the matrix correlation values of the questionnaires' paragraphs of the computer and engineering department staff, and the Palestine Medical Complex staff are statistically significant ,The p-values (Sig.) "in total "are less than 0.05, so the correlation coefficients of all field are significant at $\alpha = 0.05$, so it can be said that the items of this field are consistent and valid to be measure what it was set for which indicates the strength of the internal consistency of the tool paragraphs and that they jointly measure health information security and privacy protection in MoH from their point of view.

4.9 Questionnaire Reliability

The reliability of the questionnaire is intended to give the questionnaire the same result if the questionnaire is redistributed more than once under the same circumstances, or in other words the stability of the questionnaire means stability in the results of the questionnaire and not to change it significantly if it redistributed several times during periods given time.

The researcher verified the consistency of the study's questionnaire through Cronbach's Alpha Coefficient. Table 4.2 indicates that the consistency values of the study tool among computer and engineering department employees reached (93.3%), and among Palestine Medical

Complex employees it was (86.7%), and thus the tool (the questionnaire) had a high degree of consistency, and can be adopted to achieve the study objectives.

Table 4.2: Cronbach's Alpha results for both questionnaires.

Scale	No. of population	Number of Questions	Cronbach Alpha coefficient
The scale of Computer and engineering department staff	0.933	33	20
The scale of PMC staff	0.867	34	142

4.10 Study Phases

1. Defining the subject of the study, which is to identify the information security and privacy in the Palestinian Ministry of Health.

2. After confirming the validity of the study tool, the researcher printed and distributed (20) questionnaires to the staff of the computer and engineering department in the Palestinian Ministry of Health. Moreover distributed (142) questionnaires directed to the employees of the Palestine Medical Complex.

3. The male and female employees filled out the questionnaires with what was required, then the researcher collected the questionnaires after verifying the required data.

4. The researcher unloaded the data and entered it into the SPSS program to analyze and extract the results.

4.11 Statistical Methods

Following amassing the questionnaires and the study data, and ensuring their validity for analysis, the researcher reviewed them in formulation for entering them into the computer to perform statistical treatment of the data. They were entered into the SPSS program by assigning certain numbers to them, that is, by converting the verbal responses into digital values, indicating the response as strongly agree (5), agree (4), neutral (3), disagree (2), and strongly

disagree (1), so that the higher the degree, the greater the level of information security and privacy in the Palestinian Ministry of Health. (Table 4.3).

A descriptive analysis was applied to designate the participants' characteristics; frequencies and percentages to describe demographic variables and detect subjects' responses towards statements of all domains, as well as means to determine how far the degree and agreement of each response of the study variables. Furthermore, The standard deviation was calculated to determine the dispersion for each phrase of the study variables along with main domain, the closer they are to zero, the more concentrated responses and the lower their dispersion. Moreover, using the analytical method, the relationships between dependent and independent variables were attained using independent samples T-test, and tabular-T. The researcher deemed ($P \leq 0.05$) as significant. Data were put in and tested using the SPSS version 23 (SPSS Inc., Chicago, Illinois, USA).

4.12 Study Variables and Conceptual Framework

4.12.1 Independent Variables: administrative security, physical security, technical security, security policy, organizational security, personnel, and information security, controlling access to systems, developing and maintaining systems, BCP, and data disclosure.

4.12.2 Dependent Variable: security and privacy protection of information in the Palestinian Ministry of Health.

Figure 4.1: Conceptual framework of the study.

4.13 Scale Correction (the key to the statistical means of the study results)

A five-point Likert scale was used, which is a method for measuring behaviors and is used in questionnaires, especially in the field of statistics. The scale is based on responses indicating the degree of agreement or disagreement to the security and privacy protection of health information in the Palestinian Ministry of Health, based on arithmetic averages as in Table 4.3.

Table 4.3: Correction scale.

Mean	Magnitude	Degree	Category
1:00-1.80	1	Very low	Strongly disagree
1.81-2.6	2	Low	Disagree
2.61-3.4	3	Moderate	Neutral
3.41-4.20	4	High	Agree
4.21-5	5	Very high	Strongly agree

4.14 Ethical Consideration

The participants' recruitment has initiated with the researcher attaining the ethical approval from the Deanship of Scientific Research of Arab American University, as well as from MoH. Moreover, the researcher invited the staff of the MoH to participate in the research project being conducted in the PMC and MoH. The researcher has made it clear to them that their partaking is voluntary, and it is up to them to decide whether to take part in this study, but, before they agree, they needed to understand what the research implicates, and they are assured that their participation will not be disclosed.

4.15 Summary

This chapter deliberated the methodological approach used to undertake this study. This included; methods of data collection and analysis, in addition to the tools and samples of the study, as well as the questionnaires used. Methodological choices were evaluated and justified. Furthermore, tests of validity and reliability of the questions used in the questionnaire data analysis and ethical consideration were also included. Additionally, obstacles and difficulties in collecting or analyzing data encountered by the researcher were described.

CHAPTER FIVE
RESULTS

5.1 Overview

This chapter presents the results of the survey, including the characteristics of the respondents in addition to the survey items with the values of basic statistic terms "means, percentages, ranks, degrees, and standard deviations" which helps in answering the study question. In addition, the results of the hypotheses are presented. To the best of our knowledge, this is the first survey conducted in Palestine to assess the health information security in Ministry of Health. The results of this comprehensive survey may reveal the inaccurate protection of health information in the Ministry of Health and confirm previous studies assessing the security and privacy of health information in the Ministry of Health.

5.2 Sample Characteristics

The Table 5.1 shows that the males were more representative than females (*n*=13; 65%) vs. (*n*=7; 35%). In addition, analysis of the respondents' level of education showed the vast majority of the staff declared bachelors' degrees (*n*=16; 80%) vs. (*n*=4; 20%) higher than bachelors' degree level. Furthermore, (*n*=10; 50%) of the staff had up to 10 - 20 years of work experience. Finally, more than half (*n*=11; 55%) specified they are programmers.

Table 5.1: Characteristics of the computer and engineering department staff (*n*=20).

Variable	Sub-variable	Frequency	Percent %
Gender	Male	13	65.0
	Female	7	35.0
Education	Bachelor	16	80.0
	Master	4	20.0
Experience	Less than 10 years	8	40.0
	10-20 Years	10	50.0
	More than 20 years	2	10.0
Job Title	Programmer	11	55.0
	Engineer	6	30.0
	Information Technologist	3	15.0

The current study included a total of (950) employees, from whom a total of (142) completed the questionnaires (participation rate 15%). As shown in Table 5.2, females were more representative than males (*n*=86; 60.6%) vs. (*n*=56; 39.4%). Besides, analysis of the respondents' level of education displayed the vast majority of the staff declared bachelors' degrees (*n*=88; 62%). Furthermore, (*n*=62; 43.7%) of the staff had up to (10–20) years of work experience. Finally, less than half (*n*=60; 42.3%) specified they are nurses.

Table 5.2: Characteristics of the Palestine Medical Complex staff (*n*=142).

Variable	Sub-variable	Frequency	Percent %
Gender	Male	56	39.4
	Female	86	60.6
Education	Diploma	28	19.7
	Bachelor	88	62.0
	Master	26	18.3
Experience	Less than 10 years	55	38.7
	10-20 Years	62	43.7
	More than 20 years	25	17.6
Job Title	Doctor	21	14.7
	Nurse	60	42.3
	Registration	12	8.5
	Lab Tech	17	12.0
	Rad Tech	10	7.0
	Pharmacist	7	4.9
	Administration	10	7.0
	Others	5	3.5

5.3 Answering Study Questions

The researcher used the basic statistical tests " mean, percentage and standard deviation "to analyze the questionnaire items and one-sample T-test to test the validity of the hypotheses. The paragraph is considered positive, meaning that the sample members agree to its content if the calculated t-value is greater than the tabular t-value which equals 1.98, (or the significance level "p-value" less than 0.05) while the paragraph is considered negative, meaning that the sample

members do not agree to its content if the calculated t-value was smaller than the tabulated t-value which equals -1.98, nonetheless, attitudes of the sample to the paragraph are neutral if its significance level was greater than 0.05.

5.3.1 What is the level of security and privacy protection of health information in the MoH and PMC?

To answer the previous question, the means, percentages, and standard deviations of the level of security and privacy protection of health information in the MoH were extracted. (Table 5.3). Data displayed in Table 5.3 indicate that the security and privacy protection of health information in the MoH viewed by the computer and engineering department employees had a high degree, with (M = 3.57), (71.4%), and (SD = 0.60), while those who work in PMC had a moderate degree where (M = 3.33), (66.6%) with (SD = 0.46).

Table 5.3: Level of security and privacy protection of health information in the MoH.

Scale	Mean	Percentage%	S. D	Degree
The level of security and privacy protection of health information in MoH from the viewpoint of the computer and engineering department staff.	3.57	71.4	0.598	**High**
The level of security and privacy protection of health information in MoH from the viewpoint of the PMC staff.	3.33	66.6	0.460	**Moderate**

The main study question was divided into the following sub-questions:

5.3.1.1 The first sub-question: how far is the availability of administrative security for health information protection in the MoH from the viewpoint of the computer and engineering department staff?

To answer the previous question, the means, percentages, and standard deviations of the extent of administrative security availability of health information in the MoH were extracted from the viewpoint of the computer and engineering department staff in order of importance. (Table 5.4).

Data displayed in Table 5.4 indicate that the most important aspect of administrative security for health information protection in MoH was “There is a strict policy for the password, such as specifying the minimum length, nature, and validity of this word, in addition to having instructions explaining how to choose it” ranked in the first order, where (M = 4.50), and (90%). However, ranked in the last order “There are clear and effective policies in place to assess gaps and weaknesses in the information security system” evenly with “There is a defined and recognized entity responsible for drafting, reviewing, and updating information security policies”, with (M =2.40), and (48%). Generally, there is a notion that the total value of the availability of administrative security for health information protection in the MoH from the view point of the computer and engineering department staff was with a moderate degree, where (M = 3.38) and a general percentage 67.6%. See Table 5.4.

Table 5.4: Availability of administrative security viewed by computer and engineering department staff.

Rank	Item No.	Item Question (Administrative security)	Mean	%	S. D	Degree
1	9	There is a strict policy for the password, such as specifying the minimum length, nature, and validity of this word, in addition to having instructions explaining how to choose it	4.50	90	0.688	Very High
2	12	There is a system for monitoring the network, the servers, and the main devices operating the system	4.25	85	0.786	Very High
3	7	All privileges related to the information system will be canceled in the event of the employee’s transfer or resignation immediately	3.95	79	0.759	High
4	6	The employees are given privileges based on their job description and their daily tasks and upon the request of the management	3.90	78	1.294	High
5	8	It is forbidden to share passwords between employees or divulge their confidentiality	3.90	78	1.165	High

6	14	Backups are performed at regular intervals	3.80	76	0.768	High
6	11	Anti-virus and virus removal programs are used and these programs are constantly updated	3.80	76	0.768	High
7	3	Formal disciplinary action applies to employees who violate the hospital's information security procedures and policies	3.40	68	0.883	Moderate
7	15	Backup activities are reviewed regularly	3.40	68	1.095	Moderate
7	13	There is a plan to return the business to normal after a system failure or interruption in business performance	3.40	68	1.188	Moderate
8	16	The backup and recovery mechanisms are documented and examined periodically and properly implemented	3.10	62	1.165	Moderate
9	4	Employees are required to sign an undertaking not to disclose medical information as part of their terms of employment	2.70	54	1.174	Moderate
10	1	All potential security risks, including threats and vulnerabilities to applications and information systems, are identified	2.65	53	0.988	Moderate
11	10	All staff receive appropriate information security training and are kept informed of the latest updates on the hospital's information security policies and procedures	2.60	52	1.273	Low
12	5	There is a defined and recognized entity responsible for drafting, reviewing, and updating information security policies	2.40	48	1.231	Low
12	2	There are clear and effective policies in place to assess gaps and weaknesses in the information security system	2.40	48	1.046	Low
Total Domain Degree			**3.38**	**67.6**	**0.592**	**Moderate**

5.3.1.2 The second sub-question: how far is the availability of physical security for health information protection in the MoH from the viewpoint of the computer and engineering department staff?

To answer the previous question, the means, percentages, and standard deviations of the availability of physical security for health information protection in the MoH were extracted from the viewpoint of the computer and engineering department staff, arranged in order of importance, as shown in Table 5.5.

The data shown in Table 5.5 indicate that the most important aspect of the physical security of health information protection in the MoH is "Rooms that contain devices and information are closed or have secure lockers that can be closed", had (M = 4.30), with (86%), while the least important was "The computer screen is locked manually or automatically when not in use for a while" had (M = 3.30), with (66%). The total value was high in its degree with a mean (3.79) (75.8%); this means that the physical security for health information protection in MoH from the view point of the computer and engineering department staff is available.

Table 5.5: Availability of physical security viewed by computer and engineering department staff.

Rank	Item No.	Item Question (Physical security)	Mean	%	S. D	Degree
1	19	Rooms containing devices and information are locked or have secure lockers that can be locked	4.30	86	1.081	Very High
2	18	Data centers and information departments are set up in good and secured places and locations	4.20	84	0.894	High
3	17	physical security standards are applied to all devices responsible for operating the system to prevent unauthorized access	3.95	79	1.050	High
4	22	The hospital has a backup generator as well as energy storage devices "UPS"	3.90	78	0.912	High
4	20	Information is only available based on need, meaning that there are controls in place to control the entry of outside personnel	3.90	78	1.119	High
5	23	all types of workstations that access HIS data have been identified, such as laptops, desktop computers	3.80	76	1.196	High
6	21	There is a list of people who are allowed access to data centers, computer rooms, and the list is reviewed and updated periodically	3.65	73	1.137	High
7	26	Backup media containing basic or sensitive information is placed at a safe distance from the main site to avoid damage from a disaster in the main site.	3.50	70	0.946	High
8	24	Data storage devices that contain sensitive data are disrupted or become unnecessary by being destroyed or overwritten	3.40	68	1.188	Moderate

9	25	The computer screen is locked manually or automatically when not in use for a while	3.30	66	1.342	Moderate
Total Domain Degree			**3.79**	**75.8**	**0.802**	**High**

5.3.1.3 The third sub-question: how far is the availability of technical security for health information protection in the MoH from the point of view of the computer and engineering department staff?

The data depicted in Table 5.6 indicate that the most important aspect of technical security for health information protection in MoH was "System logged out automatically after a predetermined time of inactivity", where (M = 4.05), with (81%), while the least important one was "There are audit control mechanisms that can monitor, record, and/or examine the activity of the information system" with (M = 3.20), and (64%).

The results of this domain (technical security) demonstrate specifically that the total value was high with a mean (3.69) and (73.8%).

Table 5.6: Availability of technical security viewed by computer and engineering department staff.

Rank	Item No.	Item Question (Technical security)	Mean	%	S. D	Degree
1	28	System logged out automatically after predetermined time of inactivity	4.05	81	0.945	High
2	32	An authentication and verification mechanism are implemented for those seeking access to the electronic medical records system	3.95	79	0.510	High
3	27	each workforce member has a unique user identifier and public accounts are not used	3.85	77	1.268	High
4	29	The connection between the hospital and data center is secured and the transmitted data is encrypted	3.80	76	0.894	High
5	33	Appropriate procedures are followed to ensure that medical information is preserved from modification, alteration, or destruction in an unauthorized manner	3.75	75	1.020	High
6	30	There are policies and procedures to provide appropriate access to HIS data in emergency	3.25	65	1.209	Moderate

7	31	There are audit control mechanisms that can monitor, record, and/or examine the activity of the information system	3.20	64	1.322	Moderate
Total Domain Degree			**3.69**	**73.8**	**0.802**	**High**

5.3.1.4 The fourth sub-question: what are the aspects of security and privacy protection of health information in the MoH from the viewpoint of the Palestine Medical Complex (PMC) staff?

To answer the previous question, the means, percentages, and standard deviations of the aspects of security and privacy protection of health information in the MoH were extracted from the viewpoint of the Palestine Medical Complex staff, arranged concerning importance. (Table 5.7.)

The data prescribed in Table 5.7 indicate that the most important aspect of the security and privacy protection of health information in the MoH from the view point of the Palestine Medical Complex staff were (business continuity) with (M = 3.79), and (75.8%), followed by (development and maintenance of systems) with (M = 3.51), and (70.2%), followed by (organizational policy) with (M = 3.46), and (69.2%), followed by (security policy) with (M = 3.44) and (68,8%), followed by (system access control) with (M = 3.43) and (68.6%), followed by (data disclosure) with (M= 3.05), and (61.0%), while the least rank one was (personal security) with (M = 2.90), and (58%). Moreover, the total gross domain was in moderate degree with (M = 3.33) and (66.6%).

Tables (5.7-5.14) illustrate the means, standard deviations, and ranks of the items of the information security and privacy protection in MoH from the viewpoint of Palestine Medical Complex staff.

Table 5.7: Security and privacy protection of health information in MoH from the viewpoint of PMC staff.

Item No.	Rank	Domain	Mean	%	S. D	Degree
1	4	Security policy	3.44	68.8	0.950	High
2	3	Organizational policy	3.46	69.2	0.834	High
3	7	Personal security	2.90	58.0	0.762	Moderate
4	5	System access control	3.43	68.6	0.689	High

5	2	Development and maintenance of systems	3.51	70.2	0.629	High
6	1	BCP	3.79	75.8	0.512	High
7	6	Data disclosure	3.05	61.0	0.524	Moderate
All Domains			**3.33**	**66.6**	**0.460**	**Moderate**

5.3.2 Domain One: Security Policy

The data shown in Table 5.8 indicate that the most ranked descending aspects of the security policy for health information protection in the MoH from the view point of the Palestine Medical Complex staff was "There is a known and defined responsible department for information security policy and its review, maintenance and upgrade", with (M = 3.51), and (70.2%), followed by "There exists an information security policy known to all the employees", with (M = 3.49), and (69.8%), while the least important was "The existed information security policy states the hospital approach to manage information security", with (M = 3.33), and (66.6%). Moreover, the total gross domain was in a high degree with (M = 3.44) and (68.8%).

Table 5.8: Security policy of health information protection in MoH viewed by PMC staff.

Rank	Item No.	Item (Security policy)	Mean	%	S. D	Degree
1	3	There is a known and defined responsible department for information security policy and its review, maintenance, and upgrade	3.51	70.2	1.077	High
2	1	There exists an information security policy known to all the employees".	3.49	69.8	1.096	High
3	2	The existed information security policy states the hospital's approach to managing information security.	3.33	66.6	1.057	Moderate
Security Policy			**3.44**	**68.8**	**1.076**	**High**

5.3.3 Domain Two: Organizational Security

Data in Table 5.9 indicate that the most ranked descending aspects of the organizational security of health information protection in MoH from the view point of the Palestine Medical Complex

staff were "Employees are prohibited from using medical information for unauthorized purposes" with (M = 4.05), and (81%), followed by "Responsibilities for the protection of patient information assets and for carrying out specific security processes were clearly defined" with (M = 3.21), and (64.2%), and the least ranked one was "There is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls", with (M = 3.13), and (62.6%). Moreover, the total gross domain was in a high degree with (M = 3.46) and (69.2%).

Table 5.9: Organizational security of health information protection in MoH viewed by PMC staff.

Rank	Item No.	Item (Organizational security)	Mean	%	S. D	Degree
1	6	Employees are prohibited from using medical information for unauthorized purposes	4.05	81.0	0.963	High
2	5	Responsibilities for the protection of patient information assets and for carrying out specific security processes were clearly defined	3.21	64.2	1.071	Moderate
3	4	There is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls	3.13	62.6	1.071	Moderate
Organizational Security			**3.4624**	**69.2**	**.83449**	**High**

5.3.4 Domain Three: Personal Security

Data offered in Table 5.10 indicate that the most ranked descending aspects of personal security for health information protection in MoH from the view point of the Palestine Medical Complex staff were "The employee's job description document contains the responsibilities and tasks towards information security in the hospital", with (M = 3.51), and (70.2%), followed by "There is a formal disciplinary process in place for employees who have violated organizational security policies and procedures", with (M = 3.15), and (63.0%), while the least ranked one was

"Disciplinary measures have been taken against the employee due to the area of information security", with (M = 1.99), and (39.8%). Moreover, the total gross domain was in a moderate degree with (M = 2.90) and (59.8%).

Table 5.10: Personal security of health information protection in MoH viewed by PMC staff.

Rank	Item No.	Item (Personal security)	Mean	%	S. D	Degree
1	7	The employee's job description document contains the responsibilities and tasks towards information security in the hospital	3.51	70.2	1.070	High
2	12	There is a formal disciplinary process in place for employees who have violated organizational security policies and procedures	3.15	63.0	1.119	Moderate
3	10	A formal reporting procedure exists, to report security incidents through appropriate management channels	3.13	62.6	1.079	Moderate
4	11	A formal reporting procedure or guideline exists for users, to report security weakness in, or threats to, systems or services	2.99	59.8	1.014	Moderate
5	8	Employees are asked to sign a confidentiality or nondisclosure agreement as a part of their initial terms and conditions of the employment	2.96	59.2	1.139	Moderate
6	9	All employees of the organization receive appropriate information security training	2.53	50.6	1.264	Moderate
7	13	Disciplinary measures have been taken against you due to the area of information security	1.99	39.8	1.078	Low
Personal Security			**2.90**	**58.0**	**0.762**	**Moderate**

5.3.5 Domain Four: System Access Control

The data displayed in Table 5.11 indicate that the ranked descending aspects of controlling access to health information protection in MoH from the view point of the Palestine Medical Complex staff were "There is a unique account (username/password) for each user such as

technicians, system administrators, and operators" with (M = 4.30), and (86%), followed by "There are some guidelines in place to guide users in selecting and maintaining secure passwords" with (M = 3.68), and (73.6%), while the least ranked one was "Employees can easily access the Internet" with (M= 2.49), and (49.8%). Moreover, the total gross domain was in a high degree level with (M = 3.43) and (68.6%).

Table 5.11: System access control of health information protection in MoH viewed by PMC staff.

Rank	Item No.	Item (System access control)	Mean	%	S. D	Degree
1	17	There is a unique account (username/password) for each user such as technicians, system administrators, and operators	4.30	86.0	0.714	Very High
2	16	There are some guidelines in place to guide users in selecting and maintaining secure passwords	3.68	73.6	0.948	High
3	15	The employees are given privileges based on their job description and the daily tasks	3.67	73.4	1.063	High
4	14	There exists a regular process to review and evaluate user access rights and privileges	2.99	59.8	1.082	Moderate
5	18	Employees can easily access the Internet	2.49	49.8	1.248	Moderate
System Access Control			**3.43**	**68.6**	**0.689**	**High**

5.3.6 Domain Five: Development and Maintenance of Systems

The data contained in Table 5.12 indicate that the ranked descending aspects of developing and maintaining systems for health information protection in MoH from the view point of Palestine Medical Complex staff were "Only hospital technicians can install software on the computers" with (M = 3.93), and (78.6%), followed by "There are controls in place on installing software to computers, to reduce the risk of damage to operating systems" with (M = 3.82), and (76.4%),

while the least ranked one was “The computers are regularly maintained” with (M = 3.16), and (63.2%). Moreover, the total gross domain was in a high degree with (M = 3.51) and (70.2%).

Table 5.12: Development and maintenance of systems of health information protection in MoH viewed by PMC staff.

Rank	Item No.	Item (Systems development and maintenance)	Mean	%	S. D	Degree
1	23	Only hospital technicians can install software on your computer	3.93	78.6	0.958	High
2	20	There are controls in place on installing software to computers, to reduce the risk of damage to operating systems	3.82	76.4	1.033	High
3	24	There is an anti-virus installed on your PC	3.56	71.2	1.075	High
4	19	The entered data is validated	3.37	76.4	1.015	Moderate
5	22	There are UPSs in the wards when the power is off	3.23	64.6	1.246	Moderate
6	21	The computers are regularly maintained	3.16	63.2	1.258	Moderate
Development and Maintenance of Systems			**3.51**	**70.2**	**0.629**	**High**

5.3.7 Domain Six: Business Continuity Planning (BCP)

Data in Table 5.13 designate that the ranked descending aspects of BCP for health information in the MoH from the point of view of Palestine Medical Complex employees “System administrators are notified of any malfunction or interruption of work as soon as it occurs”, with (M = 4.30), and (86%), followed by “Patient information is entered into the system upon his return to work”, with (M = 3.98), and (79.6%), while the least ranked one was “Work continuity plans are tested regularly to ensure that they are up to date and effective”, with (M = 3.25), and (65%). Moreover, the total gross domain was in a high degree with (M = 3.79) and (75.8%).

Table 5.13: Continuity planning of work of health information protection in MoH viewed by PMC staff.

Rank	Item No.	Item (Continuity planning of work)	Mean	%	S. D	Degree
1	26	System administrators are notified of any malfunction or interruption of work as soon as it occurs.	4.30	86.0	0.661	Very high
2	28	Patient information is entered into the system upon his return to work	3.98	79.6	0.690	High
3	25	System crashes frequently.	3.91	78.2	1.065	High
4	27	There is a plan to return the system to normal after a system failure or interruption in system performance.	3.50	70.0	1.122	High
5	29	Work continuity plans are tested regularly to ensure that they are up to date and effective.	3.25	65.0	0.947	Moderate
Business Continuity			**3.79**	**75.8**	**0.512**	**High**

5.3.8 Domain Seven: Data Disclosure

Data in Table 5.14 specify that the ranked descending aspects of data disclosure of health information in MoH from the view point of the Palestine Medical Complex staff were "You Logout your account immediately when you finish your work", with (M = 4.04), and (80.8%), followed by "Medical information are shared between specialists after obtaining the consent of the patients", with (M = 3.35), and (67.0%), while the least ranked one was "You are asked unofficially to disclose the patients' information" with (M = 2.39), and (47.8%). Moreover, the total gross domain was in a moderate degree with (M = 3.05) and (61.0%).

Table 5.14: Data disclosure of health information protection in MoH viewed by PMC staff.

Rank	Item No.	Item (Data disclosure)	Mean	%	S. D	Degree
1	31	You logout your account immediately when you finish your work	4.04	80.8	1.081	High
2	34	Medical information is shared between the specialists after obtaining consent from patients	3.35	67.0	1.045	Moderate
3	30	Username and password are easily exchanged between employees	2.74	54.8	1.236	Moderate

4	33	You give information about patients if your colleagues ask to do so	2.72	54.4	1.126	Moderate
5	32	You are asked unofficially to disclose the patients' information i.e for research	2.39	47.8	1.265	low
Data Disclosure			**3.05**	**61.0**	**0.524**	**Moderate**

5.4 Testing Hypotheses

Hypothesis (H01): MoH applies security safeguards (administrative, physical, and technical) to enhance the level of information security protection in governmental hospitals.

To examine the previous hypothesis, the One Sample T-test was used for the extent of applying security safeguards for health information security and privacy protection in MoH from the viewpoint of computer and engineering department staff, as is evident in Table 5.15.

It is evident from Table 5.15 that MoH applies security safeguards of health information protection in MoH from the viewpoint of computer and engineering department employees. According to the calculated value (T = 26.721), which is greater than the tabular value (T = 1.72), the results show that there were statistically significant differences at ($\alpha \leq 0.05$), so we accept the hypothesis to the extent of applying security safeguards for health information security and privacy protection in MoH from the viewpoint of computer and engineering department staff where the significance is (0.000), which is less than the level (0.05). This indicates the validity of the hypothesis; the effectiveness and importance of the independent variable, (the application of security safeguards) in affecting the dependent variable (to enhance the level of health information security and privacy protection in MoH in the governmental hospitals), signifying that the attitudes of the computer department's employees were directly

and positively correlated and were in agreement with a large degree, which indicates that security safeguards are widely applied and therefore the first null hypothesis should be rejected.

Table 5.15: (H01): Security safeguards viewed by computer and engineering department staff.

Hypothesis (H01)					Test value = 0.05		
Item	**Mean**	**SD**	**%**	**DF**	**Tabular-T**	**T-value**	**Sig.**
Security safeguards" administrative, physical, and technical"	3.57	.597	71.4	19	1.72	26.721	0.000

Statistically significant at ($\alpha \leq 0.05$).

(H01-1): MoH applies administrative safeguards to ensure health information security and privacy protection.

To examine the previous hypothesis, the One Sample T-test was used for the extent of applying administrative safeguards for health information security and privacy in the MoH from the viewpoint of computer and engineering department staff, as is evident from Table 5.16.

It is apparent from Table 5.16 that MoH applies administrative safeguards of health information protection in MoH from the viewpoint of computer and engineering department employees. According to the calculated value (T = 25.552), which is greater than the tabular value (T = 1.72), the results show that there were statistically significant differences at ($\alpha \leq 0.05$), therefore we accept the hypothesis to the extent of applying administrative safeguards for health information security and privacy protection in MoH from the viewpoint of computer and engineering department staff where the significance is (0.000), which is less than the level (0.05). This specifies the validity of the hypothesis, signifying that the attitudes of the computer department's employees were directly and positively correlated with the application of administrative safeguards and were in agreement with a large degree, which indicates that security safeguards are widely available, consequently the null hypothesis which states that the

MoH didn't apply administrative safeguards to ensure the security and privacy of health information in the MoH, should be rejected.

Table 5.16: (H01-1): Administrative safeguards viewed by computer and engineering department staff.

	(H01-1)			Test value = 0.05			
Item	**Mean**	**%**	**SD**	**DF**	**Tabular-T**	**T-value**	**Sig.**
Administrative safeguards	3.38	67.6	0.59	19	1.72	25.552	0.000

Statistically significant at ($\alpha \leq 0.05$).

(H01-2): MoH applies physical safeguards to ensure health information security and privacy protection.

To examine the previous hypothesis, the One Sample T-test was used for the extent of applying physical safeguards for health information security and privacy in the MoH from the viewpoint of computer and engineering department staff, as is evident from Table 5.17.

It is obvious from Table 5.17 that MoH applies physical safeguards of health information protection in MoH from the viewpoint of computer and engineering department employees. According to the calculated value (T = 21.136), which is greater than the tabular value (T = 1.72), the results show that there were statistically significant differences at ($\alpha \leq 0.05$), therefore we accept the hypothesis to the extent of applying physical safeguards for health information security and privacy protection in MoH from the viewpoint of computer and engineering department staff where the significance is (0.000), which is less than the level (0.05). This specifies the validity of the hypothesis, signifying that the attitudes of the computer department's employees were directly and positively correlated with the application of physical safeguards and were in agreement with a large degree, which indicates that physical safeguards are widely available and therefore the null hypothesis which states that the MoH didn't apply physical safeguards to ensure the security and privacy of health information in the MoH, should be rejected.

Table 5.17: (H01-2): Physical safeguards viewed by computer and engineering department staff.

(H01-2)				Test value = 0.05			
Item	**Mean**	**%**	**SD**	**DF**	**Tabular-T**	**T-value**	**Sig.**
physical safeguards	3.79	75.8	0.801	19	1.72	21.136	0.000

Statistically significant at ($\alpha \leq 0.05$).

(H01-3): MoH applies technical safeguards to ensure health information security and privacy protection.

To examine the previous hypothesis, the One Sample T-test was used for the extent of applying technical safeguards for health information security and privacy in the MoH from the viewpoint of computer and engineering department employees, as is evident from Table 5.18.

It is noticeable from Table 5.18 that MoH applies technical safeguards of health information protection in MoH from the viewpoint of computer and engineering department employees. According to the calculated value (T = 26.68), which is greater than the tabular value (T = 1.72), the results show that there were statistically significant differences at ($\alpha \leq 0.05$), therefore we accept the hypothesis to the extent of applying technical safeguards for health information security and privacy protection in MoH from the viewpoint of computer and engineering department staff where the significance is (0.000), which is less than the level (0.05). This stipulates the validity of the hypothesis, suggesting that the attitudes of the computer department's employees were directly and positively correlated with the application of technical safeguards and were in agreement with a large degree, which indicates that technical safeguards are widely available and therefore the null hypothesis, which states that the Ministry of health didn't apply technical safeguards maintain the security and privacy of health information in the MoH should be rejected.

Table 5.18: (H01-3): Technical safeguards viewed by computer and engineering department staff.

(H01-3)				Test value = 0.05			
Item	**Mean**	**%**	**SD**	**DF**	**Tabular-T**	**T-value**	**Sig.**
Technical safeguards	3.69	73.8	0.618	19	1.72	26.68	0.000

Statistically significant at ($\alpha \leq 0.05$).

(H02): Security and privacy protection of health information are applied in MoH from the viewpoint of the Palestine Medical Complex staff.

To examine the previous hypothesis, the One Sample T-test was used for the application of security and privacy protection of health information in MoH from the viewpoint of the Palestine Medical Complex staff, as is evident in Table 5.19.

It is noticeable from Table 5.19 that MoH applies security and privacy protection of health information in PMC from the viewpoint of PMC staff. According to the calculated value (T = 85.094), which is greater than the tabular value (T = 1.66), the results show that there were statistically significant differences at ($\alpha \leq 0.05$), thus we accept the hypothesis to the extent of applying security and privacy protection of health information in PMC from the viewpoint of PMC staff where the significance is (0.000), which is less than the level (0.05). This specifies the validity of the hypothesis, signifying that the security and privacy protection of health information in the PMC was applied and therefore the null hypothesis should be rejected.

Table 5.19: (H02): Application of security in the MoH.

(H02)				Test value = 0.05			
Item	**Mean**	**%**	**SD**	**Tabular-T**	**DF**	**T-value**	**Sig.**
Application of security and privacy protection of health information in the MoH.	3.33	66.6	0.460	1.66	141	85.094	0.000

Statistically significant at ($\alpha \leq 0.05$).

(H02-1): There are policies applied for the security and privacy protection of health information in MoH from the viewpoint of Palestine Medical Complex staff.

To examine the previous hypothesis, the One Sample T-test was used for the extent of the application of policies for security and privacy of health information in MoH from the viewpoint of Palestine Medical Complex employees, as is evident from Table 5.20.

It is perceptible from Table 5.18 that MoH applies policies for security and privacy protection of health information in PMC from the viewpoint of PMC staff. According to the calculated value (T = 42.542), which is greater than the tabular value (T = 1.66), the results show that there were statistically significant differences at ($\alpha \leq 0.05$), thus we accept the hypothesis to the extent of applying policies for security and privacy protection of health information in PMC from the viewpoint of PMC staff where the significance is (0.000), which is less than the level (0.05). This specifies the validity of the hypothesis, signifying that the policies for security and privacy protection of health information in the PMC are applied and therefore this null hypothesis should be rejected.

Table 5.20: (H02-1): Application of policies viewed by PMC staff.

(H02-1)				**Test value = 0.05**			
Item	**Mean**	**%**	**SD**	**DF**	**Tabular-T**	**T-value**	**Sig.**
The application of policies for the security and privacy protection of health information in the Palestinian Ministry of Health is viewed by PMC staff.	3.44	68.8	0.950	141	1.66	42.542	0.000

Statistically significant at ($\alpha \leq 0.05$).

(H02-2): The organizational security for the security and privacy of medical information protection is applied in the MoH from the viewpoint of Palestine Medical Complex employees.

To examine the previous hypothesis, the One Sample T-test was used for the extent of the application of the organizational security for security and privacy protection of health

information in the MoH from the viewpoint of Palestine Medical Complex staff, as is evident from Table 5.21.

It is perceptible from Table 5.21 that MoH applies the organizational security for security and privacy protection of health information in PMC from the viewpoint of PMC staff. According to the calculated value (T = 48,729), which is greater than the tabular value (T = 1.66), the results show that there are statistically significant differences at ($\alpha \leq 0.05$), thus we accept the hypothesis to the extent of applying the organizational security for security and privacy protection of health information in PMC from the viewpoint of PMC staff where the significance is (0.000), which is less than the level (0.05). This specifies the validity of the hypothesis, signifying that the organizational security for security and privacy protection of health information in the PMC is applied and therefore this null hypothesis should be rejected.

Table 5.21: (H02-2): Application of organizational security viewed by PMC staff.

(H02-2)				**Test value = 0.05**			
Item	**Mean**	**%**	**SD**	**DF**	**Tabular-T**	**T-value**	**Sig.**
The application of organizational security for the security and privacy protection of health information viewed by PMC staff.	3.46	69.2	.0834	141	1.66	48.729	0.000

Statistically significant at ($\alpha \leq 0.05$).

(H02-3): The employees are qualified to maintain the security and privacy protection of health information in the MoH from the viewpoint of Palestine Medical Complex staff.

To examine the previous hypothesis, the One Sample T-test was used for the extent to which the employees are qualified to maintain the privacy of health information in the MoH from the viewpoint of Palestine Medical Complex staff, as is evident from Table 5.22.

It is perceptible from Table 5.22 that PMC staff are qualified to maintain security and privacy protection of health information in PMC from the viewpoint of PMC staff. Consistent with the

calculated value (T = 44,487), which is greater than the tabular value (T = 1.66), the results show that there are statistically significant differences at ($\alpha \leq 0.05$), thus we accept the hypothesis to the extent of staff qualification to maintain security and privacy protection of health information in PMC from the viewpoint of PMC staff where the significance is (0.000), which is less than the level (0.05). This agrees with the validity of the hypothesis, representing that the staff qualification to maintain security and privacy protection of health information in the PMC is available, and therefore this null hypothesis should be rejected.

Table 5.22: (H02-3): Staff qualification viewed by PMC staff.

(H02-3)				**Test value = 0.05**			
Item	**Mean**	**%**	**SD**	**DF**	**Tabular-T**	**T-value**	**Sig.**
The qualification of the employees to maintain the security and privacy protection of health information viewed by PMC staff.	2.90	58.0	0.762	141	1.66	44.487	0.000

Statistically significant at ($\alpha \leq 0.05$).

(H02-4): There is control over access to systems to maintain the security and privacy of medical information protection in MoH from the viewpoint of Palestine Medical Complex employees.

To examine the previous hypothesis, the One Sample T-test was used for the extent to which there is a control to access the systems and maintain the security of the privacy of health information protection in the MoH from the viewpoint of the Palestine Medical Complex staff, as is evident from Table 5.23

Certainly, it is observable from Table 5.23 that PMC staff have control over access to systems to maintain the security and privacy protection of health information in PMC from the viewpoint of PMC staff. Consistent with the calculated value (T = 58.395), which is greater than the tabular value (T = 1.66), the results show that there are statistically significant differences at (α

≤ 0.05), thus we accept the hypothesis to the extent of staff control over access to systems to maintain security and privacy protection of health information in PMC from the viewpoint of PMC staff where the significance is (0.000), which is less than the level (0.05). This approves the validity of the hypothesis, representing that the staff control over access to systems to maintain security and privacy protection of health information in the PMC is available, and therefore this null hypothesis should be rejected.

Table 5.23: (H02-4): System access control viewed by PMC staff.

(H02-4)				**Test value = 0.05**			
Item	**Mean**	**%**	**SD**	**DF**	**Tabular-T**	**T-value**	**Sig.**
There is a system access control to maintain the security and privacy protection of health information in MoH viewed by PMC staff.	3.43	68.6	0.689	141	1.66	58.395	0.000

Statistically significant at (α ≤ 0.05).

(H02-5): Systems are developed and maintained to have the security and privacy protection of health information in MoH from the viewpoint of Palestine Medical Complex staff.

To examine the previous hypothesis, the One Sample T-test was used for the extent to which systems were developed and maintained to have the security and privacy of health information in the MoH from the viewpoint of the Palestine Medical Complex staff, as is evident from Table 5.24

Certainly, it is apparent from Table 5.24 that PMC staff have the systems developed and maintained to have the security and privacy protection of health information in PMC from the viewpoint of PMC staff. Compliant with the calculated value (T = 65.639), which is greater than the tabular value (T = 1.66), the results show that there are statistically significant differences at (α ≤ 0.05), thus we accept the hypothesis to the extent of staff development and

maintain systems to have security and privacy protection of health information in PMC from the viewpoint of PMC staff where the significance is (0.000), which is less than the level (0.05). This approves the validity of the hypothesis, representing that the systems are developed and maintained to have security and privacy protection of health information in the PMC, and therefore this null hypothesis should be rejected.

Table 5.24: (H02-5): Development and maintenance of systems viewed by PMC staff.

(H02-5)				Test value = 0.05			
Item	**Mean**	**SD**	**%**	**DF**	**Tabular-T**	**T-value**	**Sig.**
Developing and maintaining systems to maintain the security and privacy protection of health information in MoH viewed by PMC staff.	3.51	0.629	70.2	141	1.66	65.639	0.000

Statistically significant at ($\alpha \leq 0.05$).

(H02-6): There is a continuity of planning work to maintain the security and privacy of medical information protection in the MoH from the viewpoint of Palestine Medical Complex staff.

To examine the previous hypothesis, the One Sample T-test was used for the extent to which there is continuous planning work to maintain the security and privacy of the health information protection in MoH from the viewpoint of PMC staff as is evident in Table 5.25.

Indeed, it is visible from Table 5.25 that PMC staff have continuity of planning work to maintain the security and privacy protection of health information in PMC from the viewpoint of PMC staff. Compliant with the calculated value (T = 86.892), which is greater than the tabular value (T = 1.66), the results display that there are statistically significant differences at ($\alpha \leq 0.05$), therefore we accept the hypothesis to maintain continuity of planning work to have security and privacy protection of health information in PMC from the viewpoint of PMC staff where the significance is (0.000), which is less than the level (0.05). This approves the validity of the

hypothesis, representing that there is a continuity of planning work to have security and privacy protection of health information in the PMC, and therefore this null hypothesis should be rejected.

Table 5.25: (H02-6): Continuous planning of work viewed by PMC staff.

(H02-6)					Test value = 0.05		
Item	**Mean**	**%**	**SD**	**DF**	**Tabular-T**	**T-value**	**Sig.**
There is continuous planning of work to maintain the security and privacy protection of health information viewed by PMC staff.	3.79	75.8	0.512	141	1.66	86.892	0.000

Statistically significant at ($\alpha \leq 0.05$).

(H02-7): The patient data are not disclosed from the viewpoint of Palestine Medical Complex employees.

To examine the previous hypothesis, the One Sample T-test was used for the extent of disclosure of patient data from the viewpoint of the Palestine Medical Complex staff, as is in Table 5.26. Certainly, it is observable from Table 5.26 that PMC staff do not disclose patient data, to maintain the security and privacy protection of health information in PMC from their viewpoints. Compliant with the calculated value (T = 68.150), which is greater than the tabular value (T = 1.66), the results display that there are statistically significant differences at ($\alpha \leq$ 0.05), therefore we accept the hypothesis to maintain continuity of planning work to have security and privacy protection of health information in PMC from the viewpoint of PMC staff where the significance is (0.000), which is less than the level (0.05). This approves the validity of the hypothesis, demonstrating that there is no disclosure of patient data, to have security and privacy protection of health information in the PMC, and therefore this null hypothesis should be rejected.

Table 5.26: (H02-6): Patient data disclosure viewed by PMC staff.

(H02-7)				Test value = 0.05			
Item	**Mean**	**%**	**SD**	**DF**	**Tabular-T**	**T-value**	**Sig.**
Patient data are not disclosed from the viewpoints of PMC staff among the employees themselves.	3.05	61.0	0.524	141	1.66	68.150	0.000

Statistically significant at ($\alpha \leq 0.05$).

5.5 Summary

In This chapter the researcher has confirmed the main findings of the research reported and described how they relate to the research questions and hypotheses. Reported results were framed around relevant research problems, questions, and hypotheses that were formulated earlier.

CHAPTER SIX
DISCUSSION AND IMPLICATIONS

6.1 Overview

This chapter provides detailed and summarized explanations based on the results of our literature review (Chapters 3 and 5) and on the descriptive-analytical method (Chapter 4). In this chapter, we explored the existing knowledge of privacy and security in the Palestinian Ministry of Health, which covers several research areas, including health care providers' concerns about the information security. The perceptions of information security and privacy in the Palestinian Ministry of Health are presented and discussed to find out the similarities and differences and to compare with other studies regarding the personal information provided. In addition, directions for future work and important aspects to focus on in the future are also addressed.

6.2 Discussion

Privacy protection and security of data are becoming the foremost concern of any organization. As a short explanation, privacy and security of data are about the protection of patient files from being exposed to unauthorized and adverse effect accesses. In the health sector institutions, medical data is shared between workers to enable patients to obtain the best treatment results, where opinions are exchanged and data are discussed. Nonetheless, when sharing this sensitive and personal data, a breach or leakage may occur which could lead to infringe privacy as well cause socioeconomic reflection for patients. Hitherto, ensuring the privacy and security of health data could mend the service provision of the MoH which can warrant patient trust when verified the safety of the patient record. The first major common topic between theory and practice is the notion that the right information must be made available to the right person at the

needed time and place (Utbult, 2004). This is in line with the idea that the most important goal of the Palestinian MoH is to provide the best health care service to citizens.

6.2.1 Discussing Study Questions

6.2.1.1 Level of security and privacy protection of health information in the MoH and PMC?

Results displayed that most of the respondents specified that the level of security and privacy protection of health information in MoH from the viewpoint of the computer and engineering department staff was high, and was at a moderate level in the PMC. These results are also consistent with that of (Nguyen, 2019), and (Zayar, 2014). The researcher attributes that the respondents are very keen and realized the privacy and security concerns more than the patients themselves, also, the reason for this result is the remarkable experience that the staff has in dealing with the system. Another reason is that employees are more sustainable in the modern technology update in their work. Healthcare Organizations must adapt new technologies against the threats and take risk management very seriously. Moreover, this could be due to the feeling that they maintain accurate information in patients' records, as well as they make sure that the patients are constantly asking the access for their electronic medical information and are seeking to do so by all means, they are careful to handle patients' health information to protect their privacy.

Results revealed a rate ranging from medium to high in the application of security fields like the security safeguards, and notwithstanding these results that could be acceptable in any sector rather than the healthy one, the researcher deems these results are not sufficient to achieve the requisite level of privacy protection and security of health information in the Palestinian Ministry of Health and PMC. Nonetheless, Palestinian MoH and PMC have to promote the

working to implement effective, strong and updated security policies to reflect the interest and awareness of healthcare organization and that it is feasible and effective so that they can attain an integrated level of security that guarantees the satisfaction and reassurance of patients in preserving their data from any disclosure, penetration or hacking.

6.2.1.2 Answering sub-questions from the viewpoint of the computer and engineering department staff

6.2.1.2.1 Security and privacy features in MoH

The three security-safeguard topics explicitly administrative, technical, and physical have been applied in the analysis in this research. These topics entail several security strategies used by healthcare administrations to attain best security environment . To assess the level of security and privacy of health information in the Palestinian Ministry of Health, it was indispensable to evaluate security areas based on international standards and to cover all aspects of the study subject.

With regard to the physical safeguard, our study revealed outstanding results in the field of applying security safeguards in the MoH from the viewpoint of computer and engineering department staff, where the percentage of physical security theme attained the highest rate (75.8%). The highest score recorded was for the rooms containing the devices and the datacenters. The researcher refers this result to the international standards that were tracked by the donors during the installation and operation of the health information systems in the Ministry of Health hospitals, while this sustained on this approach by the computer and engineering department so far. Other attributable causes may be that the physical safeguards are designed to protect the institution systems physically, which protects the software and hardware materially from any penetration , sabotage or unauthorized access (Zulman et al., 2011). Violation of physical security measures is one of the major causes of security breaches (Liu et al., 2015). This

result is consistent with the studies of [Shehada and Bader, 2020; Aldanaf, 2013; and Wirken, 2010]. Furthermore, it is in line with previous results of (Nguyen, 2019), and (Mehraeen et al. 2016) where the 36 IT managers in Iran study results showed a strong level of technical and physical sections decreasing to a medium in the administrative one ,In another similar study, Park and companions confirmed that the lowest standards were found in the managerial or administrative category (Park et al. 2010).

Regarding technical security, it was rated in the second position by the MoH from the viewpoint of computer and engineering department staff, where the percentage of technical security theme attained the second rate (73.8%). The highest score was recorded for logging out of the system automatically, and the user's privileges, where the lowest score was recorded for the audit controls and access to data in an emergency.

The researcher attributes this result to the impressive experience that the staff of the ministry has when collaborated during the implementation of the systems by the United States Agency for International Development (USAID) engineers, in addition to the procedures that the computer and engineering department employees follow while performing their day-to-day duties, These results are also harmonized with the study of (Nguyen, 2019), and (Zayar, 2014). Additionally, while this technical safeguard's theme performs protection of the whole information system located in the network of a health organization, it is very crucial in safeguarding the security of the organization because furthermost breaches to security ensue through the electronic media across the use of computers and other portable electronic machines (Liu et al., 2015). This theme includes security techniques for example the use of firewalls and encryption, virus checking, and actions used in verifying information (Lemke, 2013). Nevertheless, Lemke find that the firewalls and cryptography were the most functional security techniques. In addition to many security techniques like Antiviruses (Gupta and

Agrawal, 2019). Moreover, it was consistent with (Eroglu and Cakmak's, 2016) study who concluded in their study that the health organization is at a good security level, and a strong level in the infrastructure and the technical side, but they still need to enhance the regulations and decisions.

Concerning the administrative safeguard security theme, it was the least ordered and decreased to a moderate percent (67.6%), where the highest paragraph scored for password policy, and network monitoring, and the least recorded for the risk management, for security policy team, and information security training programs, which agreed with [Mehareen, 2016; Nguyen, 2019] studies. The researcher attributes this result to the weakness in the level of administrative security compared to the physical and technical to the lack of clear policies regarding the evaluation of security vulnerabilities and risk assessment procedures. Furthermore, it could be because of the policies in Palestine which pay more attention on the technical and physical side neglecting the administrative one, even if it need fewer budget and resources and it could give a great influence.

The administrative safeguard is comprised of relevant techniques policies, backups and applying appropriate information security training. It has safeguards that focus on having a yielding security procedure, policies, education, and security plans (Wikina, 2014). Eventually, these techniques that customize the logging authorization have improved privacy and security of information(Jannetti, 2014). Proposing a Chief Information Security Officer would help in managing and organizing all the security techniques and initiatives in electronic health records.

6.2.1.2.2 Security and privacy features in PMC

In the second stage, it was indispensable to evaluate security areas based on international standards and to cover all aspects of the study subject to assess the level of security and privacy of health information in the Palestinian Ministry of Health. It was necessary to question the

health sector employees, subsequently, the Palestine Medical Complex was selected as a case study that may reflect the certainty of information security in the governmental hospitals, where an investigation was made to about seven (7) security areas deduced from the international system ISO 27001 as well as to the section on disclosing medical data.

The medical information security questionnaire inaugurated with the scope of the security policy because it is the one that affords the health sector with the administrative approach to information security based on work requirements and the laws and regulations followed. It comprises the objective and vision of the institution in information security and how to ensure the continuity of the high level of information security. Thus, the questions were about the existence of a policy in the PMC and the extent of its dissemination, application, and updating, as 68.8% of the respondents showed their knowledge of this policy and the team who is responsible for its review, maintenance, and upgrade, otherwise, the rest who does not realize the policy may indicate a lack of continuity of education and awareness since the information security is a continuous process which needs updating and development, and constantly monitoring implementation and application, the result agrees with the study of [Aldanaf, 2013; Wirken, 2012; Hassan, 2013]. The researcher attributes this result to the existence of a policies and standards committee in the Palestinian medical complex, which in turn issued a policy and held training sessions for the employees, noting that this result contradicts what the employees of the computer and engineering department where 48% reported to the presence of such security policy, signifying the absenteeism of coordination between the ministry and hospitals. Accordingly, the researcher concludes by disclosing that the information security policy is an effective influence in security management information systems representing a framework for all acceptable and prohibited actions, and takes care of the necessities of availability, integrity, and confidentiality of information according to the information being protected and according

to the technical mechanisms of the operations, in addition to taking into account the elements of integration of performance and elements of financial cost and others.

The organizational security aims to organize information security in the institution to identify the team responsible for implementing security controls, so a questionnaire was conducted about the presence of the security team representing all hospital departments and whether security operations are carried out regularly in addition to security instructions for employees regarding patient information. The domain results were high, so about 69.2% of the respondents answered positively, especially about the strict instructions to the employees not to use health information for unauthorized purposes, but the percentage drops to 62% about the team that represents all departments, so the hospital should involve more representatives from all departments to have a more comprehensive security team. The results of this part agree with the study of (Al-Danaf, 2013), nonetheless, disagree with the study of (Hassan, 2013), and (Tayeh, 2008), The researcher attributes this result to the administration's dereliction in implementing a policy in Palestine Medical Complex to include representatives from all departments in periodic meetings to discuss the development of the PMC and the existence of a continuing education genuineness.

Personnel security or human resource security, which aims to ensure that all employees are aware of their role and responsibilities towards information security. Employees were asked about the job description document comprising their security responsibilities, besides, the confidentiality agreement and about penalties in addition to the formal procedures followed for reporting on weaknesses or when a security event occurred and ended about the training that the employees receive. Opinions of the respondents showed moderate results in all paragraphs, and the percentages ranged between 40% to 63% in all of the paragraphs, disciplinary measures, and the subject of training, except the job description document that contains security duties,

where the percentage rose to 70%. Therefore, based on these results, the administration should familiarize the employees with the necessary procedures regarding reporting, in terms of intensifying sessions and holding more symposiums and workshops. This result is in line with the study of (Tayeh, 2008), and (Shehada & Bader, 2020), nevertheless, disagree with (Hassan, 2013) study. The researcher attributes this result to the management's perception of the importance of individuals in information security, employees would like administrators to present some attention through questioning about their wants, as well as some recognition, and rather job without them cannot be achieved.

The result of this domain is almost close to an almost acceptable condition, so it is advised that the government does more about taking care of the security of information systems to avoid what individuals could cause from an acute internal threat to information systems. And what distinguishes this study is that it discusses a technical topic from an administrative aspect perfectly, as it touches the weakest link in the information systems, which is the individuals of all their formations in the composition of information systems.

With system access control, it should be ensured that only authorized persons can log on to the system, that persons only access information about their business processes and use them when necessary. The field of controlling access to the system aims to define the employee's privileges according to the job description and the daily tasks based on the approval of the administration and to monitor the privileges periodically by setting rules and conditions for the password to limit the access of unauthorized persons to the system. Our field result was high, as the percentage grasped 68.6%, where 86% of the respondents detailed that each employee has a username and password and that the password is subject to strict conditions, as for reviewing the privileges, the percentage decreased to 60%, and the validity of accessing the Internet was about 50% for which The researcher believes that blocking the Internet will not affect the work

of information systems in the majority of the study community because these systems and programs run on local networks. Moreover, the researcher attributes these results to the existence of a strong password policy applied to the system, while managers are slow in reviewing the privileges of employees or in reporting them at the time of transfer or retirement, and it is also at the request of the administration that not all employees should be given this authority because of its time-wasting effects if it misused. Moreover, the researcher ascribes that the government is increasingly seeking to provide direct physical protection while considering it the primary basis on which security degrees for information systems are built. Studies of [Al-Otaibi, 2010; Al-Buhaisai and Al-Sharif, 2008; Al-Qahtani, 2008] denoted the necessity of using the security perimeters to a large extent. Furthermore, the results of this part agree with the study of [Hassan, 2013; Al-Danaf, 2013; Tayeh, 2008]. Accordingly, the researcher attributes the increasing importance of controlling access to its main role in maintaining confidentiality and privacy of patient data, with the need for availability and access to patient data.

The researcher adds that several conclusions can be drawn based on the analysis of this important domain. MoH differs in its practices towards information systems related to access control issues, while a relatively high percentage agree with their vision towards enhancing the security of information systems through considering the access control of information systems as one of the most important aspects affecting the improvement of the management of security systems. Accordingly, the researcher concludes with the increasing importance of controlling access to information networks, and access to the Internet, with a focus on the need to reconcile the security of systems as a red line, the necessities of availability and access to information for the user and the beneficiary, and looking at the integrity, confidentiality, and privacy of data and information.

The system development and maintenance field was surveyed. The questions were asked about the validity of installing programs, about the existence of anti-virus, then about the maintenance of devices, and about the availability of storage batteries UPS, in addition to whether the entered data are verified.

The respondents answered positively all the questions, while the paragraphs ranged from medium to high. The most prominent of the full control of the devices is the responsibility of the technicians since no usual employee can install any program, in addition to the presence of anti-virus at a high degree. While the total degree for this domain was high, nonetheless the range decreased to a medium level when answering questions on continuous maintenance of devices and about the lake of existence UPSs. The researcher attributes this to the availability of specialists in the maintenance of computers and their attachments at a relatively low rate, or as a result of outsourcing maintenance operations, where they resort to this to reduce costs, while MoH sees this as a decrease in the levels of information security protection, and that the computer and engineering department employee plays a vital role in providing technical support to various devices. Considering these means and methods as a well-studied approach to develop the security of information systems in PMC, while it is important here to use these methods and means as arranged by the results of the study. The results of this part agree with the study of [Hassan, 2013; Tayeh, 2008; Al-Danaf, 2013].

The sixth area surveyed was the business continuity plans which specifies the system failure and business reappearance to normal in light of emergency plans. Unfortunately, 78% of respondents answered that the system frequently crashes, which requires to study thoroughly the explanations for the interruption to find solutions. Nevertheless, the good thing about it is that 80% to 86% of the respondents stated that they quickly report faults and enter medical data as soon as the system restores, likewise, about 70% answered that there is a plan-B to operate

during the system outage. The researcher attributes these results to the significance of the system in the workflow so that it cannot be dispensed for a short period, and this is evidenced by the high result of the reporting of system interruptions. Additionally, the results of this part agree with the study of (Hassan, 2013), and (Tayeh, 2008).

Data disclosure was the last domain perceived by PMC staff. The respondents answered positively about closing the account upon completion of the work by 81%, and by 67% about sharing the patient's data after obtaining consent from them. On the other hand, the negative paragraphs had a clear presence of about 50% for both sharing passwords for accounts between employees and for giving medical information about patients to colleagues in an informal way, The study of Kreicberga (2001) considered that excessive internal trust among co-workers in information systems is more hazardous to systems than transactions.

6.2.2 Discussing hypotheses

(H01): MoH applies security safeguards (administrative, physical, and technical) to enhance the level of information security protection in governmental hospitals.

According to the previous results, we can accept this hypothesis “MoH applies security safeguards (administrative, physical, and technical) to enhance the level of information security protection in the governmental hospitals.”, This hypothesis is in line with the preceding study results. According to the study of Mehraeen and associates (2016) which was conducted in Iran, which revealed a strong score due to technical and physical and decreased to medium level according to the administrative safeguards. As well as In Park and colleagues (2010) study they confirmed that the items which affiliated with managerial or administrative classification score the lowest degrees. This result somewhat matches Liu et al. (2015) apprehended that there are physical security measures in place, such as physical access controls used to prevent theft, such

as the use of locks on computers, along with technical security measures to prevent electronic intrusion through the use of firewalls and by applying encryption techniques. Amer (2015) carried out a study on "*informatics through ethical submission of genomic information and electronic health records*". He reorganized the importance of encryption in affording technical. Where (Jannetti, 2014) found the importance of firewalls in technical safeguards and the administrative will be increased through training ,education, security plans and assigning these tasks to a security officer.

The researcher attributes this to what the management information systems apply in MoH, and what characteristics they have to contribute in achieving the elements of information security. This also indicates the keenness of MoH to protect their information, take advantage of these systems, and avoid surrounding dangers out.

Hypothesis (H02): Security and privacy protection of health information are applied in MoH from the viewpoint of Palestine Medical Complex staff.

The security and privacy protection of health information was applied in the PMC.

The researcher attributes this finding to what the management information systems applied in PMC, and what they have of the characteristics that contribute to achieving the elements of information security. This also indicates the keenness of the PMC staff to protect their information, take advantage of these systems, and avoid surrounding dangers out. Moreover, the researcher attributes this to the fact that the team has the experience in achieving information security by providing access to information when needed by improving and raising the effectiveness of the applied information systems so that these systems provide appropriate information for all types of decisions and domains.

(**H02-1):** There are policies applied for the security and privacy protection of health information in the MoH from the viewpoints of Palestine Medical Complex staff.

Management's policies and procedures aim to guide the decision of users and inform the personnel of their responsibilities of security.

This result confirms a positive correlation indicating a statistical significance between security policy applied and security and privacy protection of health information. The researcher may refer to this result to conclude there is a known and defined information security policy reviewed, maintained, and upgraded. Moreover, the positive relationship may be referred to the existed information security policy that affirms how the PMC follows an effective approach to managing information security. Furthermore, this positive result confirmed that the security policies used in PMC are not complex and simply easy to be understood. There is an information grouping pattern or guideline in place which will lend a hand in shaping how the information is to be handled and protected.

(**H02-2):** The organizational security for the security and privacy protection of health information is applied in the MoH from the viewpoint of Palestine Medical Complex staff.

The researcher concludes by expressing that the availability of organizational procedures to control information systems is an effective feature in the management of information systems security in PMC. It is the sponsor and organizer of exchanging and transferring of information, and the entrance of the senior management to maintain the work of the information systems, where it develops emergency and retrieval plans within a timely planned framework, taking care of the necessities of availability, safety and confidentiality of information according to its vision and the safety of its paths, and along with its financial, human and technical capabilities. The researcher thinks this would indicate the application of health information systems to the aspects of the organizational security procedures.

This result is in accordance with the results of [Tayeh, 2008; Al-Qahtani, 2008; Al-Otaibi, 2010].

(**H02-3):** The employees are qualified to maintain the security and privacy protection of health information in the MoH from the viewpoint of Palestine Medical Complex staff.

Perceptibly, employees are well qualified in maintaining the security and privacy protection of health information.

The researcher thinks that it must be ensured that employees authorizing the collection of, or handling, the data are authorized to do so by the PMC, and aware of data protection rules, including the fact of sharing of medical information should only be carried out by a suitably qualified health professional.

The researcher may refer this result to the experience gained by health IT professionals from the foreign experts who installed HIS all over the ministry facilities and trained them to be qualified. According to their job description the IT staff are capable and qualified enough to install and support the EHR and any other electronic system. They run the technical features of handling patient health information. Their work influences the quality of care immensely. Health IT staff become more implicated in cooperating with other healthcare teams to push better-quality outcomes and new developments in inpatient care.

(**H02-4):** There is control over access to systems to maintain the security of the privacy of health information protection in the MoH from the viewpoint of Palestine Medical Complex staff.

It is very essential to know who should access what and why. As well, it should be very obvious to set access control mechanisms before designing and developing the electronic health record (EHR) software. The result of the hypothesis has indications that the respondents are well aware of the mechanisms for accessing databases in the PMC. The satisfactory result almost signifies the nonexistence of fears of man misuse in case he/she was able to obtain passwords, and would not be a prelude to making an internal threat to the information system.

The researcher attributes this result to the mindfulness and awareness of the officials that the speed of obtaining information contributes significantly in carrying out the tasks, and providing proposals and solutions to various problems, especially in the forefront of which are issues that need to verify the most important element of security information is the ability to obtain information when it is needed by authorized persons, especially when some tasks are linked to a specific time limit. The researcher believes that to raise and increase the speed of obtaining the information, hospitals must be activated around the clock and provide the information required, likewise, supposes the need to link all departments, branches, and departments with hospitals to a greater extent. However, this result was in accordance with the studies of [Kreiberga, 2010; Al-Qahtani, 2008; Al-Otaibi, 2010; Tayeh, 2008; Hassan, 2013].

(**H02-5):** Systems are developed and maintained to have the security and privacy protection of health information in the MoH from the viewpoint of Palestine Medical Complex staff.

The researcher sees that the use of effective protection programs to prevent hacking attempts and infringement of information systems, testing health information systems to check the compliance of security performance standards, and recruiting experts to protect information systems in PMC approval in their opinions of information systems personnel as one of the ways to develop and maintain systems. However, any system could have a breakdown in the hardware and software times. Therefore, maintenance should be sufficient and rapidly completed. Consequently, backup plans should be inaugurated in case of a system interruption. Data mirroring shouldn't take place on the same server. Furthermore, IT support for 24 hours should be on hand.

The result is in accordance with the studies of [Al-Qahtani, 2008; Bjorck, 2005].

(**H02-6):** There is a business continuity planning (BCP) to maintain the security and privacy protection of health information in the MoH from the viewpoint of Palestine Medical Complex staff.

This result confirms a positive relation indicating a statistical significance in business continuity planning affecting the maintenance of the security and privacy protection of health information in the MoH from the viewpoint of Palestine Medical Complex staff.

From the results it could be conclude that the PMC apply the suitable process to achieve and maintain the business continuity planning and identify the events which cause work interruption besides the training of the staff in addition to the utilization of plans to fix up any disruption or system failure in time frame.

The researcher thinks that consolidation and testing of emergency response plans for critical information systems by PMC staff are periodically tested and then combined with a business continuity plan issued by the computer and engineering department.

This result corresponds with the Tayeh (2008) and Al-Ajez (2011) studies.

(**H02-7**): The patient data are not disclosed from the viewpoint of Palestine Medical Complex employees.

The employees of PMC are aware of not disclosing the patient data or even sharing it without consent from the patient himself or his representative, they also Deny the ease of sharing their credentials. The researcher attributes this to the fact that every employee sign a pledge not to disclose medical information, in addition to the investigation committees that are constantly formed to hold employees accountable for their mistakes. This approves the validity of the hypothesis, demonstrating that there is no disclosure of patient data, to have security and privacy protection of health information in the PMC, and therefore this null hypothesis should be rejected.

6.3 Conclusions

In this chapter, the researcher demonstrated the summary and key findings of this master thesis with the aid of analysis chapter results. The results were placed into the perspective, which involved comparing the results with what was expected, with the results of other researchers, and with the research questions. Results interpretation has offered clarification and justification, concluding, and lessons learned.

The study reflected the current reality of security and privacy of Health Information in the Palestinian Ministry of Health, as it gave a clear view of all security sectors in the ministry and clarified the areas of strength and weaknesses, and accordingly, the decision makers would have sufficient information that enables them to take the necessary measures to ensure a better level of information security.

The main objective of the study was to assess the level of security and privacy of health information in the Palestinian Ministry of Health. To achieve this goal and to answer the main research question of the study, the researcher used the descriptive and analytical method where he made the necessary literature reviews to create a questionnaire for each of the employees of the computer department in all governmental hospitals in addition to a questionnaire for employees of the health sector, where the study tool was able to cover all aspects of the subject of the study and was excellently effective in answering the main study question represented in measuring the level of security and privacy of health information in the Palestinian Ministry of Health, where the results showed a rate ranging from medium to high in the application of security domains in addition to security safeguards, and despite these results that may be acceptable in any sector rather than the health sector, the researcher believes that these results

are not sufficient to achieve the required level of security and privacy of health information in the Palestinian Ministry of Health.

The researcher believes that the importance of the study came from the fact that it is the first at the level of the Ministry of Health and it is the first to target the segment of hospitals after the establishment of a main data center that contains all the Ministry systems in addition to a comprehensive computerized health system that contains all the important medical information. Therefore, the study has achieved all the required goals and was able to Measure the availability of administrative, technical and physical safeguards, in addition to being able to measure the extent of application of the various security domains at the employee's level.

After the necessary planning, the appropriate decisions, the correct policies, the efforts of the technicians, and the understanding and awareness of the health sector employees, the Ministry can reach a level of security that guarantees the satisfaction and reassurance of patients in preserving their information from any disclosure, penetration or hacking.

6.3.1 Final Findings

1. Computer and engineering department staff specified that MoH applies security safeguards to maintain the security and privacy protection of health information at a high level, as the statistical average extended to 3.57 (71.4%).

Figure 6.1 shows each field percentage as follows:

a) Physical security is available with a statistical mean of 3.79 and (75.5%).

b) Technical security is available with a statistical mean of 3.69 and (73.8%).

c) Administrative security is available with a statistical mean of 3.38 and (67.6%).

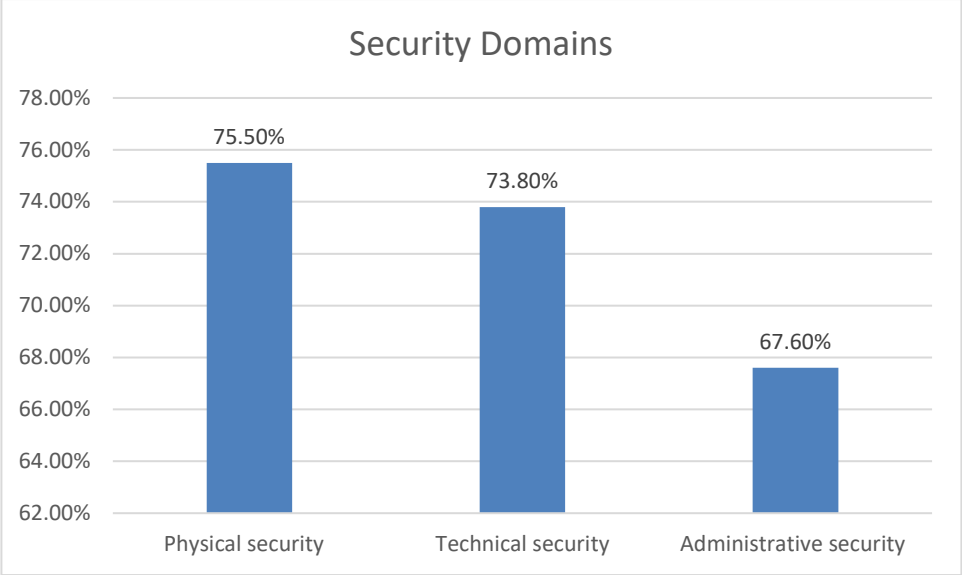

Figure 6.1: Security domains level from the viewpoint of computer and engineering department staff

2. The Palestine Medical Complex staff identified that the level of application of overall fields of information security to maintain the security and privacy protection of health information was at a moderate level, where the statistical mean of all security fields was 3.33 which equals 66.6%.

Figure 6.2 shows each field percentage as follows:

1. Business continuity planning 75.8%
2. Development and maintenance of systems 70.2%
3. Organizational policy 69.2%
4. Security policy 68.8%
5. System access control 68.6%
6. Personal security 58%
7. Data disclosure 61%

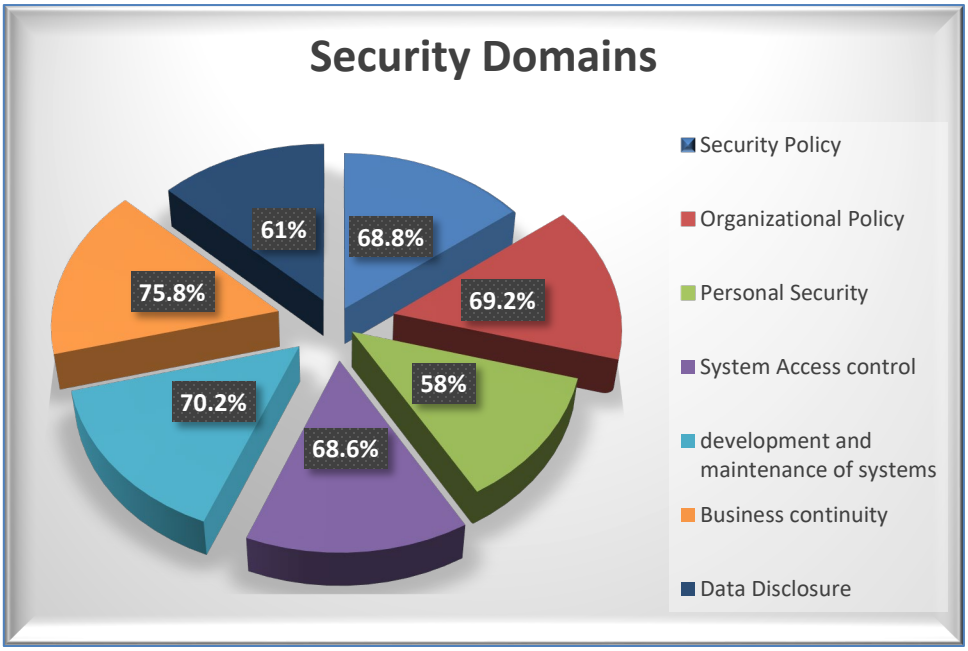

Figure 6.2: Security domains level from the viewpoint of PMC staff

3-There are positive significant statistical correlations at level ($\alpha \leq 0.05$) between all the fields of information security and the security and privacy protection of health information in MoH and Palestine Medical Complex.

6.4 Recommendations

Accordingly, it is recommended to:

1. The computer and engineering department must build its information security policies, and endeavor to publish and implement them in all hospitals, develop and review them, the processes, roles, and responsibilities should be clearly defined as these policies have an impact on improving security procedures and clarifying frameworks that would guide individuals' work mechanisms, and increasing the awareness of individuals towards information security.
2. Designation chief information officer would help in managing and organizing all the security techniques and initiatives in health information systems as well as establishing

a specialized unit in information security, and employing a proficient technician to be responsible for the information assets at each hospital.

3. Developing and promoting capabilities of the data center and information technology department.
4. Since all dimensions of information security are interrelated, it is very important to evaluate them periodically.
5. Ensuring information security is a dynamic event and depends on the cooperation of employees. To ensure that the policies are effective, cooperation should be ascertained between managers and all employees, and all units should be actively involved.
6. To ensure information security, threats and risks should be well defined, appropriate methods of protection should be selected and reviewed regularly, Pre-defined action plan must be kept ready for emergencies.
7. It is necessary to realize that information security cannot be achieved just by creating a technical infrastructure. In reality, security success belongs to employees. It should not be forgotten that employees' attention to security will significantly affect the processes. Information security awareness and training programs should be held to achieve information security-conscious behavior.
8. Regular training and end-user awareness allow for the dissemination of knowledge on best practices and methods. Continuous awareness is also the basis for better understanding and participation. The importance to be given to this issue should be reminded by announcing information security accidents with different methods in the hospitals.
9. Managers should ensure the confidentiality, integrity, and availability of information in the institutions they work with. Without administrative support information security

programs can only remain just a recommendation. If the necessary support and incentives and resources are not provided, the program can neither be effective nor accepted by employees.

10. Healthcare processes have to be analyzed to obtain both good information flow and protection. Supplementary innovations of technical solutions for logging management, access control, and authentication for the healthcare sector are needed as well.
11. Furthermore, it is of great importance for the healthcare business to obtain sufficient follow-up routines for compliance and education of users to achieve a high level of security awareness in the healthcare field.
12. Using a new developed techniques like the blockchain will enhance the level of information security in the health sector.

6.5 Directions for Future Work

Future studies should address the limitations and extend the findings in this research, into future projects.

1. Involving the patients in a such information security study to know the extent to which patients are aware of the importance and value of their medical information and their eagerness to preserve it.
2. Analyzing the roles of the healthcare workers to find out the amount of medical information needed to complete treatment operations and to give privileges accordingly.
3. The study of security risk management will be the cornerstone of the application of any information security policy.
4. Applying the study to all government hospitals and comparing it to the private sector hospitals.

5. Study the readiness of Ministry of Health hospitals to implement the business continuity planning.
6. Mechanisms for facing information security threats in the Palestinian Ministry of Health.
7. Economic feasibility study for the application of international standards for information security in the Palestinian Ministry of Health.

6.6 Challenges and Limitations

The researcher had to deal with many challenges during the study conduction:

1- Differences in the language of the study with the preferred language of the respondents, which forced the researcher to translate and distribute Arabic version of the questionnaire .

2- The workload on health sector employees is due to the shortage of staff, and the increased number of patients because of the Corona pandemic and the medical staff contamination.

3- Declaring emergency procedures that would restrict mobility between governorates.

4- The people by nature didn't like questionnaires, thus the researcher encountered many complaints from the respondents, such as physicians who are well known for their unpleasant corporation.

5- There is a shortage of studies and statistics showing which security standards are most appropriate for information security policies.

6- Syndicates strike.

References

1. Abd Aljaber Y. (2013). The Degree of Effectiveness of Internal Control Procedures in Providing Electronic Information Security in Jordanian Manufacturing Companies. Master Thesis. Al-Aqsa University-Gaza. http://scholar.alaqsa.edu.ps/id/eprint/5006
2. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big Data Security and Privacy in Healthcare: A Review. *Procedia Computer Science*, *113*, 73–80. https://www.sciencedirect.com/science/article/pii/S1877050917317015. Accessed February 18, 2021.
3. Al-Ajez, I. (2011). The role of organizational culture to activate the application of e-management. Islamic University of Gaza, Palestine.
4. Al-Buhaisai, M., and Al-Sharif, H. (2008). Threats that affect computrised accounting information systems: Case study of the banks in Gaza Strip – Palestine. IUG Journal of Humanities Research. Gaza. 16(2). Pp 895-923.
5. Al-Danaf, A. F. (2013). The reality of information systems security management in technical colleges in the Gaza Strip and ways to develop them. Gaza, Palestine.
6. Al-Gharbi, K. N., Gattoufi, S. M., Al-Badi, A. H., & Al-Hashmi, A. A. (2015). Al-Shifa Healthcare Information System in Oman: A Debatable Implementation Success. *The Electronic Journal of Information Systems in Developing Countries*, *66*(1), 1–17. https://doi.org/10.1002/j.1681-4835.2015.tb00471.x
7. Alhassan, M, M., & Adjei-quaye, A. (2017). *Information Security in an Organization.* The International Journal of Computer (IJC). Global Society of Scientific Research and Researchers. http://ijcjournal.org/
8. Alhelou, A. (2021). Personal communication. Director of compiter and engineering unit at Palestinian Ministery of Health.
9. Al-Otaibi, O. (2010). Information security on websites and its compatibility with local and international standards. Naif Arab University for Security Sciences. KSA. Ph.D. Thesis. Pp 207-213. http://repository.nauss.edu.sa/123456789/50817
10. Al-Qahtani, M. (2008). Information security threats and ways to confront them: a survey study on the employees of the Computer Center of the Royal Saudi Naval Forces in Riyadh. Naif Arab University for Security Sciences. KSA. Master Thesis.
11. Amer K. (2015). Informatics: ethical use of genomic information and electronic medical records, J Am Nurses Assoc;20(2).
12. Anderson J, and Goodman K. (2002). Ethics and Information Technology: A Case-Based Approach to a Health Care System in Transition. ED. (1), (pp. 63–112). Springer New York. https://doi.org/10.1007/978-0-387-22488-6_4
13. Antonio F. Trillo-Cabello, Jesús A. Carrillo-Castrillo, Juan C. Rubio-Romero. (2020). Perception of risk in construction. Exploring the factors that influence experts in occupational health and safety, Safety Science, 10.1016/j.ssci..104990, 133, (104990), (2021).
14. Appari, A. and Eric Johnson, M. (2010). 'Information security and privacy in healthcare: current state of research, Int. J. Internet and Enterprise Management, Vol. 6, No. 4, pp.279–314.
15. Asress B M. (2014). Health Information Systems in Ethiopia. Addis Ababa, Ethiopia. Accessed April 23, 2021.
16. Atchinson, Brian K.; Fox, Daniel M. (1997). "The Politics of the Health Insurance PortabilityandAccountabilityAct" (PDF). http://www.library.armstrong.edu/eres/docs/er

es/MHSA86351_CROSBY/8635_week2_HIPAA_politics.pdf **16** (3):146-150. doi:10.1377/hlthaff.16.3.146. PMID 9141331. Archived from the original (PDF) on 2014-01-16. Retrieved 2021-05-21.

17. Australian Privacy Act. (1988). (Cth).
18. Bjorck, F. (2005). Discovering Information Security Management. Unpublished Ph.D. Thesis, Sweden: Stockholm University & Royal Institute of Technology.
19. Centers for Medicare and Medicaid Services (CMS). (2016). HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules.1–8.https://www.cms.gov/Outreach-and-Education/Medicare-LearningNetworkMLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf%0Ahttps://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf
20. Chiang, TungJu, Jen ShiangKouh, and Ray-I. Chang. (2009). "Ontology-based risk control for the incident management." International Journal of Computer Science and Network Security9.11: 181-189.
21. Clark, C., & McGhee, J. (Eds.). (2008). Private and confidential? Handling personal information in the social and health services. (pp. Iii-Iv). Bristol: Bristol University Press. doi:10.2307/j.ctt9qgtcv
22. Damschroder, L. J., Pritts, J. L., Neblo, M. A., Kalarickal, R. J., Creswell, J. W., & Hayward, R. A. (2007). Patients, privacy and trust: patients' willingness to allow researchers to access their medical records. *Social science & medicine (1982)*, *64*(1), 223–235. https://doi.org/10.1016/j.socscimed.2006.08.045
23. Davidson, P. L. (2002). A Complex Multi-Location Enterprise: Issues and Possible Solutions. In Healthcare Information Systems (pp. 89-100). Auerbach Publications.
24. Dhillon, G. (2001). Information security management: global challenges in the new millennium. Hershey, Pa.; London: Idea Group Pub.
25. Eguren, E, (2005). Protection Manual for Human Rights Deffenders. Peace Brigades International, European Office (PBI/BEO). Front Line for the Protection of Human Rights Deffenders. 16 Idrone Lane, Off Bath Place, Blackrock, County Dublin, Ireland.
26. eHealth Ontario. (2010). *Guide to Information Security for the Health Care Sector Information and Resources for Complex Organizations*. http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_Complex.
27. El-Gazzar, R., & Stendal, K. (2020). Blockchain in health care: hope or hype?. *Journal of Medical Internet Research*, *22*(7), e17199.
28. Eroğlu, Ş., & Çakmak, T. (2016). Enterprise Information Systems within the Context of Information Security: A Risk Assessment for a Health Organization in Turkey. *Procedia Computer Science*, *100*(July 2017), 979–986. https://doi.org/10.1016/j.procs.2016.09.262
29. Eroğlu, Ş.,& Çakmak, T. (2016). Enterprise Information Systems within the Context of Information Security: A Risk Assessment for a Health Organization in Turkey. Procedia Computer Science, 100 .doi: 10.1016/j.procs.2016.09.262
30. Farn, K.-J., Hwang, J.-M., & Lin, S.-K. (2007). Study on applying ISO/DIS 27799 to medical industry's ISMS. *Electrical and Computer Engineering*, *4*(8), 630–635.
31. Fenz, S., Plieschnegger, S., & Hobel, H. (2016). Mapping information security standard ISO 27002 to an ontological structure. Information & Computer Security, 24(5), 452-473.
32. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á., &Toval, A. (2013). Security and

privacy in electronic health records: a systematic literature review. *Journal of biomedical informatics*, *46*(3), 541–562. https://doi.org/10.1016/j.jbi.2012.12.003

33. Feyzabadi, V. Y., Emami, M., & Mehrolhassani, M. H. (2015). Health information system in primary health care: The challenges and barriers from local providers' perspective of an area In Iran. *International Journal of Preventive Medicine*, *2015*(July). https://doi.org/10.4103/2008-7802.160056
34. Filkins, B. L., Kim, J. Y., Roberts, B., Armstrong, W., Miller, M. A., Hultner, M. L., Castillo, A. P., Ducom, J. C., Topol, E. J., & Steinhubl, S. R. (2016). Privacy and security in the era of digital health: what should translational researchers know and do about it?. American journal of translational research, 8(3), 1560–1580.
35. Flaumenhaft, Y., & Ben-Assuli, O. (2018). Personal health records, global policy and regulation review. In *Health Policy* (Vol. 122, Issue 8, pp. 815–826). Elsevier Ireland Ltd. https://doi.org/10.1016/j.healthpol.2018.05.002
36. Gray, D. E. (2014). Chapter 10: Designing descriptive and analytical surveys. Doing Research in the Real World, 3rd Edn.
37. Guo, K.H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security, 32(0), (pp. 242-251).
38. Gupta, B. B., & Agrawal, D. P. (Eds.). (2019). Handbook of research on cloud computing and big data applications in IoT. IGI Global.
39. Hamidovic H, and Kabil J. (2011). J An Introduction to Information Security Management in Health Care Organizations. VOLUME 5. (www.isaca.org/journal). Accessed 12 May 2021.
40. Hassan, A. A. A. M. (2013). Information Security Management for Strategic and Effective Implementation of e-Management in the Governmental Institutions in Gaza. *Asian Journal of Business Information Management*, *20*(13), 67–74. Mater thesis.
41. Hoffman, S. and Podgurski, A. (2007). Securing the HIPAA Security Rule. Journal of Internet Law, Case Legal Studies Research Paper No. 06-26, Available at SSRN: https://ssrn.com/abstract=953670 Accessed April 03, 2021.
42. https://www.mtit.pna.ps/ 2021). Accessed 21 May 2021.
43. IBM Corp. Released (2013). IBM SPSS Statistics for Windows, Version 23.0. Armonk, NY: IBM Corp.
44. ISO. (2016). Health informatics — Information security management in health using ISO/IEC 27002. Edition**:** 2 Technical Committee ISO/TC 215 Health informatics. Accessed 21 May 2021.
45. James, D. G. (2007). HIPAA Related Information Security Concerns In Health Care 1 HIPAA In Health Care: Information Security in a Health Care Environment Daniel G. James. 1–15.
46. Jannetti, M. (2014). Safeguarding patient information in electronic health records. *AORN Journal*, *100*(3). pp. C7-C8, https://doi.org/10.1016/S0001-2092(14)00873-4
47. Karasneh, R. A., Al-Azzam, S. I., Alzoubi, K. H., Hawamdeh, S. S., & Muflih, S. M. (2019). Patient data sharing and confidentiality practices of researchers in Jordan. *Risk Management and Healthcare Policy*, *12*, 255–263. https://doi.org/10.2147/RMHP.S227759
48. Khalifa, M. (2017). Perceived benefits of implementing and using hospital information systems and electronic medical records. *Studies in Health Technology and Informatics*, *238*, 165–168. https://doi.org/10.3233/978-1-61499-781-8-165
49. Kovalenko, O., & Kovalenko, T. (2018). Knowledge Model and Ontology for Security

Services. In *2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC)* (pp. 1-4). IEEE.

50. Kreicberga, L. (2010). Internal Threat Information Security –Countermeasures and human factor within SME, Master Thesis, Sweden: Luela University Of Technology.
51. Lemke, J. (2013). Storage and security of personal health information. *OOHNA J*, *32*(1), 25-26.
52. Liu, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. *Jama*, *313*(14), 1471-1473.
53. Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health Information Security in Hospitals: the Application of Security Safeguards. *Actainformaticamedica : AIM: journal of the Society for Medical Informatics of Bosnia & Herzegovina: casopisDrustvazamedicinskuinformatikuBiH*, *24*(1), 47–50. https://doi.org/10.5455/aim.2016.24.47-50
54. Ministry of Telecommunication and Information Technology. (n.d.). Retrieved September 17, 2020, from https://www.mtit.gov.ps/
55. Mishah, N., Albukhari, A., AlMutairi, B., & Mohreq, M. (2019). Status of e-security and privacy protection in Saudi hospitals. *Computer Methods and Programs in Biomedicine*, *171*(August), 5–6. https://doi.org/10.1016/j.cmpb.2018.12.012
56. MoH. (2016). MoH Service Purchase Unit Referral Procedures Manual for Israeli Hospitals and Referral Procedures Manual for Palestinian Non-PMoH Referral Facilities Accessed 26 May 2021.
57. Molok A, and Nuha N. (2011). Disclosure of organizational information by employees on Facebook: Looking at the potential for information security risks. 22nd Australasian Conference on Information Systems,
58. Nemasisi, E. (2007). A Legal Compliance Model for Privacy and Confidentiality in South African Rural Hospitals. In Academic Dissertation, Nelson Mandela Metropolitan University. South Africa.
59. Nguyen, L. (2019). Information Security in Healthcare: An exploratory study of hospitals in Vietnam. *May*.
60. NIST. (2012). NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. *NIST Special Publication*, *September*, 95. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf%0Ahttp://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf%0Ahttp://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf%5Cnhttp://csrc.n
61. Olifer, D. (2015). "Evaluation metrics for ontology-based security standards mapping," *Open Conference of Electrical, Electronic and Information Sciences (eStream)*, pp. 1-4, DOI: 10.1109/eStream.2015.7119494
62. Ormandjieva, O., El Barachi, M., & Khelifi, A. (2012). Guide to ISO 27001: UAE Case Study. *Issues in Informing Science and Information Technology*, *9*(October 2018), 331–349. https://doi.org/10.28945/1625
63. Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in clinical research*, *6*(2), 73–76. https://doi.org/10.4103/2229-3485.153997
64. Palestinian health capacity project. (2018). MoH saves money, improves quality of care through its health information system. Washington DC: USAID and Intra health International; (https://www.intrahealth.org/sites/ihweb/files/attachment-

files/phcphistubasimplementation.pdf, Accessed 17 March 2021).
65. Palestinian National Authority (PNA). (2017). Presidential Decree No. 16 of 2017 Regarding Cybercrime.
66. Park, W. S., Seo, S. W., Son, S. S., Lee, M. J., Kim, S. H., Choi, E. M., Bang, J. E., Kim, Y. E., Kim, O. N. (2010). Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. Healthcare Informatics Research, 16(2), 89-99.
67. PNIPH. (2021). Retrieved May 14, 2021, from https://pniph.org/en/about/about-pniph. https://pniph.org/index.php/en/pniph-focus-area/health-systems-and-registries
68. Popescul, D. (2011). The confidentiality-integrity-accessibility triad into the knowledge security: A reassessment from the point of view of the knowledge contribution to innovation. Innovation and Knowledge Management: A Global Competitive Advantage - Proceedings of the 16th International Business Information Management Association Conference, IBIMA 2011, 4(June 2011), 1821–1828.
69. Pritts J. (2008). The importance and value of protecting the privacy of health information: Roles of HIPAA Privacy Rule and the Common Rule in health research. http://www.iom.edu/CMS/3740/43729/53160.aspx.
70. Ranong, P. N., & Phuenngam, W. (2009). Critical success factors for effective risk management procedures in financial industries: a study from the perspectives of the financial institutionsin Thailand (Master's thesis). 1–76. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A233985&dswid=9415
71. Report, F. (n.d.). Security of eGovernment Systems Final Report.
72. Rinehart-Thompson LA, Harman LB. Privacy and confidentiality. In: Harman LB, editor. Ethical Challenges in the Management of Health Information. 2nd ed. Sudbury, MA: Jones and Bartlett; 2006. p. 53
73. Rodrigues, J. J. P. C., De La Torre, I., Fernández, G., & López-Coronado, M. (2013). Analysis of the security and privacy requirements of cloud-based electronic health records systems. Journal of Medical Internet Research, 15(8), 1–9. https://doi.org/10.2196/jmir.2494
74. Rognehaugh R. (1999).The Health Information Technology Dictionary. Gaithersburg, MD: Aspen; p. 125.
75. Sahma,T., Simpson, L., and Lane, B. (2013). Security and Privacy in eHealth: Is it possible? A sociotechnical analysis. Paper Presented at 15th International Conference on e-Health networking, Applications and Services, Lisbon, Portugal. Available from: https://www.researchgate.net/publication/269329631_Security_and_Privacy_in_eHealth_Is_it_possible [accessed May 20 2021].
76. Shehada, F., & Bader, M. (2020). (The Reality of Electronic Information Security in Bank of Palestine "Case Study"). SSRN Electronic Journal, 2020, 1–26. https://doi.org/10.2139/ssrn.3686554
77. Shoniregun C.A., Dube K., and Mtenzi F. (2010). Electronic Healthcare Information Security. Vol. 53. London – UK, New Zealand and Dublin - Ireland. https://doi.org/10.1007/978-0-387-84919-5.
78. Smith, A. M., & Toppel, N. Y. (2009). Case study: Using security awareness to combat the advanced persistent threat. Paper presented at the 13th Colloquium for Information Systems Security Education (CISSE), University of Alaska, Fairbanks, Seattle.
79. Solms, B., & Solms, R. v. (2004). The 10 deadly sins of information security management. *Computers and security, ELSEVIER, 23*, 371-376.

80. Sophos. (2010). Security Threat Report: 2010. Boston, Massachusetts: Sophos Group. https://www.researchgate.net/publication/49280707_Information_Leakage_through_Online_Social_Networking_Opening_the_Doorway_for_Advanced_Persistence_Threats [accessed May 11 2021].
81. Stoneburner G, Goguen A, and Feringa A. (2002). Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930. (Vol. 1).
82. Straub, Detmar W., and Richard J. Welke. (1998) "Coping with systems risk: security planning models for management decision making." MIS quarterly: 441-469.
83. Takura B, and Jomin G. (2019). Security, Confidentiality and Privacy in Health of Healthcare Data." Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.373-377, URL:https://www.ijtsrd.come-ISSN:2456-6470from: https://www.researchgate.net/publication/334050168_Security_Confidentiality_and_Privacy_in_Health_of_Healthcare_Data [accessed May 21, 2021].
84. Tan, J. (2005). Ed, E-Health Care Information Systems, United States of America, San Francisco: ossey-Bass.
85. Tandon, A., Dhir, A., Islam, N., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Computers in Industry*, *122*, 103290.
86. Tayeh, A. M. (2008). Effectiveness of Information Security Management at the Palestinian Information Technology Companies. Master thesis.
87. Tezera R. (2013). E-health Policies in the Ethiopian Policy and Strategy Documents. Addis Ababa, Ethiopia. Master Thesis.
88. Tham, I. (2018). Singapore's privacy watchdog to investigate SingHealth data breach. Available from https://www.straitstimes.com/singapore/singapores-privacy-watchdog-to-investigate-singhealth-data-breach.
89. Truta, T.M., Fotouhi, F., Barth-Jones, D. (2004) "Assessing Global Disclosure Risk in Masked Microdata," *Workshop on Privacy in Electronic Society.*
90. UNAIDS. (2007). Guidelines on Protecting the Confidentiality and Security of Hiv Information : Proceedings from a Workshop. May 2006, 1–61.
91. United States Department of Health Human Services. (2003). Summary of the HIPAA Privacy Rule. OCR Privacy Brief. HIPAA Compliance Assistance. https://www.stimmel-law.com/en/articles/hipaa-basic-privacy-law-health-insurance-portability-and-accountability-act-1996
92. Utbult, M., Holmgren, A., Larsson, R., Lindwall, C.L. (2004). ‟Patientdata – brist och överflöd i vården.‟ *Teldok rapport, Almqvist & Wiksell*, Uppsala, Sweden.
93. Van de Castle, B., Kim, J., Pedreira, M. L., Paiva, A., Goossen, W., & Bates, D. W. (2004). Information technology and patient safety in nursing practice: an international perspective. International journal of medical informatics, 73(7-8), 607–614. https://doi.org/10.1016/j.ijmedinf.2004.04.007
94. Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in health information management*, *11*(Fall).

95. Win, K. T., & Susilo, W. (2015). A Systematic Literature Review on Security and Privacy of Electronic Health A systematic literature review on security and privacy of electronic health record systems : technical perspectives. https://doi.org/10.12826/18333575.2015.0001.Rezaeibagha
96. Wirken, G. (2012). Information security in Dutch hospitals. *January*. http://igitur-archive.library.uu.nl/student-theses/2012-0620-200514/UUindex.html
97. Wyatt J C, and Sullivan F. (2005). What is health information? *BMJ* 331:566 doi:10.1136/bmj.331.7516.566
98. Yaraghi, N., & Gopal, R. D. (2018). The role of HIPAA omnibus rules in reducing the frequency of medical data breaches: Insights from an empirical study. The Milbank Quarterly, 96(1), 144-166.
99. Yarmohammadian, M. H., Raeisi, A. R., Tavakoli, N., & Nansa, L. G. (2010). Medical record information disclosure laws and policies among selected countries; a comparative study. *Journal of research in medical sciences: the official journal of Isfahan University of Medical Sciences*, *15*(3), 140–149.
100. Zayar, S. (2014). The introduction of digital risk management to counter the risks of using information technology: a field study in a sample of Iraqi banks.
101. Zulman, D. M., Nazi, K. M., Turvey, C. L., Wagner, T. H., Woods, S. S., & An, L. C. (2011). Patient interest in sharing personal health record information: a web-based survey. *Annals of internal medicine*, *155*(12), 805-810.

APPENDICES

Appendix A: Arbitrators table

No	Name	Place of work
1	Prof. Mohammad Awad	American Arab University
2	Dr. Rami Hodrob	American Arab University
3	Dr. Abed Alkareem Awwad	Beirzait University
4	Mr. Ali Alhelou	Ministry of Health
5	Mr. Alaa Alzarier	Yatta Hospital
6	Mr. Yurub Awwad	Ministry of Telecommunication

Appendix B: Computer and engineering department Arabic Questionnaire

الجامعة العربية الأمريكية
ARAB AMERICAN UNIVERSITY

الأخوة / الأخوات موظفي وحدة الهندســـة والحاســـــوب حفظكم الله ورعاكم،،،

السلام عليكم ورحمة الله وبركاته ،،،

يقوم الباحث باجراء دراسة بعنوان

"أمن وخصوصية المعلومات الطبية في وزارة الصحة الفلسطينية"

"وذلك استكمالاً لمتطلبات الحصول على درجة الماجستير في المعلوماتية الصحية في الجامعة العربية الأمريكية

ولهذا الغرض قام الباحث ببناء هذه الاستبانة التي بين أيديكم لمعرفة واقع امن المعلومات في وزارة الصحة.

ونظرا لاهمية ارائكم في هذه الدراسة، يرجو الباحث تعاونكم الجاد والصادق لإنجاح هذه الدراسة من خلال التكرم بالإجابة عن جميع فقرات الاستبانة بدقة وعناية وموضوعية وأن تكون الإجابة معبرة عن ارائكم، علماً بأن المعلومات الواردة في هذه الاستبانة ستحظى بالسرية التامة ولن تستخدم الا لأغراض البحث العلمي فقط".

وشكرا جزيلا على وقتكم

الباحث: محمد صلاح الدين

الجزء الاول: معلومات عامة

الرجاء وضع اشارة "X" أمام الإجابة الصحيحة

1-الجنس : ذكر ☐ انثى ☐

2-المستوى التعليمي : دبلوم ☐ بكالويوس ☐ ماجستير ☐

3-سنوات الخبرة : اقل من 10 سنوا ت ☐ من 11 -20 سنة ☐ أكثر من 20 سنة ☐

4- المسمى الوظيفي : مهندس ☐ مبرمج ☐ تكنولوجيا معلومات ☐

الجزء الثاني : أمن المعلومات

الجزء الاول : الأمن الاداري						
الرقم	**الفقرات**	**اوافق بشدة**	**اوافق**	**محايد**	**اعارض**	**اعارض بشدة**
1	يتم تحديد جميع المخاطر الأمنية المحتملة ، بما في ذلك التهديدات ونقاط الضعف للتطبيقات ونظم المعلومات					
2	يوجد سياسات واضحة وفاعلة لتقيم الثغرات ونقاط الضعف في نظام امن المعلومات					
3	يتم تطبيق إجراءات تأديبية رسمية على الموظفين الذين ينتهكون إجراءات وسياسات أمن المعلومات في المستشفى					
4	يتم الطلب من الموظفين التوقيع على تعهد بعدم الافصاح عن المعلومات الطبية					
5	هناك جهة محددة ومعروفة مسؤولة عن صياغة ومراجعة وتحديث سياسات أمن المعلومات					
6	يتم اعطاء الموظفين صلاحيات بناء على وصفه الوظيفي ومهامه اليومية ويطلب من الادارة					
7	يتم إلغاء جميع الامتيازات المتعلقة بنظام المعلومات في حال انتقال او استقالة الموظف فورا					
8	يمنع مشاركة كلمات المرور بين الموظفين أو إفشاء سريتها					
9	يوجد سياسة صارمة لكلمة المرور كتحديد الحد الأدنى لطول هذه الكلمة وطبيعتها ومدة صلاحيتها ، بالإضافة إلى وجود إرشادات توضح كيفية اختيارها					
10	يتلقى جميع الموظفين تدريبا مناسبا خاصا بأمن المعلومات، ويتم إطلاعهم على آخر التحديثات على سياسات وإجراءات أمن المعلومات في المستشفى					
11	يتم استخدام برامج مكافحة وزاله الفيروسات ويتم تحديث هذه البرامج باستمرار					
12	يوجد نظام لمراقبة الشبكة والسيرفرات والاجهزة الرئيسية المشغلة للنظام					
13	يوجد خطة لإعادة الأعمال إلى طبيعتها بعد حدوث إخفاق في النظام أو انقطاع في أداء العمل					
14	يتم تنفيذ النسخ الاحتياطي على فترات منتظمة					
15	يتم مراجعة نشاطات النسخ الاحتياطي بشكل منتظم					
16	يتم توثيق آليات النسخ الاحتياطي والاسترداد و تفحص بشكل دوري وتنفذ بشكل سليم					

الجزء الثاني : الامن الفيزيائي						
الرقم	الفقرات	اوافق بشدة	اوافق	محايد	اعارض	اعارض بشدة
17	تطبق معايير الامن المادي على جميع الاجهزة المسؤوولة عن تشغيل النظام لمنع الوصول للاشخاص غير المصرح لهم					
18	تقام مراكز البيانات وأقسام المعلومات في أماكن ومواقع جيدة ومحمية ومؤمنة					
19	الغرف التي تحتوي على الأجهزة والمعلومات تكون مغلقة أو بها خزانات آمنة يمكن إغلاقها					
20	المعلومات متاحة فقط على أساس الحاجة لها، بمعنى أنه يوجد ضوابط تحكم دخول الأفراد الخارجيين					
21	يوجد قائمة بأسماء الأشخاص المسموح لهم الوصول إلى مراكز البيانات وغرف الكمبيوتر وما شابه، ويتم مراجعة وتحديث القائمة بشكل دوري					
22	UPSالأجهزة محمية من انقطاع الكهرباء، بمعنى أنه يوجد في المستشفى مولد كهرباء احتياطي بالاضافة الى اجهزة لتخزين الطاقة					
23	يتم تحديد انواع ومواصفات الاجهزة التي تستطيع تشغيل النظام متل اللابتوبات واجهزة الكمبيوتر					
24	يتم التخلص جيدا من أجهزة حفظ البيانات التي تحتوي على بيانات حساسة وتتعطل أو تصبح لا لزوم لها وذلك بالإتلاف أو الكتابة فوقها					
25	يتم تأمين شاشة الحاسوب بشكل يدوي أو آلي عند عدم استخدامها لفترة ما					
26	يتم وضع وسائط النسخ الاحتياطي التي تحتوي على المعلومات الأساسية أو الحساسة على مسافة آمنة من الموقع الرئيسي من أجل تفادي الأضرار الناجمة عن كارثة في الموقع الرئيسي					

الجزء الثالث : الامن التقني						
الرقم	الفقرات	اوافق بشدة	اوافق	محايد	اعارض	اعارض بشدة
27	يوجد حساب اسم مستخدم / وكلمة مرور خاص لكل مستخدم ولا يتم استخدام حسابات عامة يستخدمها أكثر من شخص					
28	يتم الخروج تلقائيا من النظام بعد انقضاء مدة زمنية محددة ومعروفة بدون اجراء اى حركات					
29	يتم استخدام تقنيات التشفير في الاتصال بين المستشفى ومركز البيانات الرئيس لحماية بيانات المرضى					
30	توجد إجراءات معمول بها لتوفير الوصول المناسب إلى بيانات السجلات الطبية الإلكترونية في حالات الطوارئ					
31	توجد آليات رقابة تدقيق يمكنها مراقبة وتسجيل و / أو فحص نشاط نظام المعلومات					
32	يتم تنفيذ آلية مصادقة وتحقق لأولئك الذين يسعون للوصول إلى نظام السجلات الطبية الإلكترونية					
33	يتم اتباع اجراءات مناسبة للتاكد من حفظ المعلومات الطبية من التعديل او التغيير او الاتلاف بطريقة غير مصرح بها					

Appendix C: Computer and engineering department English Questionnaire

الجامعة العربية الأمريكية
ARAB AMERICAN UNIVERSITY

Dear Sir/Madam

The researcher is conducting a study about:

Information Security and privacy in Palestinian Ministry of Health

"*This is to complement the requirements for obtaining the master degree in Health informatics from Arab American University.*

For this purpose, the researcher has developed this questionnaire - which is in your hands - to recognize the adoption Level of information security in the Mistry of Health.

Given the importance of your opinion in this study, the researcher hopes for your serious and sincere cooperation for the success of this study through answering all the questions of this questionnaire carefully and objectively, where the answers should express your opinions.

Note that the information contained in this questionnaire will be confidential and will only be used for research purposes".

Thank you very much for your time

Researcher: Mohammad Salaheddeen

Part one: General Information

Please place an (x) next to the answer:

1. Gender: ☐ Male ☐ Female

2. Education ☐ Diploma ☐ Bachelor ☐ Master

3. Years of Experience: ☐ ≤ 10 years ☐ 11 to 20 years ☐ > 20 years

4. Job description: ☐Engineer ☐ Programmer ☐Information Technology

Second Part: information security

Part A: Administrative Safeguards						
No.	**Item "Question"**	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
1	All potential security risks, including threats and vulnerabilities to applications and information systems, are identified					
2	There are clear and effective policies in place to assess gaps and weaknesses in the information security system					
3	Formal disciplinary action applies to employees who violate the hospital's information security procedures and policies					
4	Employees are required to sign an undertaking not to disclose medical information as part of their terms of employment					
5	There is a defined and recognized entity responsible for drafting, reviewing, and updating information security policies					
6	The employees are given privileges based on their job description and their daily tasks and upon the request of the management					
7	All privileges related to the information system will be canceled in the event of the employee's transfer or resignation immediately					
8	It is forbidden to share passwords between employees or divulge their confidentiality					
9	There is a strict policy for the password, such as specifying the minimum length, nature, and validity of this word, in addition to having instructions explaining how to choose it					
10	All staff receive appropriate information security training and are kept informed of the latest updates on the hospital's information security policies and procedures					
11	Anti-virus and virus removal programs are used and these programs are constantly updated					

12	There is a system for monitoring the network, the servers, and the main devices operating the system					
13	There is a plan to return the business to normal after a system failure or interruption in business performance					
14	Backups are performed at regular intervals					
15	Backup activities are reviewed regularly					
16	The backup and recovery mechanisms are documented and examined periodically and properly implemented					

Part B: Physical Safeguards

No.	Item "Question"	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
17	physical security standards are applied to all devices responsible for operating the system to prevent unauthorized access					
18	Data centers and information departments are set up in good and secured places and locations					
19	Rooms containing devices and information are locked or have secure lockers that can be locked					
20	Information is only available based on need, meaning that there are controls in place to control the entry of outside personnel					
21	There is a list of people who are allowed access to data centers, computer rooms, and the list is reviewed and updated periodically					
22	The hospital has a backup generator as well as energy storage devices "UPS"					
23	all types of workstations that access HIS data have been identified, such as laptops, desktop computers					
24	Data storage devices that contain sensitive data are disrupted or become unnecessary by being destroyed or overwritten					
25	The computer screen is locked manually or automatically when not in use for a while					
26	Backup media containing basic or sensitive information is placed at a safe distance from the main site to avoid damage from a disaster in the main site.					

Part C: Technical Safeguards						
No.	**Item "Question"**	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
27	each workforce member has a unique user identifier and public accounts are not used					
28	System logged out automatically after a predetermined time of inactivity					
29	The connection between the hospital and data center is secured and the transmitted data is encrypted					
30	There are policies and procedures to provide appropriate access to HIS data in emergency					
31	There are audit control mechanisms that can monitor, record, and/or examine the activity of the information system					
32	An authentication and verification mechanism are implemented for those seeking access to the electronic medical records system					
33	Appropriate procedures are followed to ensure that medical information is preserved from modification, alteration, or destruction in an unauthorized manner					

Appendix D: Palestine Medical Complex Arabic Questionnaire

الجامعة العربية الأمريكية
ARAB AMERICAN UNIVERSITY

الأخوة / الأخوات العاملون في مجمع فلسطين الطبي حفظكم الله ورعاكم،،،

السلام عليكم ورحمة الله وبركاته ،،،

يقوم الباحث باجراء دراسة بعنوان

"أمن وخصوصية المعلومات الطبية في وزارة الصحة الفلسطينية"

"وذلك استكمالاً لمتطلبات الحصول على درجة الماجستير في المعلوماتية الصحية في الجامعة العربية الأمريكية

ولهذا الغرض قام الباحث ببناء هذه الاستبانة التي بين أيديكم لمعرفة واقع امن المعلومات في وزارة الصحة.

ونظرا لاهمية ارائكم في هذه الدراسة ، يرجو الباحث تعاونكم الجاد والصادق لإنجاح هذه الدراسة من خلال التكرم بالإجابة عن جميع فقرات الاستبانة بدقة وعناية وموضوعية وأن تكون الإجابة معبرة عن آرائكم، علماً بأن المعلومات الواردة في هذه الاستبانة ستحظى بالسرية التامة ولن تستخدم إلا لأغراض البحث العلمي فقط".

وشكرا جزيلا على وقتكم

الباحث: محمد صلاح الدين

الجزء الاول: معلومات عامة

الرجاء وضع اشارة "X" امام الاجابة الصحيحة

1-الجنس : ذكر ☐ انثى ☐

2-المستوى التعليمي : دبلوم ☐ بكالويوس ☐ ماجستير ☐ دكتوراه ☐ البورد ☐

3-سنوات الخبرة : اقل من 10 سنوا ت ☐ من 10 -≤ 20 سنة ☐ أكثر من 20 سنة ☐

4- المسمى الوظيفي : طبيب ☐ ممرض ☐ موظف تسجيل ☐ فني مختبر ☐ فني اشعة ☐

اداري ☐ غير ذلك ☐ .....

الجزء الثاني : أمن المعلومات

الرقم	**المجال الأول: سياسة الأمن Security Policy**	**اوافق بشدة**	**اوافق**	**محايد**	**اعارض**	**اعارض بشدة**
1	يوجد في المستشفى سياسة لأمن المعلومات معتمدة من قبل الإدارة ويعرفها جميع الموظفين.					
2	سياسة أمن المعلومات الموجودة تبين مدى التزام الإدارة وطريقة المستشفى في إدارة أمن المعلومات.					
3	هناك شخص محدد ومعروف مسؤول عن سياسة أمن المعلومات ويقوم بمراجعة تلك السياسة وتحديثها .					
	المجال الثاني: الأمن التنظيمي Organizational Security	**اوافق بشدة**	**اوافق**	**محايد**	**اعارض**	**اعارض بشدة**
4	يوجد في المستشفى فريق (مكون من أفراد ممثلين لجميع الأقسام) مسؤول عن إدارة أمن المعلومات.					
5	تم تحديد مسؤوليات حماية معلومات المرضى وتنفيذ عمليات أمنية محددة بوضوح.					
6	يمنع الموظف من استخدام المعلومات الطبية للإغارض غير المصرح بها.					
	المجال الثالث: الأفراد وأمن المعلومات Personnel Security	**اوافق بشدة**	**اوافق**	**محايد**	**اعارض**	**اعارض بشدة**
7	تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في المستشفى.					
8	يتم الطلب من الموظفين التوقيع على تعهد بعدم الإفصاح عن المعلومات الطبية كجزء من شروط توظيفهم.					
9	يتلقى جميع الموظفين تدريبا مناسبا خاصا بأمن المعلومات، ويتم إطلاعهم على آخر التحديثات على سياسات وإجراءات أمن المعلومات في المستشفى.					

10	تتبع المستشفى إجراءا رسميا لرفع التقارير بحوادث الأمن في المستشفى من خلال القنوات الإدارية المناسبة وبالسرعة الممكنة					
11	يوجد إجراءا رسميا يتبعه المستخدمون لرفع التقارير بمواطن الضعف والمخاطر الأمنية في الأنظمة والخدمات.					
12	يتم تطبيق إجراءات تأديبية رسمية على الموظفين الذين ينتهكون إجراءات وسياسات أمن المعلومات في المستشفى.					
13	تم اتخاذ اجراءات تاديبية بحقك بسبب مجال امن المعلومات					
	المجال الرابع: ضبط الوصول للأنظمة System Access Control	**اوافق بشدة**	**اوافق**	**محايد**	**اعارض**	**اعارض بشدة**
14	يوجد عملية دورية لمراجعة صلاحيات المستخدمين في الوصول للنظام.					
15	يتم اعطاء الموظفين صلاحيات بناءا على وصفه الوظيفي ومهامه اليومية.					
16	يوجد توجيهات مطبقة لإرشاد المستخدمين في اختيار كلمات المرور والمحافظة عليها.					
17	يوجد حساب (اسم مستخدم/ وكلمة مرور) خاص لكل مستخدم مثل الفنيون ومديرو الأنظمة والمشغلون.					
18	يستطيع الموظفون الوصول الى شبكة الانترنت بسهولة.					
	المجال الخامس: تطوير وصيانة الأنظمة Systems Development and maintenance	**اوافق بشدة**	**اوافق**	**محايد**	**اعارض**	**اعارض بشدة**
19	يتم التحقق من صحة البيانات المدخلة.					
20	يوجد ضوابط مطبقة على تنزيل البرامج على اجهزة الحاسوب، وذلك بهدف تقليل مخاطر تعرض أنظمة التشغيل للتلف.					
21	يتم إجراء صيانة مستمرة لاجهاز الكمبيوتر الخاص بك					
22	يوجد اجهزة امداد الطاقة ups في القسم عند انقطاع التيار الكهربائي					
23	فقط فنيو المؤسسة يمكنهم تثبيت البرامج على جهاز الكمبيوتر الخاص بك					
24	يوجد مضاد للفايروسات على جهازك					
	المجال السادس: تخطيط استمرارية العمل Business Continuity Planning	**اوافق بشدة**	**اوافق**	**محايد**	**اعارض**	**اعارض بشدة**
25	يتعرض النظام الى اعطال بشكل متكرر .					
26	يتم ابلاغ مسؤولي النظام باي عطل او انقطاع عن العمل فور حدوثه .					
27	يوجد خطة لإعادة الأعمال إلى طبيعتها بعد حدوث إخفاق في النظام أو انقطاع في أداء العمل.					
28	يتم ادخال معلومات المرضى على النظام فور عودته الى العمل .					
29	يتم اختبار خطط استمرارية العمل بشكل دوري للتأكد من أنها محدثة وفعالة.					
	المجال السابع :افشاء البيانات Data Disclosure	**اوافق بشدة**	**اوافق**	**محايد**	**اعارض**	**اعارض بشدة**
30	يتم تبادل اسم المستخدم وكلمة المرور بين الموظفين بسهولة					
31	تقوم باغلاق الحساب الخاص بك فور انتهائك من العمل					
32	يطلب منك الافصاح عن معلومات المرضى في اطار غير رسمي					
33	تقوم باعطاء معلومات عن المرضى في حال طلب منك زملاؤك ذلك					
34	يتم مشاركة المعلومات الطبية بين الاخصائيين بعد الحصول على موافقة من المرضى					

Appendix E: Palestine Medical Complex English Questionnaire

الجامعة العربية الأمريكية
ARAB AMERICAN UNIVERSITY

Dear Sir/Madam

The researcher conducts a study on:

Information Security and privacy in Palestinian Ministry of Health

"This is to complement the requirements for obtaining the master degree in Health informatics from Arab American University.

For this purpose, the researcher has developed this questionnaire - which is in your hands - to recognize the adoption Level of information security in the Mistry of Health.

Given the importance of your opinion in this study, the researcher hopes for your serious and sincere cooperation for the success of this study through answering all the questions of this questionnaire carefully and objectively, where the answers should express your opinions.
Note that the information contained in this questionnaire will be confidential and will only be used for research purposes ".

Thank you very much for your time

Researcher: Mohammad Salaheddeen

Part one: General Information

Please place an (X) next to the answer:

1. Gender: ☐ Male ☐ Female

2. Education ☐ Diploma ☐ Bachelor ☐ Master ☐ Ph.D. ☐ Board

3. Years of Experience: ☐ ≤ 10 years ☐ 11 to 20 years ☐ > 20 years

4. Job description: ☐ Doctor ☐ Nurse ☐ Registrar ☐ lab technician ☐ Rad technician

☐ Administrative ☐ other, Specify…….

Part Two: Information Security Fields

No:	Domain 1: Security Policy	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	There exists an information security policy known to all the employees.					
2	The existed information security policy states the hospital's approach to managing information security.					
3	There is a known and defined responsible department for information security policy and its review, maintenance, and upgrade					
	Domain 2: Organizational Security	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
4	There is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls.					
5	Responsibilities for the protection of patient information assets and for carrying out specific security processes were clearly defined.					
6	Employees are prohibited from using medical information for unauthorized purposes					
	Domain 3: Personnel Security	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
7	The employee's job description document contains his responsibilities and tasks towards information security in the hospital.					
8	Employees are asked to sign a confidentiality or nondisclosure agreement as a part of their initial terms and conditions of employment.					
9	All employees of the organization receive appropriate Information Security training.					
10	A formal reporting procedure exists, to report security incidents through appropriate management channels.					
11	A formal reporting procedure or guideline exists for users, to report security weakness in, or threats to, systems or services.					
12	There is a formal disciplinary process in place for employees who have violated organizational security policies and procedures.					

No:	Domain 1: Security Policy	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
13	Disciplinary measures have been taken against you due to the area of information security					
	Domain 4: System Access Control	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
14	There exists a regular process to review and evaluate user access rights and privileges.					
15	The employees are given privileges based on their job description and their daily tasks					
16	There are some guidelines in place to guide users in selecting and maintaining secure passwords.					
17	There is a unique account (username/password) for each user such as technicians, system administrators, and operators.					
18	Employees can easily access the Internet.					
	Domain 5: Systems Development and Maintenance	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
19	The entered data is validated.					
20	There are controls in place on installing software to computers, to reduce the risk of damage to operating systems.					
21	The computers are regularly maintained					
22	There are UPSs in the wards when the power is off					
23	Only hospital technicians can install software on your computer.					
24	There is an anti-virus installed on your PC					
	Domain 6: BCP	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
25	System crashes frequently.					
26	System administrators are notified of any malfunction or interruption of work as soon as it occurs.					
27	There is a plan to return the system to normal after a system failure or interruption in system performance.					
28	Patient information is entered into the system upon his return to work					
29	Work continuity plans are tested regularly to ensure that they are up to date and effective.					
	Domain 7: Data Disclosure	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
30	Username and password are easily exchanged between employees					
31	You Logout your account immediately when you finish your work					
32	You are asked unofficially to disclose the patients' information i.e for research					
33	You give information about patients if your colleagues ask to do so					
34	Medical information is shared between the specialists after obtaining consent from patients					

الملخص

تقييم أمن المعلومات الصحية وحماية الخصوصية في وزارة الصحة الفلسطينية

الخلفية: تلعب أنظمة المعلومات دورًا مهمًا في مؤسسات الرعاية الصحية التي تتعامل مع المعلومات الخاصة والحساسة للمرضى ، ونتيجة للاستخدام السريع واسع النطاق لأجهزة الكمبيوتر والإنترنت ، أصبح أمن المعلومات أحد أهم القضايا في مجال نظم المعلومات الصحية بسبب التهديدات المتزايدة والمخاطر التي تسببها .

الأهداف: هدفت هذه الدراسة الى تقييم مستوى امن المعلومات الصحية وحماية الخصوصية في وزارة الصحة الفلسطينية ومجمع فلسطين الطبي ، ومدى توافر الضمانات الادارية والمادية والفنية اللازمة لحماية انظمة المعلومات الصحية ،بالاضافة الى تقييم مدى تطبيق مجالات امن المعلومات وحماية الخصوصية لنظام المعلومات الصحية في وزارة الصحة ومجمع فلسطين الطبي .

المنهجية والاجراءات : استخدم الباحث المنهج الوصفي التحليلي حيث طور الباحث استبيانين هما: التحقيق في الضمانات الادارية والمادية والفنية في وزارة الصحة ، وكذلك تصورات موظفي القطاع الصحي العاملين في مجمع فلسطين الطبي، حيث قام الباحث باليحث في سبعة مجالات صحية امنية. اجريت الدراسة في الفترة ما بين اذار 2020 وايار 2021 .تمت دعوة الموظفين الذين يعملون في وزارة الصحة ومجمع فلسطين الطبي للمشاركة في هذه الدراسة باستخدام استبيانات ،تألف كادر وزارة الصحة لكافة موظفي وحدة الهندسة والحاسوب العاملين في المستشفيات الحكومية وعددهم 20 موظفا بنسبة استجابة (100%)،بينما تم تجنيد (142) موظفا يعملون في مجمع فلسطين الطبي باستخدام العينة الطبقية العشوائية لاختيار (142) من اصل (950) موظفا. كانت الاداة عبارة عن استبيان مشتق من الادبيات السابقة. علاوة على ذلك، تم اجراء التحليلات باستخدام الحزمة الاحصائية للعلوم الاجتماعية (SPSS).

النتائج والاستنتاجات: أظهرت الدراسة ان الاناث كانت اكثر تمثيلا من الذكور (*n*=93; 57%) مقابل (*n*=69; 43%)في كلا الموقعين.بالاضافة الى ذلك ، اعلنت الغالبية العظمى من الموظفين حصولها على درجات البكالوريوس (*n*=104; 64.2%) مقابل (*n*=30; 18.5%) درجة اعلى من مستوى درجة البكالوريوس. علاوة على ذلك فان (*n*=72; 44.4%) من الموظفين لديهم ما يصل الى 10-20 عاما من الخبرة في العمل . أخبر موظفو قسم الحاسوب والهندسة ان وزارة الصحة تطبق الضمانات

الامنية للحفاظ على امن و حماية خصوصية المعلومات الصحية بمستوى عالٍ (71.4٪)، حيث الامن المادي (75.5٪) والتقني (73.8٪) والامن الاداري (67.6٪). ومع ذلك، اوضح موظفو مجمع فلسطين الطبي ان مستوى تطبيق امن المعلومات للحفاظ على امن وخصوصية حماية المعلومات الصحية كان عند مستوى متوسط (66.6٪)، مع تخطيط استمرارية الاعمال(75.8٪)، تطوير وصيانة الانظمة(70.2٪)، السياسات التنظيمية (68.6٪)، الامن الشخصي(58٪)، وافشاء البيانات(61٪). كما اظهرت الدراسة انه توجد ارتباطات ذات دلالة معنوية موجبة على مستوى($\alpha \leq 0.05$) بين جميع مجالات امن المعلومات وامن و حماية خصوصية المعلومات الصحية في وزارة الصحة ومجمع فلسطين الطبي.

وخلصت الدراسة الى وجود معدل يتراوح بين متوسط الى مرتفع في تطبيق مجالات امن النظام ، بالاضافة الى الضمانات الامنية لامن وخصوصية المعلومات الصحية في وزارة الصحة الفلسطينية ومجمع فلسطين الطبي.

التوصيات : توحيد الجهود بين وحدة الهندسة والحاسوب وجميع المستشفيات الحكومية وانشاء وحدة امن معلومات متكاملة لصياغة وتنفيذ وتحديث ومراقبة تطبيق سياسة امن المعلومات الصحية ، ومن الضروري أيضًا لموظفي القطاع الصحي تلقي التدريب والتعليم المناسبين باستمرار للوصول إلى مستوى عالٍ من الوعي بأمن المعلومات في مجال الرعاية الصحية. علاوة على ذلك ، سيساعد تعيين كبير مسؤولي المعلومات في إدارة وتنظيم جميع التقنيات والمبادرات الأمنية في أنظمة المعلومات الصحية.