# Observational Measures for Effective Profiling of Healthcare Staffs' Security Practices

1st Prosper K. Yeng
Department of Information Security
and Communication Technology
*Norwegian University of Science
and Technology*
Gjøvik, Norway
prosper.yeng@ntnu.com

2st Bian Yang
Department of Information Security
and Communication Technology
*Norwegian University of Science
and Technology*
Gjøvik, Norway
bian.yang@ntnu.no

3rd Einar Arthur Snekkenes
Department of Information Security
and Communication Technology
*Norwegian University of Science
and Technology*
Gjøvik, Norway
einar.snekkenes@ntnu.no

***Abstract*—The healthcare sector is characterized with variant situations and services such as emergency services, *collaborations in patient care and patient referrals. These activities require erratic accesses and electronic exchange of personal health information (PHI) between health professionals and healthcare organizations. Also, healthcare information is deemed to be among the most confidential of all types of personal data. Analyzing and modeling the security threats emanating from healthcare staffs' security practices therefore need an efficient approach. There is a need for tailored measures to be adopted in assessing healthcare personnel security practices in relation to Confidentiality, Integrity and Availability (CIA) threats. Standards and technical security implementations, required by regulatory bodies, have resulted in tracking healthcare staffs' security practices in various data sources which can be explored for security countermeasures.***

***A literature survey was adopted to obtain the most appropriate observational measures that can be used to empirically study healthcare staffs' security practice analysis, modeling and incentivization (HSPAMI). The survey was conducted in journal and conference articles, healthcare security breaches reports and AI tools for detecting anomalous healthcare staff security practices. The survey results did not find a comprehensive and tailed observational measures suitable for the HSPAMI project. A comprehensive and tailored observational measures were therefore developed from healthcare standards, legal, regulatory aspects, and the code of conduct. Observational measures relating to healthcare security practices such as self-authorization, inter-organizational accesses to PHI and ICT readiness were found to be unique and have not been factored in existing observational measures for efficient profiling of healthcare staffs.***

***Keywords*—observational measures, staff security profiling, Code of Conduct**

## I. Introduction

Natural human beings have their basic right to privacy in many parts of the world. The European Union has therefore enacted a General Data Protection Regulation (GDPR) for all European Union and European Economic Area (EU/EEA) member countries to respect this human right to privacy [1]. Norway is bounded to the GDPR through its affiliation to EU [2]. The GDPR of EU has been highly recognized and respected as enshrined in the laws of these member countries [2, 3]. Laws have therefore been promulgated by EU/EEA member countries to implement the GDPR to prevent the abuse of right to privacy of natural persons through the processing of personal data [1]. Personal data relates to data and assessments that can be connected to a natural person [3] and it includes basic identity information such as name, address and ID numbers, Web data such as location, IP address, cookie data and Radio Frequency identification tags, Health and genetic data, Biometric data, Racial or ethnic data, Political opinions and Sexual orientation [2, 3]

In healthcare services, there exists mutual trust and mutual need between healthcare providers and the patients. Much as patients need cure, they require healthcare personnel to be confidential with their disclosed intimate data and information [4]. In the same way, healthcare personnel need and relies on the information and data given by patients to provide effective diagnosis and treatment [4]. This mutual need implies patients to compromise their right to privacy to a limit by sharing their personal information to healthcare personnel with a high trust and condition of confidentiality from the healthcare providers. Healthcare personnel therefore have the responsibility to prevent others from gaining access to or gaining knowledge of information concerning patients' health or medical condition and other personal information known to them in their role as healthcare personnel [4, 5]. Healthcare providers have therefore been mindful to collect only the necessary and relevant patients' data and to be able to keep them as secret as possible to prevent confidentiality breach [4, 6]. However, with the adoption of information Communication Technology (ICT) in healthcare, the confidentiality has been a major challenge. There exists an antagonistic interest between ICT and healthcare provider confidentiality requirement [4]. ICT has muscles for huge data storage, processing and sharing unlimited information while healthcare confidentiality requirement focuses on limiting the spread of information [4]. The evidence is the result of the frequent data breaches in healthcare [7, 8]. Aside the loss of their dignity, the patients suffering may range from fraud to patient injury or death in healthcare related data breaches [6, 9]. Healthcare workers have subtle variant behavior in the usage of ICT systems which can threaten the CIA of the PHI [10]. It has been recorded that, two-thirds of employees have contributed to data breaches [11, 12] through mistakes or deliberate actions.

978-1-7281-2607-4/19/$31.00 ©2019 IEEE
DOI 10.1109/COMPSAC.2019.10239

Technological counter measures such as firewalls, intrusion detection systems, encryption and other security technologies, have been heightened and the adversaries are exploiting the weakest link (humans) in the security chain. The security practices of employees hence need to be strengthened to enhance security in the healthcare [13].

Observational measurement areas in healthcare include but not limited to authorization, authentication, encryption, access control, data or file backups and potential threats to the CIA of the PHI [14]. Therefore, the general objective of this study was to determine the most appropriate and comprehensive means of profiling healthcare staff security practices for empirically analyzing and modeling healthcare staff security practices. The specific objectives aimed to seek answers to the following questions; What security measures would be observed and profiled to constitute the necessary and holistic behavioral pattern of each healthcare staff for efficient analysis and modeling? How and where will the security measure be effectively observed? To address these questions, various literatures were surveyed for the common mode of ingress into healthcare systems which are related to healthcare staff practices. Comprehensive data sources and observational measures in which healthcare security practices can be efficiently profiled, were also explored in the survey.

## II. Methodology and Scope

A literature survey was explored as an initial effort to understand the research area under Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI) project which is operated by the Centre of Cyber and Information Security of NTNU and funded by the Ministry of Health and Care of Norway. IEEE-Xplore, Google Scholar, Elsevier and Science Direct were searched through for journals and conference papers for observational measures towards profiling healthcare staffs' security practices. The literatures were critically analyzed to be used in the study of HSPAMI. Based on the results, Literatures relating to healthcare data breaches reports, healthcare providers and personnel mandated security practices, standards and best practices were explored. This provided comprehensive view for specifying efficient data sources and observational measures for the efficient profiling of healthcare staff security practices. This was achieved by determining the hypothetical security practices, the alternative hypothetical security practice and the possible security impact of the alternative hypothetical behavior. Possible observational measures were then developed. The study did not include ethical and legal clearance towards the scientific study of personal health information.

## III. Results

### *A. The state-of-the-art*

Healthcare staffs' profile consists of a dataset and information which indicate the interaction between the user and a system within a given time [15]. The profiling involves modeling and analyzing their security actions from collected and processed data [16]. So, a comprehensive security actions of healthcare personnel are deemed to be necessary for understanding their goals, habits, interest, preferences, knowledge and skills gaps [14]. So, the data source should be comprehensive to include traces of healthcare security practices of personnel as provisioned in legislatures, regulations and code of conducts [14]. The data gathering should be clear with minimum but necessary and relevant user actions such that the computers or network resources are not impacted [14]. The data should also be gathered to include healthcare staff actions time life-cycle to cover all the needed dataset [14]. The healthcare personnel goals, habits, interest, preferences and knowledge often change due to changes in healthcare services such as emergency situations. Therefore, in profiling healthcare security practices, the data gathering need to include all these specific activities in the healthcare services for holistic and efficient results [17]. The healthcare security environment is also deemed to be most critical since it carries a very sensitive and rich information and therefore require much more protection. So, data gathering for profiling staffs' security practices need to take all subtle security practices into consideration [17]. To the best of our knowledge, there has not been such a tailed comprehensive literature survey relating to healthcare security practices.

Foroughi et al. analyzed IT security reports and best practices to develop observational measures for cyber security purposes [14]. The knowledge on common causes of security breaches and expected users' IT security behavior were analyzed to profile various IT security observational measures. The source of measures includes system setting, installed programs, running processes, online activities, browser history, network connections, warnings, file system and running processes of backup task. Stimulating the observational measures base on user's security practices, provided reliable data sources which can be mined to generate reliable patterns of user behavior [15]. However, Foroughi et al. study did not cover personnel security practices in the healthcare. Personnel behavior is often erratic in healthcare as they strive to provide healthcare in critical situations such as accidents and other emergencies [15]. Therefore, analyzing the security practices of personnel in a mission critical organization would provide a tailed knowledge on the observational measures which can be mined for accurate and efficient patterns of anomalous behaviors.

Additionally, Jason et al. developed a framework for characterizing attacks to detect insider adversaries [18]. The framework has classes of components such as attack catalyst, actor, attack and organization characteristics. Attack catalyst consists of events that can have negative impact on staffs or users including demotion. Actor characteristics include potential insider threat such as IT security employee skill set with the potential to attack. Organizational characteristics includes vulnerabilities associated with assets such as networks and servers while attack characteristics deal with behaviors towards attacking a system. These include, for instance, planning and executing logic bomb leading to hacking into company server. After the implementation of the framework, some of the observational measures include inappropriate browsing, accidental leaking sensitive data via email, fraudulent engagement of personnel in logistic company, prison and tax offices respectively. Much as the framework can identify observational measures towards detecting insider-threat from behavioral and technical security practices relating to human factors, the framework faces challenges relating to direct applications to various sectors. For instance, in the healthcare sector, the framework needs to be tuned to accommodate personnel behavior under various services such as emergency services to reduce false alarms.

Similarly, Boddy et al. approach to the development of the observational measures was conducted through conceptualization and designing of a framework in healthcare infrastructure [19]. In the framework, input data from computers and medical devices were collected and processed by removing away irrelevant data. The processed data was then stored in a database together with stored known attack behaviors of dataset. This was used to compare with input dataset with the aim to detect malicious intentions. The stored dataset was then processed again and visualized. The output of the visualization could be interfered by the users to set parameters to achieve their situational awareness goals of the infrastructure. An experiment was further conducted with the framework in which an active directory domain controller network statistic (netstat) was captured, analyzed and visualized. The connection type (TCP), source and destination IPs and connection states were captured in the network statistics. Most frequent accesses from foreign IP addresses were realized to be a security threat. The study provided knowledge on how anomalous behavior could be detected by using user behavior visualization technique and also indicated some observational measures such as source and destination IPs. The experiment showed how attackers from external source could be detected but there was no demonstration of how to detect security breaches relating to IP address spoofing or insider attack. Besides, healthcare staffs conduct, involve collaborating on patients care which enables external personnel access. So, using external accesses as a threshold to security threats in the practical demonstration without considering external healthcare personnel legitimate accesses would increase false alarms. This calls for analyzing the entire obligatory conduct of healthcare personnel to determine how their activities can be observed for improved security. Boddy et al. did not also indicate how their approach in the framework would not affect system performance since patient input data would always be compared with the known attack patterns.

Walker-Roberts et al. conducted a systematic review of the availability and effectiveness of security solutions to internal threats in healthcare ICT systems [20]. Various methods of security measures including machine learning, profiling and risk control were used. None of the solutions completely counteracted insider threat. Walker-Roberts et al. study did not disclose if healthcare personnel mandated security practices were considered in the development of the security measures. Therefore, there was a limited knowledge on observational measures of the literatures that could be relied on to conduct an empirical study in the healthcare staffs' security practices. However, the study indicated a need for proactive security countermeasures in healthcare which would be considered in this study.

### *B. Survy on vendors providing AI solutions in human behavioral security countermeasures in healthcare*

In surveying for observational measures and their related data sources in vendors providing AI solutions in human behavioral security countermeasures in healthcare, Sennaar et al., reported on observational variables and their related data sources. According to Sennaar et al.[21], Darktrace system relied on end users and the devices connected to healthcare networks to analyze raw network traffic to uniquely profile the clients' healthcare environment. An acquaintance of the normal security pattern and the associated security tolerance range enables detection of potential threats. Cylance algorithms were fed with data sources from Windows, Mac, and Linux frameworks, consisting of large records of safe and unsafe files and events. Observational variables which are being analyzed include file size, imports, headers and directories which were further aggregated into related clusters in respect to malicious and safe properties.

ClearDATA [21, 22] system mines electronic health records of patients and healthcare personnel records for known security threats. The pattern is then compared with data accesses to determine abnormal accesses. ClearDATA objective was to meet HIPAA compliance across various EHR. Agar's machine learning system intelligence [21, 23, 24] was based on learning about 2 trillion emails per year from email hosting platforms including Yahoo and Google. Features including sender and email type were filtered, analyzed and classified into various categories such as malicious, spam or safe emails for analyzing new emails for maliciousness. Wiretap [21] uses data from various components of healthcare network such as private messages, content files, content from internal and external users of programs such as Facebook, Slack and Microsoft Office and compared to expected behavior of other healthcare staffs to determine the risk of personnel security practices. Though the various vendors solutions met some observational variables, none of their solutions considered a compressive approach towards meeting the CIA of PHI.

### *C. Literature survey in healthcare security breaches*

The literature survey was extended to healthcare security breaches report for possible observational measures and to provide understanding of trends on common attacks and mode of ingress. The survey found that, in 2018, through the aid of a staff, the health care records of about half the total population of Norway (3 million) were compromised [7]. Also, a phishing attack resulted in breaching 38,000 patients records at Portland, Oregon-based Legacy Health in the United State of America [8]. Personal data such as patients' email accounts, demographic information, dates of birth, health insurance data, billing details, medical data, Social Security numbers and driver's licenses were stolen. In a similar incidence [8], about 1.5 million patient records, including data of the prime minister of Singapore, were breached. A front-end workstation was first compromised to get access to privileged user credentials. In the United States, about 365 breaches were reported in 2018 with hacking being the leading cause of healthcare data breaches followed by unauthorized access and disclosure incidents [25].

### *D. Literature survey in Healthcare Staffs' Required Conducts*

This section of the study explores efficient methods for determining observational measures of healthcare staffs' practices in literatures related to healthcare staffs' mandated conducts, regulations and standards towards the CIA of patients' information. A Comprehensive healthcare staffs' obligated security and confidentiality conduct are spelled out in legal, regulatory, code of conducts, standards and best practices for healthcare organizations and staffs [4]. According to the Norwegian ministry of health and care, the GDPR, the Health Records Act, the Health Personnel Act, the Personal Health Data Filing System Act, the Health Research Act, and the Patients' and Users' Rights Act are deemed most relevant for healthcare data controllers, processors and personnel [4, 26]. These laws, regulations and standards have specified the confidential responsibilities of healthcare staff [5, 9]

As of 25th May 2018, all countries under EU/EEA are being regulated on their personal data privacy and security management. The GDPR outlined rules for protecting natural persons fundamental right to privacy in relation to the processing of personal data and rules relating to personal data movement. Essentially, the GDPR requires businesses and institutions to protect the personal data and privacy of EU citizens in their dealings within EU/EEA member countries. Failure to comply with this regulation corresponds to a heavy fine [27]. The GDPR was implemented in Norway through the Personal Data Act of Norway, 2018[3, 28]. The main purpose of the act was for the implementation of the GDPR [3]. The Act ensures that personal data are processed in accordance with fundamental human right to privacy [3].

In the Health Records Act, accesses to patients' records have been improved such that the patient' health records now move along with patients even in referral situations [4, 29]. This helps for the relevant and necessary data to be available for healthcare personnel accesses. The personnel are required to rightly access the patient's data for the provision of quality healthcare while being responsible to confidentiality of the patients' data [4, 29].

The Personal Health Data Filing System Act [30], also exists to provide patients' information and knowledge to public health services and administrations for effective and adequate medical treatment while preserving the patients right to privacy. The Act also support research into patients' data to provide an insight on the state of public health, causes of decreased health and illness. Through research and statistics, the Act contributes toward information on and knowledge of the state of public health. The information and knowledge gained is used for quality assurance, administration, planning and management measures. Much as any person who handles personal health data in relation to [30] has the responsibility of being confidential with patient's personal information, the data controller and processor are responsible to plan with risk assessment measures to have satisfactory security for the CIA of the personal health data.

One of the main objectives of the health personnel act [5] is to ensure trust in health personnel and the health service. Therefore, the health personnel have been constrained with the responsibility to respect patients' personal data confidentiality as specified in chapter 5 of the health personnel Act. The patients act was also enacted to support the respect for human dignity, life and integrity [31] In the reviewed acts [4], there was no technical provisions as how the security measures can be implemented to safe guide CIA of the PHI in healthcare.

The Code of conduct for information security and data protection in the healthcare and care services sector (the code of conduct) [6] was created to facilitate the implementation of adequate technical and organizational measures to meet the CIA requirements for personal data processing. It was developed by the Directorate of e-health in Norway for the implementation of the personal data act in respect to the GDPR [6]. The code of conduct spelled out how the technical and organizational measures are to be implemented to fulfil the personal data privacy requirement and indicated the responsibilities of data controllers, data processors and healthcare personnel in insuring the protection of the personal data.

The code of conduct clearly indicated that, Persons outside the organization or within the organization must not be able to gain unlawful access to personal health information (PHI) and personal data (PD). A summary of the technical implementation requirement includes;
Staffs transactions such as, changes, corrections and deletions must be logged in PHI and PA filing systems such as EHR and HR systems. The purpose is to form an audit trail of healthcare security practices. PHI and PD must be accessed by authorized users for only official and therapeutic purpose within the confidentiality arrangement. The technical measures should include self-authorization as an option for authorized users to gain access to PHI and PD without following conventional procedures to access PHI and PD. However, the reason for self-authorization must be documented. For instance, access to PHI and PD filing systems for therapeutic reasons is valid when personnel are officially responsible for a patient who has a planned or completed schedule implementation of measures for the medical treatment. Healthcare personnel's accesses should include their identity, the role to which the authorization has been allocated (if roles are used by the organization), purpose of the authorization and time at which the authorization was given, among others.

Similar provisions were found in other jurisdictions. Health Insurance Portability and Accountability Act (HIPAA) [32] ensures security and privacy of PHI through the HIPAA privacy rule and the HIPAA security rule. HIPAA privacy rule protects personal identifiers, health conditions and payment provision for healthcare. So, appropriate measures and procedures should be kept in place to control abuse of the use and disclosure of PHI. HIPAA security rule protects all personal health information which are created, received, maintained or transmitted in electronic form by the healthcare providers. The rule protects PHI from unauthorized disclosure, integrity and availability of all PHI. The rule also identifies and protect against potential threats to CIA.

International Standard Organization (ISO) [17], also provides guidance to healthcare providers and other organizations that possess PHI on the appropriate method to protect CIA of such information. ISO provides unique guidelines on CIA needs of the health sector and its unique operating environments [17]. The ISO 27799 applies ISO/IEC 27002 to the healthcare domain with the appropriate security controls for efficiently protecting personal health information. The ISO 27799 was comprehensively developed with guidelines of personal data protection legislations, obligations, privacy and security best practices, individual and organizational accountability. ISO 27799 aims to protect information such as PHI, pseudonymized data derived from PHI, statistical and research data, including anonymized data derived from PHI.

The Hippocratic oath which is taken by most healthcare personnel, remains very relevant in maintaining CIA of PHI after it was formulated in almost 2500 years ago [9]. In part, healthcare personnel are required to upheld confidentiality with PHI which they might have been aware of due to their official interactions with the patients [9].

In summary, the observational measures which were found in the study includes: Patterns of attempted accesses to PHI, Assessment of trust level of security configurations of computers and networks accessing PHI, Monitoring and controlling social Network accesses in healthcare network, assessing file sharing security, analyzing access identities and analyzing encryption of PHI. Other observational measures include monitoring and controlling, compliance of authorization, access control, authentication, physical accesses of networks, computers and EHR systems, remote communication devices, links and access, backup and recovery management, Audit trails of accesses to computers and peripherals, physical security, networks and EHR, physical security of communications, computer, and display systems and Self-authorization measures.

The data sources which were mostly analyzed for the observational measures of healthcare staff includes system Setting, Installed Programs, running processes, online activities, browser history, network connections logs, warnings, file system and running processes of backup task, social media and email and text messages content analysis and Access Control logs of Electronic Health Records (EHR).

## IV. Discussion

The literature survey was to determine comprehensive observational measures and their related data sources that can be used to empirically study into healthcare staffs' information security practices in HSPAMI project. The impending HSPAMI project results are intended for building a strong security culture towards enhancing the security countermeasures in healthcare. Security countermeasures include diverse aspects such as psycho-socio-cultural context, organizational factors and training. But this study is limited to analyzing and modeling various data sources which are created by healthcare staffs' such as access control logs, network and operating systems logs and other histories of their practices which can be reconstructed to form their unique individual security behavioral profile. The study did not also include ethical and regulatory clearance for researching into personal data.

Table 1: Summary of observational measures for analyzing and modeling healthcare stare security practices.

| **Hypothesis** | **Possible causes and Related Threats** | **Detection/Observational Measure** | **Source** |
|---|---|---|---|
| ***1. Access Control*** | | | |
| There are unauthorized accesses to PHI | user access misconfiguration, impersonations resulting in direct violation of patient' confidentiality, security and privacy issue on necessary and relevant accesses | Compare user access profile with current accesses. Check accesses with authorization register eg purpose, time, location, authorizer, access rights, planned therapeutic patient and schedule, quantum of authorize access,Check misuse of self-authorization and interorganizational accesses | EHR, Network log |
| Personnel do not have unique authentications Eg password sharing | This can cause unauthorized accesses. | Check for sharing authentication criteria, logins after shift time, and location of logins, login with default password and unique user computer behavior such as keystrokes and mouse clicks dynamics. | EHR |
| ***2. Employees, competence and attitude-forming campaigns*** | | | |
| Former employee does not return resources with healthcare data | PHI can be accessed without authorization | Check for dissociated staffs, and assets returned, revoking access right during dissociation such as transfer etc. | EHR |
| ***3. Communications Security*** | | | |
| Internet is connected to where PHI is processed | This can provide room for data breaches | Test to ensure internet service is logically separated from areas where PHI is being processed | Network Logs |
| Not all Healthcare personnel have authorization to use other IT services | The behavior can impact security if websites with trojans and viruses are visited. | Check if user has authorization for email, internet etc., downloaded and installed software. Check if downloads and installations were approved. Check IT services usage with authorization and purpose. | Network logs, browser history, server event logs |

| | | | |
|---|---|---|---|
| PHI is disclosed through the usage of e-mail, text or other unencrypted channels | It compromises the right of patients to confidentiality | Use content filtering to scan email text, images and attachments, for potential threats. Test to get PHI and user credentials via social engineering and phasing attacks | EHR |
| ***4. Physical security and the handling of equipment*** | | | |
| Not all personnel obtain keys/access/cards/password through known procedures | Unauthorized persons can have Keys/Access cards to computing resources | Check for abnormal physical access profile of users. Eg. Abnormal physical accesses will deviate from their established profile or pattern | Physical access log |
| personnel access to data without predefined and preconfigured equipment | Pre-defined equipment helps to identify unknown client computers of a network | Check for user attempted accesses with unregistered endpoint devices, unsuitable, outdated preconfigured devices. | Network,OS, Assets,Updates log |
| ***5. Security IT operations*** | | | |
| Healthcare personnel not backing up and testing for prompt recovery of their data, logs and files | Data and Files can get loss when the user computer malfunctions. Without the log, it will be difficult to detect who course a breach | Test backup schedules and recovery, Analyze and test the information system logs and network logs for validity | Backup files<br>Network logs<br>EHR |
| Technical vulnerabilities in equipment are not being managed | Vulnerabilities in equipment's and change management can hinder CIA | Overview of ICT equipment, software, supplier, version numbers, and updates should be monitored and managed. Test for technical vulnerabilities in equipment's, software and change management | ICT equipment and software register change management plan |
| There is no defined network traffic of personnel accesses | Dictionary, DSS, ransomware and unknown malware[33] attacks | Test for white-listing measure with simulation attack | |
| ***6. Digital Communication with healthcare users*** | | | |
| PHI are being sent to patients and to the wrong recipients | There is unauthorized disclosure of PHI | Verify procedures and scan content of information sent to healthcare users | Data handling procedure documents |
| ***7. ICT Readiness*** | | | |
| Shutdown of EHR will cause non-availability of essential PHI | Non-available essential PHI will result in a range of incorrect patient treatment to loss of lives | Test for the availability of essential PHI in electronic information shutdown scenarios | |
| ***8. Handling of information security breaches*** | | | |
| information security breaches are not being reported | This will prevent, restoring normal system status, eliminating cause of breaches and prevent reoccurrence | Test for reporting information security breaches in a breach scenario | |
| ***9. Suppliers and Agreements*** | | | |
| Suppliers, Providers and contractors access donot follow established CIA reules | Adversaries can pose as such and compromise security | Compare accesses with generic normal profiled security practice. Test CIA measures as suppliers, security provider etc. | EHR, Network log |

It is assumed that, the necessary ethical clearance would be obtained prior to researching into personal data. Various literature studies were surveyed for tailored and comprehensive observational measures and their respective data sources that can be explored for healthcare staffs' security countermeasures as summarized in section B, subsection 3 and in Table 1.

Under section III, subsection A, various approaches were used to obtain the observational measures and their related data sources. [14] surveyed literatures relating to general security incidence reports and recommended best security practices, by industry players, to compose a security observational measures for insider threats mitigation. Further, [19]and [18] used a conceptualization approach to develop frameworks for observational measures towards insider threat mitigation in healthcare. A systematic review of the availability and effectiveness of security solutions to internal threats in healthcare ICT systems [20] was also explored for observational measures. None of the above studies indicated their observational measures to meet the key security lookups as provisioned in various standards and code of conducts for healthcare security and data privacy protection in Norway [6] as shown in in Table 1.

The healthcare sector is characterized with variant situations and services such as emergency services and collaborations in patient care which require electronic exchange of personal health information (PHI) between health professionals and healthcare organizations. Also, healthcare information is deemed to be among the most confidential of all types of personal data [17]. Analyzing and modeling the security threats emanating from healthcare staffs' security practices therefore need a holistic, tailored and efficient approach [17]. There is hence a need for tailored measures to be adopted in assessing healthcare personnel security practices in relation to CIA threats in all aspect of the recommended security controls. Standards and regulatory require healthcare organizations to adopt to adequate technical security implementations to be able to proactively detect and mitigate all aspect of the healthcare security issues [6]. This is to reduce risks ranging from unauthorized accesses to denial of services of healthcare electronic information systems [17]. This is to ensure the CIA of the relevant and necessary PHI in healthcare. [14] [18, 19] and [20] studies, covered areas such as access control, physical security, remote access and mobile computing but security measures such as ICT readiness, suppliers and agreements, inter-healthcare-organizational accesses and self-authorizations were not considered [6]. Self-authorization is a technical requirement which is enshrined in the code of conduct for information security and data protection of healthcare in Norway [6]. Self-authorization variable enables healthcare personnel to access individual PHI for therapeutic reasons without following the conventional procedures for PHI access authorization [6]. This is mainly necessary for use in emergency care situation and it is perfectly aligned with the security principle of availability [4, 34]. Though self-authorization is very necessary for patients care, it poses security challenge of blacklisting defenses against inappropriate accesses of PHI since it is susceptible to abuse [6]. Essentially, healthcare staffs' security solutions which lack such tailored observational measures may not be effective since they may impede legitimate PHI accesses, or they may ignore a very big security foot hole for the advisories [17].

After analyzing healthcare security incidence reports and top AI counter measures for insider threat mitigations, snooping on the medical records, exfiltrating sensitive data to personal accounts, competitors, or bad actors, printing, downloading and exporting patient records and reports, ransomware and phishing attacks were found to be most common [8, 21, 22]. The approaches of the vendor solutions were found to vary from one another but none, employed measures to address all the key security areas which have been provided in the Norwegian code of conduct for healthcare on information security and data protection. This could be due to financial and algorithm computational cost since these AI algorithms gain their intelligence from very large data sources such as emails, endpoint devices and staffs operating practices [21].

Base on the above short comings, a comprehensive and tailored observational measures for profiling, analyzing and modeling healthcare staff security practices were developed in the literature survey. Some of the surveyed literature that were explored include the Code of conduct for information security and data protection for the healthcare in Norway, ISO 27799:2016 and HIPAA security and privacy standards [6, 17]. The observational measures were found to spread across various security measures including access control, employee competence and attitude forming campaigns, communication security, physical security and handling of equipment, security IT operations, digital operations with healthcare users, ICT readiness, handling of information security breaches and suppliers and agreements [6]. All healthcare providers in Norway are to follow details of this spectrum of security controls in the code of conduct to provide efficient technical solutions towards safeguarding the CIA of PHI [6]. The code of conduct was developed by the Norwegian eHealth directorate [6]. Various sources such as the GDPR, Personal Data Act and Healthcare Personnel Act were considered in the development of the code of conduct [6]. The ISO 27799 and the HIPAA security and privacy standards also have similar security measures [32]. The observational measures include self-authorization, interorganizational PHI accesses and ICT readiness as shown in Table 1.

What is unique and essential about this finding is the holistic and tailored approach which was adopted to obtain the spectrum of the observational measures. Additionally, the findings were resulted from a mandated security conducts combined with standards which are most particular to healthcare information security. Though these standards and code of conducts are not silver bullets, they are measured up to global standards, legal and regulatory requirement which are being revived to improve upon their vitality for healthcare security counter measures [6, 17]. Additionally, under each of the security controls in the code of conduct [6], there are various hypothetical technical implementations which are outlined for users to adopt. For instance, under access control, technical measures are to be kept in place to prevent unauthorized accesses to PHI. So, the observational measures were developed by forming an alternative hypothesis from the technical security measures. In this instance, the alternative hypothesis was formed as, "There are unauthorized accesses to PHI", as shown in table 1. The alternative hypothesis presented a responsibility and a challenge for us to explore and synthesize the observational measures for that alternative hypothesis.

[14] [18, 19] and [20] studies which provided some observational measures were generic and lacked the specific and detailed security attention required in healthcare [6, 17]. For instance, in observing interorganizational accesses of PHI, there is the need to observe for PHI accesses relating to collaborative patient care and accesses by other organizations who have the required permission but not for some therapeutic reasons like collaborative patient care.

Additionally, due to the delicate nature of healthcare services, non-availability of a healthcare service could be deemed critical [6]. Critical issues could include life-threatening for patients, organization's operation issues, the incorrect treatment of a patient, loss of efficiency, loss of revenues for the organization and low patient's trust among others [6]. The adoption of the study aim has resulted in similar observational measures which can be observed towards safeguarding the CIA of PHI.

Further to this, how each measure would be observed, were identified to include profiling for machine learning, creating test scenarios and verification of security counter measures for their viability. The profiling of individual security practices towards detecting anomalous practices can be conducted in access control related data such as physical, network and EHR access control related logs [14]. However, it is comparatively complex to adopt to machining learning techniques to determine metrics of healthcare staffs in relation to social engineering activities such as phishing [21]. Therefore, tests scenarios would be deemed most effective [6]. For instance, a supposed phishing email can be sent to healthcare staffs in a controlled environment and the metrics of staffs who pick the bait would be determined. Even if one person is involved would require comprehensive security training and management attention in that regards. Because, the adversaries may require at least, one legitimate user to click the malicious link [35].

Moreover, various data sources were identified alongside with the observational measures. These include logs from EHR, Network, browser history, physical security access logs and OS as shown in Table 1. Mining a combination of these logs for anomalous practices could potentially enhance the efficacy of the detection system [14]. For instance, an advisory who want to access EHR through healthcare facility would have variant physical, network and operating system access profile. Therefore, if there exist deviations in all three or four data sources, the probability of the individual being an intruder would be quite high. But in observing such measures, effective and efficient training of the algorithms are required in order not to prevent legitimate healthcare personnel from accessing systems for therapeutic reasons.

## V. Limitations, Conclusion and future works

Healthcare PHI is deemed to be one of the most sensitive personal data which its CIA require enhanced security controls. The richness of the PHI has attracted malice despite the technological security countermeasures. The advances of the advisory for PHI has the tendency of impacting CIA, ranging from fraud to loss of life.

This has motivated a HSPAMI study which stands to study into healthcare staffs' security practices towards building a security conscious care behavior through incentivization. A literature survey was then conducted in this regard to explore for comprehensive and tailed security observational measures which can be used to analyses and model to detect anomalous behaviors.

Literatures relating to healthcare security breaches report, some top AI systems for healthcare insider threat detection, standards, regulations and legislations, code of conducts and other literatures relating to observational measures were surveyed.

Comprehensive and tailed security observational measures such as self-authorization, interorganizational accesses of PHI and ICT readiness were identified to be some of the most essential observational variables. Machining learning technique can be used to analyze and model the observational measures to profile individual staffs' security practices for anomalous tracking. Test scenarios can also be developed from the results to test for social engineering related behaviors of healthcare staffs. The study results can also be used to test for ICT readiness by testing scenarios to determine if the necessary and relevant PHI would be available in situations where the electronic health records is deemed not available.

The observational measured identified are deemed to be of high level and would require more detailed requirement analysis prior to implementation. A second expert opinion would also be required to assess these variable before they are used for empirical study.

## References

[1] The European Parliament And The Council Of The European Union, Regulation (Eu) 2016/679 Of The European Parliament And Of The Council, in 95/46/EC, 2016 Official Journal of the European Union.

[2] @ICLG_GLG. International Comparative Legal Guides. 2019; Available from: https://iclg.com/practice-areas/data-protection-laws-and-regulations/norway.

[3] beredskapsdepartementet, J.-o., Proposition 56 LS (2017–2018)/Act on the processing of personal data (the Personal Data Act). 2018, regjeringen.no.

[4] Pedersen, S. and G. Hartvigsen, Lessons learned from 25 years with telemedicine in Northern Norway. 2015.

[5] 5omsorgsdepartementet, H.-o., Act of 2 July 1999 No. 64 relating to Health Personnel etc., in 042051-200005. 2002, regjeringen.no.

[6] e-helse, D.f., Code of conduct for information security and data protection in the healthcare and care services sector, D.f. e-helse, Editor. 2018.

[7] digitalhealth2, Norway healthcare cyber-attack could be biggest of its kind. 2018.

[8] HealthcareITNews. Healthcare IT News. 2019; Available from: https://www.healthcareitnews.com/.

[9] Kantarjian, H. and D.P. Steensma, Relevance of the Hippocratic Oath in the 21st Century. 2014.

[10] Shilton, K., et al., Qualitative Approaches to Cybersecurity Research. 2016.

[11] CNN. CNN.com - A convicted hacker debunks some myths, 2005.http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/.

[12] CISCO, Cisco 2017 Annual Cybersecurity Report: Chief Security Officers Reveal True Cost of Breaches and the Actions Organizations are Taking. 2017.

[13] Tetz, E., Network Firewalls: Perimeter Defense - dummies. 2018.

[14] Foroughi, F. and P. Luksch. Observation Measures to Profile User Security Behaviour. in 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). 2018.

[15] Ouaftouh, S., A. Zellou, and A. Idri. User profile model: A user dimension based classification.10th International Conference on Intelligent Systems: Theories and Applications (SITA). 2015.

[16] Kussul, N. and S. Skakun. Intelligent System for Users' Activity Monitoring in Computer Networks. in 2005 IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. 2005.

[17] ISO, ISO 27799:2016(en), Health informatics Information security management in health using ISO/IEC 27002. 2016.

[18] Nurse, J.R.C., et al. Understanding Insider Threat: A Framework for Characterising Attacks.IEEE Security and Privacy Workshops. 2014.

[19] Boddy, A., et al. A Study into Detecting Anomalous Behaviours within HealthCare Infrastructures. in 2016 9th International Conference on Developments in eSystems Engineering. 2016.

[20] Walker-Roberts, S., M. Hammoudeh, and A. Dehghantanha, A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access, 2018. 6: p. 25167-25177.

[21] Sennaar, K., Cybersecurity in Healthcare – Comparing 5 AI-based Vendor Offerings | Emerj. 2019, @emerj.

[22] ClearDATA.HealthcareTech.-ClearDATA.2019; https://www.cleardata.com/healthcare-segments/healthcare-tech

[23] Agariinc. Advanced Threat Protection Solutions|Agari Email Protection.2019;https://www.agari.com/products/advanced-threat-protection/.

[24] Ayyagari, R., An Exploratory Analysis of Data Breaches Trends and Insights. http://dx.doi.org/10.1080/15536548.2012.10845654, 2014.

[25] Hipaa Journal, Healthcare Data Breach Statistics. 2019.

[26] Norwegian Centre for E-health Research. Diabetesdagboka.no. 2018; Available from: http://www.diabetesdagboka.no/en/.

[27] EUR-Lex, The European Parliament and the Council of the European Union, Regulation (EU) 2016/679, EU, Editor. 2016.

[28] e-helse, D.f. Implementation of GDPR in health care sector in Norway. 2019; Available from: https://ehelse.no/personvern-og-informasjonssikkerhet/eus-personvernforordning/implementation-of-gdpr-in-health-care-sector-in-norway.

[29] LOVDATA, Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) - Kapittel 3. Taushetsplikt, innsynsrett og rett til å motsette seg behandling av helseopplysninger. 2019.

[30] omsorgsdepartementet, H.-o., Act of 18 May 2001 No. 24 on Personal Health Data Filing Systems and the Processing of Personal Health Data (Personal Health Data Filing System Act), in 042041-990016. 2006, regjeringen.no.

[31] Supervision, N.B.o.H., The Act of 2 July 1999 No. 63 relating to Patients' Rights (the Patients' Rights Act) in 63. 1999.

[32] Neuhaus, C., A. Polze, and M. M R Chowdhuryy, Survey on Healthcare IT Systems: Standards, Regulations and Security. 2011.

[33] GDPR.Report, Businesses at risk due to unidentified network traffic according to global survey - GDPR.Report. 2018.

[34] Michael Goodrich and R. Tamassia, Introduction to computer security. 1st ed. 2014: peason.

[35] Islam, R. and J. Abawajy, A multi-tier phishing detection and filtering approach. Journal of Network and Computer Applications, 2013. 36(1): p. 324-335.