IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 9, 2021, accepted December 7, 2021, date of publication December 10, 2021,
date of current version December 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3134873

A Conceptual Framework to Ensure Privacy in Patient Record Management System

FARIDA HABIB SEMANTHA, SAMI AZAM, (Member, IEEE), BHARANIDHARAN SHANMUGAM, KHENG CHER YEO, AND ABHIJITH REDDY BEERAVOLU

College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT 0810, Australia

Corresponding author: Sami Azam (sami.azam@cdu.edu.au)

ABSTRACT Privacy has become an increasingly significant apprehension in today's rapidly changing economy primarily for personal and sensitive user data. The levels of personal data violation are increasing day by day however privacy-preserving frameworks are available. This paper conducted an in-depth analysis of contemporary frameworks to identify the key mechanisms to produce a sophisticated data privacy framework to reduce the rate of data breach particularly for the Patient Record Management System (PRMS). There are several studies available that stated healthcare data privacy, still, complete data protection solution with the application of privacy by design towards patients' health data by ensuring privacy in each layer of the PRMS are quite limited, which is the focus of this study. PRMS manages personal and sensitive data while delivering healthcare services to the patients and as such, have also the potential to carry significant risks to the privacy of their data. A novel conceptual framework with three distinct and sequential phases is suggested in this research, each of which is defined in a distinct section. The first phase is defined as the planning to identify the key limitations of contemporary frameworks so these can be minimized to ensure privacy in each layer of data processing. The second phase incorporates the key components of data privacy to satisfy the efficiency and effectiveness of the proposed framework. Finally, the third phase is the implementation of the selected requirements of the assessment phase to prevent privacy incursion events in PRMS. The complete framework is anticipated to deliver a sophisticated resistance in contradiction to the continuous data breaches in the patients' information domain.

INDEX TERMS Data privacy framework, data protection methods, privacy by design, privacy design strategies, privacy impact assessment, patient record management system.

I. INTRODUCTION

Nowadays privacy is an increasingly imperative concern when considering information systems that collect personal and sensitive user data [1]. Constructing a regulatory framework for the assets of an organization in contradiction of the rising tide of cyber threats is an enormous concern of governments around the world. Most organizations provide e-services to identify and manage the personal information of users that are stored in the information system [2], [3]. Data breaches can lead to malicious activities in financial interruption as well as reputational damages on both the personal and organizational front. Major intimidations to data privacy had been succeeded due to unauthorized access, data theft, data loss, hacking of IT incidents, and improper data disposal [4], [5].

In our previous research, statistics of data breaches along with the associated costs had been highlighted to detect the data breach hazards that were growing every year around the world [6]. Between 1 January to 30 June in 2020, healthcare service providers confronted maximum data breaches than other sectors in Australia, where 115 data breaches were reported by healthcare sectors according to the Office of the Australian Information Commissioner (OAIC) [7]. The average data breach cost comprising of 1 million data is almost AUD 40 million [8]. Many organizations have constantly encountered data breaches and have so far struggled to discover effective way-outs [9]. Single data breach costs AUD 408 in healthcare organizations which is three times more per record than all other sectors [10].

The associate editor coordinating the review of this manuscript and approving it for publication was Jerry Chun-Wei Lin.

Privacy by design is an approach that ensures personal control over an individual's privacy in the operations of information systems and business practices by proactively embedding good privacy practices resulting in a sustainable competitive advantage for organizations [11]. Developing a trustworthy system is a major challenge in the software engineering field particularly to perform personal or professional activities. Limited methods have been suggested by researchers to discourse the solution to data breach problems [12], [13]. Some of these methods are separation of data, Anonymous, Pseudo anonymous, Block-chain based solution, K-Anonymity algorithm, and so on [14]–[17]. However, current methods of data privacy fortifications are behind in providing an adequate outcome to reduce the data breach complications [18], [19].

A comprehensive investigation of data privacy by design was presented in our previous paper [6]. We had critically and identified the extensive restrictions of data privacy in the healthcare sector by using a systematic literature review (SLR). Besides, a comparative analysis based on seven existing privacy by design frameworks was conducted. Our prior research had suggested sustainable future research and development direction as the existing frameworks are behind to control and reduce the rate of data breaches around the world [6]. The aim of this research is to develop a conceptual framework by using fundamental mechanisms of Privacy by Design (PbD) to safeguard patients' health records.

The novelty of this work presented here lies in the fact that the proposed framework is not a single entity but a collaboration of globally verified components such as fundamental principles of Privacy by Design (PbD) by Ann Cavoukian, privacy design strategies by Hoepman Jaap-Henk, suitable standards, and best practices, and Privacy Impact Assessment (PIA) to ensure a comprehensive privacy-preserving environment in healthcare system design. An extensive analysis of existing frameworks supports this research to identify the key components and their limitations. Seven data privacy frameworks are nominated to conduct a comparative analysis that helps our research to determine the key components of personal data privacy. Existing frameworks are further investigated to understand their integrity and effectiveness towards the confidentiality of personal and sensitive user data. Based on the comparative analysis we identified that the existing frameworks are not entirely incorporated these key components to construct their privacy context, therefore the potentiality of these frameworks are inadequate towards the confidentiality of personal information. Our research combines the key components which are globally verified and compulsory mechanisms to design a privacy-preserving framework especially for the personal and sensitive data of the patients to ensure maximum defence. In addition, seven fundamental Privacy by Design (PbD) principles by Ann Cavoukian are combined into four healthcare principles (HPs) to simplify and guarantee the data privacy contexts as a design pattern in the PRMS. The proposed healthcare principles (HPs) are applied to each layer of the healthcare data processing system to safeguard patients' sensitive data while collecting and processing.

The compatibility of our proposed framework with two bench-mark standards APPs and GDPR is established that presents the proposed healthcare principles (HPs) are completely in compliance with these standards. Besides, the implementation of the proposed key components into the PRMS are elaborately presented to determine the performance. Research initiatives that combine all of the key components to fully support the confidentiality of patients' health records are hard to find, especially concerning the proven data privacy mechanisms to develop an entirely protected PRMS. The contribution of this research is to develop a conceptual framework that incorporates the key limitations of the existing studies as well as ensures maximum privacy in each layer of personal data while processing them in the healthcare system. This work will guarantee the compliance of comprehensive data privacy by design mechanisms to achieve a superlative outcome of personal data protection.

II. STRUCTURE OF THE PAPER

The rest of the paper is structured as follows: information about Patients' health records are presented in Section III, the necessary background studies are analysed in Section IV. This section also provides a comparative analysis of the existing privacy by design frameworks. Section V has an in-depth explanation of the proposed framework along with planning, assessment, and implementation phases; and finally, Section VI concludes the paper and future works are presented in Section VII.

III. PATIENTS' HEALTH RECORDS

Patients' health records are associated with the collection of personal identification, demographic data, medical and financial data. Healthcare providers use patients' health records to support healthcare professionals and health organizations, e.g. hospitals, clinics or laboratories for the management of healthcare services to the patients [20], [21]. Personal identification and demographic data are related to personal details (Title, First Name, Last Name, Gender, Marital Status, Street & Suburb, State), next of kin details (Name, Relationship), emergency contacts (Name, Relationship), cultural background information (Aboriginal or Torres Strait Islander Origin, Other Cultural Background, Country of Birth, Is English your First Language, Do you Require an Interpreter, Language). Medical data are mainly associated with allergies and medical information (List of Allergies, Any Intolerance to Medications, Describe the Reaction, Regular Medication and Doses). Financial data are related to the insurance and billing information (Medicare Card No., Medicare Reference No., Medicare Expiry Date, Private Health Fund Details, Payment Amount, Debit/Credit Card Details). Healthcare providers collected these records while enlisting a new patient to manage the registry of the healthcare services and maintain a permanent register of the patient. Additional medical records

are included as clinical information when the diagnosis or treatment of the patient is in progress [22]–[24].

IV. RELEVANT STUDIES

Research initiatives in the field of healthcare data privacy with complete resolution towards the protection of personal and sensitive data are rather scant, despite that, the following section analysed some of the closely related works to address the key aspects to design prolific privacy by design framework.

Bari and O'Neill [22] suggested that patients' health records are collected by different platforms such as social media, pregnancy and mental health apps, depression and smoking cessation apps, wearable fitness trackers. All these platforms are joined to medical records and can be shared with third parties for advertising and other purposes, often without any consent from the individual using the applications. The range and volume of patient data that are in digital form are rapidly growing [22]. The Health Insurance Portability and Accountability Act of 1996 is known as HIPAA that outlines the legal use and disclosure of health information [25]. The European General Data Protection Regulation (GDPR) [26] and the California Consumer Privacy Act (CCPA) [27] are two data protection laws that use a similar conceptual approach to permit and prohibit the use of personal information and rights and obligations of access and control [28]. HIPAA and GDPR contain similar patterns for patient and users consent for use or disclosure and rules to be analysed to ensure that individuals are notified if any data breach occurs [28]. This research recommended that modernizing HIPAA by comparing the models HIPAA and GDPR. Moreover, their research extended and adapted the HIPAA framework and suggested five areas to preserve the privacy of patients' information by using new data-driven tools to manage their healthcare. The areas are health data in scope, regulated entities, permitted use of personal health data, security standards, breach notification requirements [22]. The limits of HIPAA framework are almost a quarter century old. Public may not trust the appearance of repeated scandals without clear guidelines. Therefore, the potentiality to adopt HIPAA is challenging to ensure confidentiality for digital health data [22].

Sahi *et al.* [29] suggested that e-healthcare provides benefits to the patients' and healthcare providers, however, the services are not fully developed and has lacked widely implemented obligatory facilities such as confidentiality, integrity, privacy and user trust. The quality of healthcare services and patient trust are the primary features of any healthcare operation. Trusts of the patients are dependent on the issues of confidentiality, authenticity and data management. Ensuring privacy is one of the biggest obstacles to achieving the success of the healthcare solution in winning the trust of the patients [30]. Privacy requirements are compounded by the fact that the healthcare data managing is extremely personal and private in nature, consequently, the misconduct either intentionally or by mistake can seriously affect the patient as well as the organizational prospects. Privacy concerns are identified in this research that focuses on certain failure parts of the healthcare organization to address all the aspects of privacy. Their research gradually alters the e-healthcare enterprise controls from an organizational level to the level of patients while doing the implementation. In this way, patients have more control over decision making to protect their healthcare information. Their investigation requires more efforts to do this assessment for altering to patients' level control from the e-health enterprise control. Moreover, their existing research is divided based on techniques used such as anonymization/pseudonymization and access control for the privacy of stored data that supports the privacy requirements (accountability, integrity, identity management) [15]. Their research mainly reviews existing related studies to find out if their proposals have any possibilities to the privacy requirements and concerns of the patients [29].

Shenoy and Appel [31] recommended that electronic health records (EHRs) support facilitated communication, ease of transferability and decrease rate of medical errors. While legal protections have been employed, EHRs still unable to ensure the privacy of patient's data and can face data breaches, therefore, the confidentiality of patient's health data is still a significant concern [31]. Keshta and Odeh [32] mentioned that medical professionals, patients and healthcare services can have many benefits if they adopt electronic health records for their healthcare organization. Besides, electronic health data management is a big concern particularly privacy and security of patient data in the healthcare organization. Their investigation mainly presented the privacy and security concerns of healthcare organizations and examine the available solutions. Effective encryption schemes to the patients' health records and multidisciplinary team, e.g. telecommunication, instrumentation and computer science to efficiently manage the electronic health records are recommended [32].

George and Bhila [33] suggested that keeping up confidentiality is the most crucial factor to maintain privacy in the healthcare sector. Professionals who do communicate with patients and have access to patients' health data must keep them confidential. Privacy towards personal data especially associated with health is significant for any human being. This research used an interpretive methodology that helps to identify the reality in health sectors with a face to face communications. Their investigation identified that the common threats of data loss and theft are dependent on certain disclosure types mostly unintentional and by third parties, hence, safeguarding confidentiality and privacy from breaches is obligatory [23]. Consequently, consent must be collected from patients in writing or electronically about medical data and this consent must be signed by the patient or authorised member. The patient must be aware of what kind of data is collected, where the collected data will be disclosed and the expiry of the consent. Correspondingly, the healthcare organization must ensure privacy by securing their database and can only disclose the data to the healthcare management team who have obligation to protect the data. Their study

mainly discovers the issues related to confidentiality and privacy in healthcare and its value to the patients and associated sectors [33].

The above investigations identified the critical data privacy areas, still, complete solutions are missing towards the construction of a data privacy framework. In the following section, we will investigate existing data privacy frameworks that have critically considered personal information protection for healthcare and similar environments. We critically analysed the below frameworks to identify the necessary components as well as their key limitations to establish a competent data privacy solution.

A privacy protection framework for public sector organizations is suggested by the Victorian public sector based on the context of privacy by design [34]. The purpose of this framework is to entirely safeguard personal data while collecting and managing it within the system. Besides, this framework offers embedded privacy into the design and architecture of the system from the commencement. An additional community dimension added by Privacy by Design (PbD) is to recognize that privacy contributes to the creation of public value, though privacy is considered an individual right. Privacy impact assessment is mentioned as the most useful tool to implement privacy by design. This tool is a point-in-time process to identify and evaluate privacy solutions by mitigating the risks. The potentiality of this framework is uncertain; therefore, privacy design strategies need to be considered in parallel with privacy by design principles to safeguard data leakages efficiently [34]–[36].

Moncrieff *et al.* [37] suggested a framework for the design of privacy-preserving in the healthcare sector. The objective of this framework is to eliminate enormous obstructions to setting up a ubiquitous healthcare system by detecting the issues through technology acceptance. A built-in information process flow is represented by this framework to achieve the objectives [37]. The outcome of the data fortification should be emphasized as the structure of this framework does not mention the information if any verified method had been used to construct this framework, for example, if any privacy by design standards, principles, and tools, etc. have been incorporated or not [38]. Moreover, patients' health data sensitivity and its surroundings are further limitations that can have a massive impact on the adaption of this framework [39].

'PReparing Industry to Privacy-by-design by supporting its Application in REsearch' (PRIPARE) is privacy by design framework that incorporates standards, contemporary practices, and studies on privacy engineering [40]. Subsequently, a method of system development phases is proposed by this framework. International Organization for Standardisation (ISO) 29100 is incorporated to establish the operational process of PRIPARE, the process is divided into seven phases and an additional one was assigned with organizational structure [41]. Privacy impact assessment is incorporated in parallel with one of the phases named analysis. Yet, privacy by design principles should be considered with privacy design strategies as they are fundamental components to outline the organizational and technical requirements [42].

Shrestha *et al.* [43] recommended a framework of 'Enhanced e-Health for privacy and security in the healthcare system'. This framework proposes to detect unauthorized user access to the patient's health records by following the privacy by design principles. Multi-authority-based access control is suggested by this study to defend unauthorized access of patient's personal data as the administrator of the system can misuse them while accessing the system and patients' health records are often exposed to third parties for healthcare purposes [30], [44]. Accordingly, the sensitive data should be retrieved by the doctor's consent or in some cases by the patient's consent to overcome this problem. While storing the data in the cloud, the pseudonymization technique is a preference to safeguard the privacy of personal data [45], [46]. Authorization and authentication are enhanced data privacy techniques that regulate the strategy to improve the effectiveness of the e-health system privacy. However, to ensure a competent privacy-preserving environment in the system, there is no attention to significant components e.g. privacy design strategies, privacy impact assessment which need to be measured appropriately [43].

'Privacy by design framework for assessing Internet of Things (IoT) applications and platforms' is suggested by Perera *et al*. [47]. Privacy by design fundamental principles and privacy design strategies are the core foundation of this framework. Privacy competencies and limitations of the current IoT applications are assessed in this study. Data breach threats are not measured by IoT applications [47]. Risk assessment should be considered, to do so privacy impact assessment should be explicitly considered by the IoT applications. Due to the insufficiency of systematic approaches, the intention of designing privacy for the software development measures in IoT is comparatively behind [48], [49].

Foukia *et al.* [50] suggested a method that mainly validates the data sources with privacy sensitivity and the data trail controller and delivers rights for third-party data processing during their application. This framework is termed as 'PISCES' which means privacy incorporated and security-enhanced system. One of the main functionalities of this framework is the separation between the data controller and the provider, where the provider manages the privacy of the data and the controller manages the privacy fortification of the provided data [51], [52]. This framework incorporates privacy protection from the initiation and during the operation of the information system which supports the fundamental principles of privacy by design [52], [53]. PISCES should incorporate with privacy by design components such as privacy design strategies and/or any security management tools that will be adverse to this framework to ensure an effective privacy-friendly system [54].

Privacy by design objectives are combined with International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 29110 to construct

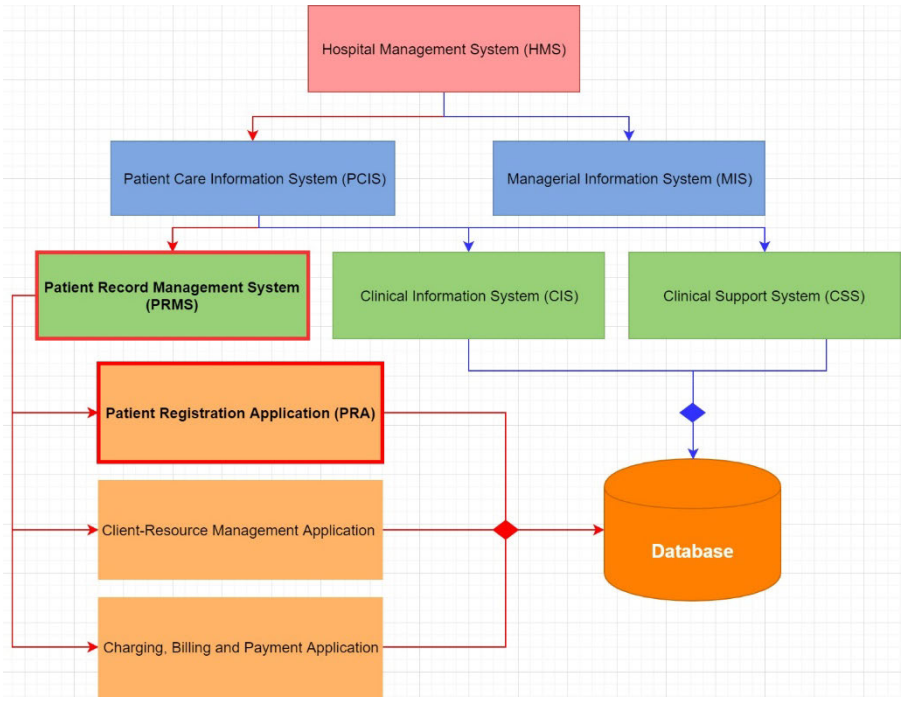

FIGURE 1. Relations of Patient Record Management System (PRMS).

a framework named 'ISO/IEC 29110 basic profile privacy by design in the healthcare sector' [55]. The goal of this framework is to provide direction to project management and software implementation to improve the quality of information systems. While developing this framework, fundamental principles of privacy by design are incorporated as a standard and privacy design strategies are unified as the functionality of the framework [56]. The consequences of adopting this framework may not be widespread as privacy impact assessment should be considered while developing this framework [57].

The key contexts of privacy by design are identified and discussed in this in-depth analysis. Detailed comparative analysis suggested by existing researches on data privacy frameworks had been highlighted in our previous research [6]. Based on the analysis key parameters of contemporary privacy by design frameworks are revealed to identify the limitations of each of the frameworks. These parameters are divided into categories such as Ann Cavoukian's seven fundamental principles of privacy by design, privacy design strategies, privacy impact assessment (PIA). We came to an assumption that the listed privacy by design key parameters is quite generic, thus the potentiality of developing the research towards building a framework is rather promising. Likewise, the available practices for dealing with data breaches are not the ultimate effective approach as has been mentioned and therefore a more comprehensive methodology is required to consider the several perspectives of the problem.

In this research, we identified the Hospital Management System (HMS) and its associated information systems that are holding patients' sensitive information presented in Fig. 1. The HMS is focused primarily on the operations management of the hospital. Two broad systems make up the Hospital Management System. They are the Patient Care Information System (PCIS) and Managerial Information System (MIS). The divisions of the Hospital Management System into these two broad systems are theoretical [20], [24].

A. PATIENT CARE INFORMATION SYSTEM (PCIS)

PCIS involves patients' personal and medical information, which are collected, managed, and released by this system. PCIS mainly consists of three sub-systems as outlined below [24].

1) PATIENT RECORD MANAGEMENT SYSTEM (PRMS)

PRMS is a sub-system of PCIS and consists of applications that enable care providers to keep track of individual or groups of patients in a fast, responsive, flexible, and friendly manner with efficient use of available resources. The PRMS consists of mainly three applications; Patient Registration Application (PRA), Client-Resource Management Application and Charging, Billing and Payment Application [20], [24]. Patient Registration Application (PRA) mainly managed the registry of the healthcare facility clients. Enlisting a new person as a patient in a healthcare institution is performed by this application. The functions include the collection of personal identification and demographic data, preserving the patient's personal record, maintaining

a permanent register of patients. Client-Resource Management Application mainly supports appointments, scheduling, allocation of the resources, patient tracking, creation of worklists, availability of resource tracking. Based on the needs of the patients, this application assigns the correct resources to a patient such as services of care provider, physical site (room/bed), etc. The Charging, Billing and Payment Application support the charging of actual assignment, bill calculation, e.g. payment made, credit balances, accounts receivable, etc. The design of this application is dependent on the policy as this is completely a business function [58], [59].

2) CLINICAL INFORMATION SYSTEM (CIS)

CIS facilitates patient care directly such as activities for care providers primarily doctors. nurses and medical professionals [59]. Healthcare professionals get support and assistance from CIS to perform their daily work, e.g. planning for care, clinical data entry, data storage, provision of clinical decision support, quality control, data retrieval and display. All of this collected information is stored in the database [24], [58].

3) CLINICAL SUPPORT SYSTEM (CSS)

CSS provides services to perform tests and provide supplies based on the tests. Care providers request these facilities through the CSS. Results of the test are submitted to the database of CSS from where they are made available. Supplies such as drugs, food, blood products and setline supplies are distributed to the responsible persons or units requesting them by CSS. The delivery details and the receipts are stored in the database [24], [58].

B. MANAGERIAL INFORMATION SYSTEM (MIS)

Managerial Information System (MIS) consists of several applications and sub-systems. MIS supports the hospital management team primarily for business operations, physical facilities and hospitality services. The components of MIS are wide-ranging and complex [24]. The business operations such as general administrative, hospitality management activities and facility activities are facilitated by MIS. The business operations are associated with Administration Information System, Accounting System, Human Resource Management System, Finance and Budgetary System and Purchasing and Inventory System. Physical facilities that support the hospital management are consists of Facility Engineering System, Equipment Maintenance System, Environmental Health, Safety and Waste Management System. The hospitality services are facilitated by Bed Management and Food-Beverage Order-Supply System. MIS is not within the scope of this research, however, mentioned as this is a sub-system of HMS [20], [24], [58]–[60].

Since our goal is to safeguard privacy designed for personal data collected from the patients, therefore this research focuses mainly on the protection of PRMS. PRMS principally collect, manage, store and release sensitive information related to the patients. In this research, the Patient Registration Application (PRA) of PRMS is selected to plan and execute our proposed framework. As we highlighted in our study that certain core mechanisms are missing in the current frameworks, hence, a sophisticated and enhanced framework is anticipated by integrating the obligatory mechanisms into the system architecture of PRMS.

V. THE PROPOSED FRAMEWORK

Multiple data privacy components such as strategies, principles, tools have been measured in the construction of the proposed framework. In this section, a detailed discussion on each of the subprocesses of the complete framework is carried out. A design science methodology is taken into consideration as no comprehensive method is presented by the existing studies to interpret privacy by design into system requirements. A literature review from our existing work is correspondingly used to outline the requirements [6]. Based on ISO/IEC 29100 [41], [55], the personal data privacy components are listed and mapped to design the proposed framework. Privacy standards and best practices and privacy impact assessment are measured in the delivery of a comprehensive privacy-preserving environment in the system design. The proposed framework has three main phases P1, P2, and P3 which are constructed based on ISO/IEC 15288 [61]–[63]. An overview of the phases is described below.

A. P1 - PLANNING PHASE

In this phase, privacy issues are acknowledged so they can be addressed in the implementation phase. Characterizing the system from privacy perception is the key objective. The limitations of contemporary privacy by design frameworks and suitable standards and best practices are identified here to safeguard the confidentiality of patients' health records.

1) P 1.1 COMPARATIVE ANALYSIS ON EXISTING PRIVACY BY DESIGN FRAMEWORKS

The key parameters of seven existing privacy by design frameworks are identified and presented in Table 1. A comparative analysis has been established based on the existing frameworks to highlight the limitations for each of them. There are several components suggested in existing studies, however, three globally verified components are relatively common. These components are selected by theoretical analysis in our research to identify the key limitations of existing studies. The selected components are seven fundamental principles of Privacy by Design (PbD) by Ann Cavoukian, privacy design strategies by Hoepman Jaap-Henk and privacy impact assessment (PIA). Seven fundamental principles of Privacy by Design (PbD) by Ann Cavoukian are applied as an essential component of fundamental privacy protection for personal information such as medical data. Privacy design strategies support privacy by design in the system development life cycle. Eight privacy design strategies deliver patterns for designing a privacy-friendly system. Privacy impact assessment identifies the impact of the proposed framework by applying systematic assessment on individuals' privacy. PIA works as a vital component in privacy protection and part of overall risk management. The success of the proposed

TABLE 1. Comparative analysis of existing frameworks.

Key Components of Privacy by Design	Frameworks						
	1	2	3	4	5	6	7
Seven Fundamental Principles of Privacy by Design (PbD) by Ann Cavoukian	**Privacy by Design in Victorian Public Sector [34-36]**	**Framework for the Design of Privacy-Preserving in Health care [37-39]**	**PRIPARE [40-42]**	**Enhanced E-Health Framework for Privacy in Health care System [30, 43-46]**	**Privacy by Design Framework for Assessing IoT Applications [47-49]**	**PISCES [50-54]**	**ISO/IEC 29110 with Privacy by Design in Health Care Sector [55-57]**
PbD1 Proactive not reactive; preventative not remedial	√			√	√	√	√
PbD2 Privacy as the default	√			√	√	√	√
PbD3 Privacy embedded into design	√			√	√	√	√
PbD4 Full functionality—non-zero positive-sum	√			√	√	√	√
PbD5 End-to-end security—full lifecycle protection	√			√	√	√	√
PbD6 Visibility and transparency—keep it open	√			√	√	√	√
PbD7 Respect for user privacy—keep it user-centric	√			√	√	√	√
Privacy Design Strategies by Hoepman Jaap-Henk							
a. Data-oriented strategies:							
i. Minimise		√	√		√		√
ii. Hide		√	√		√		√
iii. Separate		√	√		√		√
iv. Abstract		√	√		√		√
b. Process-oriented strategies:							√
i. Inform		√	√		√		√
ii. Control		√	√		√		√
iii. Enforce		√	√		√		√
iv. Demonstrate		√	√		√		√
Privacy Impact Assessment (PIA)							
a Integral	√		√			√	
b Fit for purpose	√		√			√	
c Comprehensive	√		√			√	
d Available	√		√			√	
e Enables compliance	√		√			√	
f Ongoing	√		√			√	
g Constructive	√		√			√	

framework depends on whether it meets the privacy expectation of the community and legislative privacy expectations. As the proposed framework will safeguard personal data, seven core elements of PIA are considered to design the privacy assessment to address the risks and their mitigation plan. A systematic literature review was conducted on our previous research which supports in parallel to detection the key parameters of data privacy frameworks. Therefore, these selected verified components are significant towards developing the proposed framework.

The key limitations of existing frameworks are identified based on a comparative analysis of seven existing privacy by design frameworks [6]. As we can see, the selected frameworks are not copiously included at least one or more of the key components to archetype the privacy contexts of their systems. Therefore, the potentialities of their proposed studies are crucial to the success of personal data privacy. To construct the proposed framework, we considered all the three globally verified key components to ensure a maximum privacy-preserving environment to patients' health records. The selected key components are mentioned as follows:

- Seven fundamental principles of privacy by design by Ann Cavoukian.
- Privacy by design strategies by Hoepman Jaap-Henk.
- Privacy impact assessment (PIA).

2) P 1.2 SELECTING STANDARDS AND BEST PRACTICES

We selected suitable standards and best practices to structure this framework such as covering the process and lifecycle stages, a set of controls to process personally identifiable information, identifying the privacy requirements in the system, etc. The standards and best practices considered to construct the proposed framework are outlined in Table 2.

B. P2 - ASSESSMENT PHASE

The assessment phase outlines the components and architecture to satisfy the requirements of the proposed framework. In this phase, seven fundamental principles of privacy by

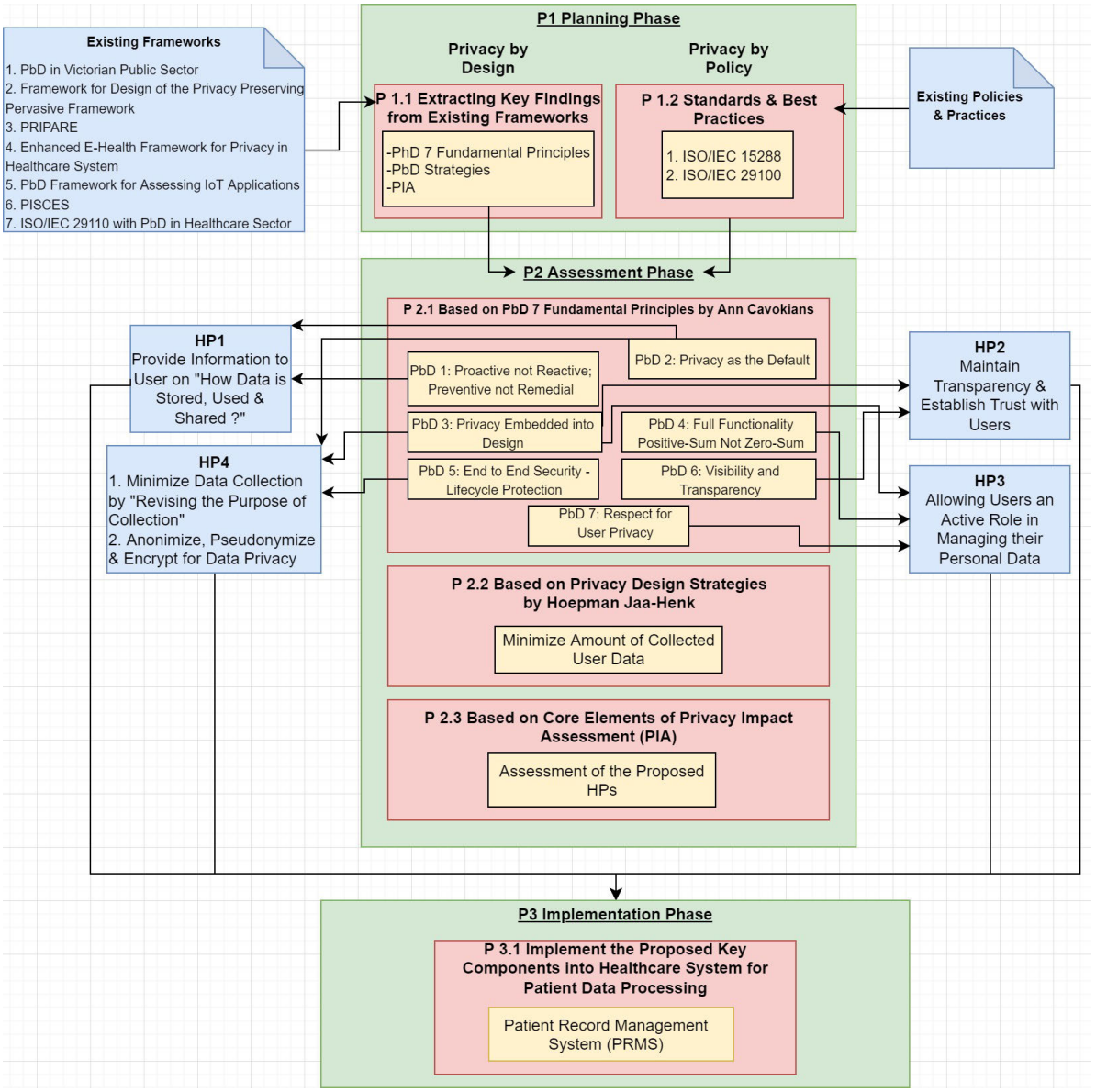

FIGURE 2. **Proposed Conceptual Framework. Key/Note: PbD - Privacy by Design, HP - Healthcare Principle, PIA - Privacy Impact Assessment, ISO/IEC - International Organization for Standardization/International Electrotechnical Commission, PRMS - Patient Record Management System**

design by Ann Cauvokian are assessed. Privacy design strategies suggested by Jeep-Hank Hoepman and privacy impact assessment is respectively considered to achieve the best consequences. By using the key components of privacy by design, necessary data protection and privacy requirements are acknowledged for the healthcare system in Fig. 2.

1) P 2.1 APPLYING THE FUNDAMENTAL PRINCIPLES OF PRIVACY BY DESIGN BY HYBRIDIZING WITH FOUR HEALTHCARE PRINCIPLES (HPs)

In the assessment phase, the first step does the function of assuring and coordinating compliance with the verified seven fundamental principles of privacy by design (PbD) suggested by Cavoukian [35]. Based on the fundamental principles of PbD, four healthcare principles (HPs) have been introduced to safeguard the personal data flow of patients. Seven fundamental PbD principles are defined as follows [36], [64].

PbD 1 PROACTIVE, NOT REACTIVE; PREVENTATIVE NOT REMEDIAL:

This principle commands that the privacy by design approach is considered proactive rather than reactive behaviour. In this technique, privacy-invasive events can be predicted and prevented before they even occurred. PRMS does not require waiting for a data breach to occur nor after it has occurred as the goal of this principle is to avoid the threats from happening.

PbD 2 PRIVACY AS THE DEFAULT:

This principle assures that the privacy of personal data is protected automatically in any system by its default. Users of the PRMS don't need any type of action to protect their

TABLE 2. Selected standards and best practices.

Standards and Best Practices	Description	Application
ISO/IEC 15288	A system engineering standard covers the processes and defines the lifecycle stages of systems that establish a common framework created by humans [61-63].	The proposed framework is constructed based on three stages planning, assessment, and implementation according to this standard.
ISO/IEC 29100	Framework and set of controls for organizations that process personally identifiable information [41, 55].	Based on this standard, potential privacy measures are listed and mapped to design the framework.

privacy as this principle ensures the privacy of personal data as its default operation. Thus, privacy by design principles enables the highest level of data fortification in healthcare systems.

PbD 3 PRIVACY EMBEDDED INTO DESIGN:

This principle ensures the integration of data privacy through the development of the PRMS. The core functionality is assimilated into privacy as an essential component of the PRMS without diminishing its functionality. PRMS is set up with this principle comprehensively and holistically throughout the system architecture. This principle, therefore, estimates the impact of privacy and reduces the data breach of PRMS through usage, error, or misconfiguration with potential measurements.

PbD 4 FULL FUNCTIONALITY—POSITIVE-SUM NOT ZERO-SUM:

This principle accommodates the objectives and legitimate concerns in a positive-sum and rejects which are redundant such as availability vs privacy or security. The full functionality approach is significant to evade while any unnecessary trade-offs of privacy occur between the user and the system.

PbD 5 END TO END SECURITY - LIFECYCLE PROTECTION:

This principle guarantees that privacy is integrated throughout the PRMS life-cycle process in a constant manner and data is erased at the end of the process promptly. Privacy by design is embedded in PRMS before the initial information is processed towards the end of the lifecycle.

PbD 6 VISIBILITY AND TRANSPARENCY:

All stakeholders involved in business practice or the technologies with PRMS are assured by this principle that all actions need to remain visible and transparent to the providers and the users. This principle assures that PRMS can operate as per its goals and promises with autonomous verification.

PbD 7 RESPECT FOR USER PRIVACY:

To keep the individuals' uppermost interest, privacy by design offers noticeable principles to the processes by offering robust privacy measurement as default. This principle offers user-friendly options to the users of PRMS with appropriate notices and possibilities while collecting personal data intended for keeping the system user centric.

We combined the seven fundamental privacy by design principles with four healthcare principles (HPs) to simplify the design process. Implementing the HPs as a design framework allows to feature data privacy by default.

The proposed HPs will ensure strong privacy and personal control over sensitive information for a justifiable competitive benefit to healthcare organizations. The proposed HPs function as follows.

HP1. PRIVACY AND DATA SHARING NOTICES:

HP1 delivers strong confidentiality and data sharing notices to let users know how the personal data are stored, used, sharing and deleted. This principle delivers a brief description of the data once the user will submit them and notify if the data will be stored in a database or sent to a third party and the time boundary of data storage. Based on the requirements of the specific healthcare organization, the notices will be designed. HP1 is founded on PbD 1 Proactive not reactive; preventative not remedial & PbD 2 Privacy as the default (Fig. 3 (a)).

HP2. TRANSPARENCY AND TRUST WITH THE USERS:

HP2 provides notices with an advanced layer of information privacy that work by demonstrating a quick message to the specific fields as soon as a user is about to enter their personal information in a registration form. This notice delivers the purpose of the collection of specific data fields such as a medical report, laboratory or diagnosis purposes, etc. HP2 is based on PbD 3 Privacy embedded into design & PbD 6 Visibility and transparency (Fig. 3 (b)).

HP3. ALLOWING USERS TO MANAGE PERSONAL DATA:

HP3 authorizes the users to accomplish a dynamic character in the management of their data by requesting them to tick a checkbox to accept that they've read through the terms and conditions of the collection of their personal or sensitive information. As per HP3, checkboxes are not pre-ticked, and users must agree with the terms and conditions to continue. HP3 is based on PbD 3 Privacy embedded into the design, PbD 4 Full functionality—Positive-Sum Not Zero-Sum & PbD 7 Respect for user privacy (Fig. 3 (c))

HP4. DATA COLLECTION MINIMIZATION:

HP4 minimizes data collection amount by reviewing the reason for which this system is accumulating them as well as anonymize, pseudonymize or encrypt them to ensure the privacy of the collected data. HP4 is grounded on PbD 2 Privacy as the default with PbD 3's Privacy & PbD 5's End-to-end security - Lifecycle Protection (Fig. 3 (d)) embedded into its design.

Healthcare principles work as core assumptions whereas privacy design strategies are guidelines that function throughout the behaviour and development of the PRMS. In the following step, privacy design strategies are evaluated to be comprised in the system development during the implementation phase.

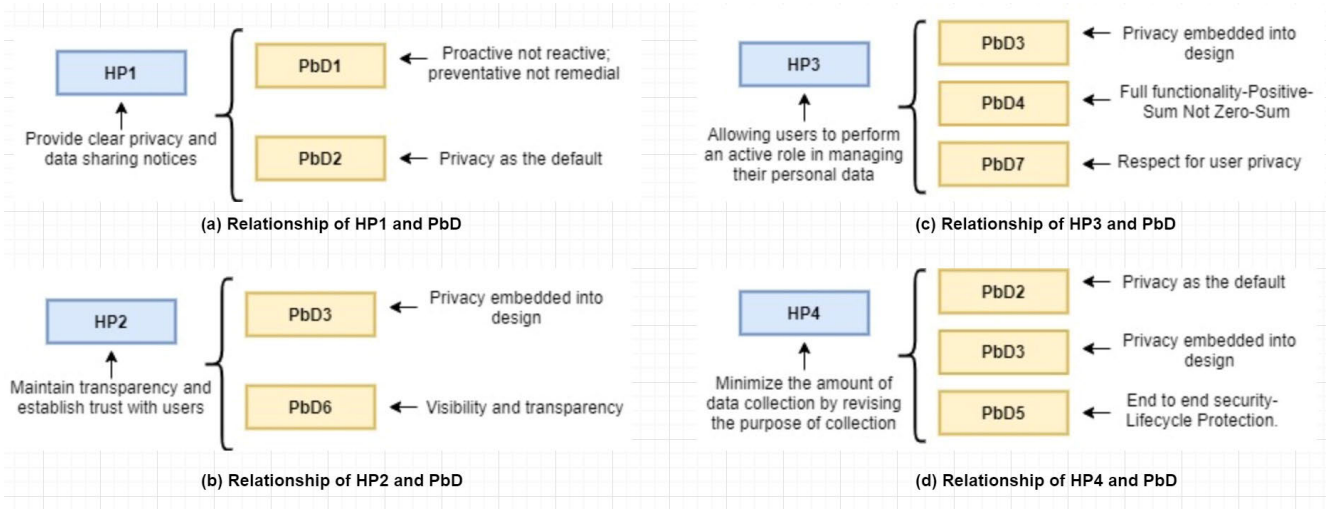

FIGURE 3. Relationship of HPs and PbD.

2) P 2.2 IMPLEMENTING PRIVACY DESIGN STRATEGIES

Hoepman [65] suggested privacy design strategies that are applied in this step to establish a privacy defensive environment in the PRMS. Privacy design strategies assess the privacy impact of the available systems and suggest possible design patterns to establish an entirely preserved system through suitable privacy methods. During the concept development, design strategies support system architects to evaluate the privacy of personal data in the software development life cycle [65]. Privacy design strategies are divided into two parts.

a: DATA-ORIENTED STRATEGIES

1) i. MINIMIZE

In this proposed framework, the most elementary data-oriented strategy is the minimize as it offers the assurance of a limited amount of personal data collection. This strategy recommends that only essential data needs to be collected from the patients to provide medical services, therefore, the chances are less for data theft, accidental data leakage, and misuse of personal data [65]. Moreover, individual users have the right to take decisions by choosing the options to process or obliterate their data while using the system. Anonymisation is a design pattern for this strategy [66].

2) ii. HIDE

This strategy delivers restrict access to personal data by preserving properly protected data collection by masking them from plain view to evade a variety of misuses. Hide allocates the data away from other parties while collecting and processing legitimately by a single unit. This strategy suggests that the information that requires privacy must not be comprehensible in plain sight particularly their interrelationships. Personal data masking from plain view helps to avoid data exploitations. This strategy keeps the data secure from other parties while the data is collected and administered legitimately within a single entity [65]. The Hide strategy mainly ensures the confidentiality of the patients' health data in PRMS. The design pattern recommended by this strategy is the pseudonymization technique that will de-link connections such as attribute-based credentials [67], [68].

3) iii. SEPARATE

This strategy provides data separation by data property perception where data is collected and processed anonymously wherever possible. Information contents enclosed within them are categorized while collecting and forming in the system [65]. This strategy enhances the personal information privacy to any type of patients' health data including non-stored data in the database such as emails, reports, system logs. Patients' health data that are stored in transactional and analytical systems of PRMS may result in privacy violations if accessible by unauthorized people [65]. Encryption is a design pattern recommended by this strategy. Using the encryption method strongly reduces the probability of exposure to private information [69], [70].

4) iv. AGGREGATE

In this strategy, the capacity of personal information within the group of attributes is controlled and managed with minimum feasible details and a maximum level of combination to make them less sensitive [65]. A limited number of data are authorized to the individual patient as the data group sizes are extensive, despite the fact, the data are uneven for protecting privacy [71], [72]. Data encryption is a design pattern that allows users to encrypt the entire database to secure the data in the database [73].

b: PROCESS-ORIENTED STRATEGIES

1) i. INFORM

This strategy resembles the concepts of data transparency and ensures up-to-date data subjects while processing

personal data. Patients will be notified about categories of data and the purpose of processing the data when uses the PRMS. Besides, if any information is required to share with the third parties that will be informed to the patient or authorized receipts while necessary [65]. The data access privileges are informed to the users and the behaviours to exercise those privileges. This strategy is applied via healthcare principle 1 (HP1). Informing the users of PRMS from the understanding of human-computer interfacing is a design pattern of this strategy that stimulates the diversity of data privacy design [35].

2) ii. CONTROL

While processing personal data, mandatory measurements are encouraged by the users by this strategy. In some cases, users have the right to control their personal information while data protection legislation is in place. Inform strategy and control strategy are compatible with each other. The system will request permission from the users to control specific information to get them processed [65]. This strategy is executed by healthcare principle 3 (HP3) that will ask the users to select the checkbox option for authorizing the terms and conditions of personal data collection. Control applies the rights to the data protection, therefore, data quality will increase as users will be able to control error correction [35].

3) iii. ENFORCE

Enforce confirms privacy policy with legal obligations is in place in a precise manner. This strategy assures the privacy measurement in place during the operation of PRMS and the policies will be imposed when necessary [65]. Healthcare principle 4 (HP4) works as a design pattern for this strategy that will be executed by access control and minimization of personal data [35].

4) iv. DEMONSTRATE

This strategy supports by controlling the compliance of privacy policy and the public key infrastructure. Data controllers are required by this strategy to regulate that it is in control. In case of any issues, users can directly assess any viable data breach [65]. Healthcare principle 2 (HP2) is applied as a design pattern for this strategy over auditing, management of privacy, and logging practice. Strong privacy and security technique implementation are additional support while embedding the public key infrastructure in healthcare systems [35].

P 2.3 DATA PROTECTION USING PRIVACY IMPACT ASSESSMENT (PIA)

This step does data fortification by measuring the privacy impact of the proposed healthcare principles. Privacy impact assessment (PIA) is a critical part of the assessment phase. To overcome substantial and undesirable privacy impacts, PIA is undertaken early enough to influence the implementation. To do the impact analysis of privacy, guidelines of PIA suggested by the Office of the Australian Information Commissioner are applied. This assessment does ensure that privacy is put into consideration throughout the process of planning [74]. The PIA being used consistently does avoid and mitigate the risks and minimizes the privacy issues within the entity. Seven core elements of privacy impact assessment are used in parallel to frame this assessment plan. The purpose of the seven core elements towards the privacy impact assessment is described here [57], [74]–[76].

a: INTEGRAL TO ORGANIZATIONAL GOVERNANCE

The structure of the health organization governance is an integral part of the privacy impact assessment. This is one of the most effective elements while assessing privacy risks and developing the impact assessment report of the healthcare organization.

b: FIT FOR PURPOSE

According to the potential privacy risks, privacy impact assessment needs to be shaped. If low risks are identified with a preliminary assessment, a short PIA is adequate. A more extensive PIA is required if a high risk of privacy issues to sensitive information to a large number of individuals is identified.

c: COMPREHENSIVE

Privacy impact assessment covers the issues of information privacy and provides support to construct or regulate the plans of privacy management and policies of human resources when required.

d: AVAILABLE

A summary report on considered privacy issues will be available to search and notify for providing feedback or else a privacy impact assessment full report will be publicly available for the feedback.

e: ENABLES COMPLIANCE

Privacy impact assessment addresses all privacy obligations containing obligations under privacy requirements for movement of health information for instance healthcare principles (HPs) and PIA guidelines.

f: ONGOING

A constant review mechanism is considered to estimate privacy issues during the lifecycle of the proposed system. If any substantial changes to how the personal information is managed, then a further privacy impact assessment will be undertaken.

g: CONSTRUCTIVE

The privacy impact assessment contributes to the success and includes value to the privacy culture of the healthcare organization by managing the privacy risks of the proposed healthcare system.

The privacy implications are assessed concerning the proposed healthcare principles (HPs) in Table 3. As this is

TABLE 3. Privacy impact assessment compliance with the proposed HPs.

HP1: Privacy and data sharing notices		Y	N	HPs
1.1	Does the system involve healthcare information?	X		HP1 – PbD 1 & PbD 2
1.2	Do all the personal data that are collected important for this system?	X		HP1 – PbD 1 & PbD 2
1.3	Is the personal data received directly from the individual user?	X		HP1 – PbD 1 & PbD 2
1.4	Will any of the personal data be gathered indirectly from another source?	X		HP1 – PbD 1 & PbD 2
1.5	Will this information be provided "where and how will personal information be stored?"	X		HP1 – PbD 1 & PbD 2
1.6	Will the system notify the user of performing any further use of personal data?	X		HP1 – PbD 1 & PbD 2
1.7	Will the system inform the user about the time limit of holding personal data?	X		HP1 – PbD 1 & PbD 2
1.8	Will any personal data be shared outside of the healthcare organization such as another healthcare department, laboratory, or diagnostic centre?	X		HP1 – PbD 1 & PbD 2
HP2: Transparency and trust with the users				
2.1	Will the user be notified by the system while collecting personal data?	X		HP2 – PbD 3 & PbD 6
2.2	Will this be informed to the users if their data have been collected from other sources, e.g., other clinics/hospitals?		X	HP2 – PbD 3 & PbD 6
2.3	Will the user be reported for collecting the necessary personal information?	X		HP2 – PbD 3 & PbD 6
HP3: Allowing users to manage personal data				
3.1	Will the user be authorized in managing their personal or sensitive data?	X		HP3 – PbD 3, PbD 4 & PbD 7
3.2	Is the sensitive or personal data in the system that require the user's authorization to be used or disclosed for the primary purpose for which it has been collected?	X		HP3 – PbD 3, PbD 4 & PbD 7
3.3	Does the system use or disclose personal information (including sensitive information) for a new or additional purpose that will require authorization by users other than the original purpose of collection?	X		HP3 – PbD 3, PbD 4 & PbD 7
HP4: Data collection minimization				
4.1	Are the existing or proposed privacy measures in place to shield the personal data collected and managed in this system?	X		HP4 – PbD 2, PbD 3 & PbD 5
4.2	Will the collected data be minimized before storing it in the database?	X		HP4 – PbD 2, PbD 3 & PbD 5
4.3	Do users have the option to not identify themselves, or use a pseudonym when dealing with the data?		X	HP4 – PbD 2, PbD 3 & PbD 5
4.4	Will the personal information will be deleted once no longer required?	X		HP4 – PbD 2, PbD 3 & PbD 5
Risk identifier: If any of the above answers are NO then this will need to address the risk appropriately in the 'Privacy Risk Mitigation' in Table 4.				

a preliminary privacy impact assessment, therefore the assessment is not static, more privacy implications can be included if necessary. PIA Guidance from the Office of the Australian Information Commissioner is used for examples of potential risks while doing the following assessment [57], [74]. Based on the assessment, the identified risks are analysed, and a risk mitigation plan is established for individual risks in Table 4. The outcome of the privacy risk

TABLE 4. Privacy risk assessment.

Risk No	Description of the identified risk	Impact	Likelihood	Risk level	Risk mitigation Plan	Residual risk level
2.2	Users will not be notified if the information has been collected from another source, e.g., other clinics/hospitals.	High	Medium	Medium	If the patient is incapable to provide information, a healthcare organization may collect data from another source to provide urgent medical services. In this case, an authorized 'next to kin' will be notified to continue the treatment.	Low
4.3	Users will not have the option to be unidentified themselves or use a pseudonym when dealing with the data.	Medium	Low	Medium	As this information will be collected for medical purposes, so the users will not have the option to pseudonym themselves while getting their treatment. This proposed system will provide a high level of data privacy as no information will be disclosed anywhere without the consent of the user.	Low

assessment is low; therefore, the proposed framework is highly potential to do the implementation.

h: COMPATIBILITY OF THE PROPOSED PRINCIPLES AND AUSTRALIAN PRIVACY PRINCIPLES (APPS)

The Australian Privacy Principles (APPs) control the collection and use of personal information within Australia [77]. Correspondingly, The General Data Protection Regulation (GDPR) regulates how personal information can be managed by the European Union (EU). Table 5 highlighted that the principles of the proposed framework are compatible with the Australian Privacy Principles (APPs) [77].

i: COMPATIBILITY OF THE PROPOSED PRINCIPLES AND THE GENERAL DATA PROTECTION REGULATION (GDPR)

The General Data Protection Regulation (GDPR) enforced by the EU is a landmark in the evolution of the European privacy framework. Seven data protection principles are supported by GDPR that provide organizations with guidance on collecting, processing and storing individuals' personal data and achieving compliance with GDPR [26]. The purpose of GDPR is to deliver a set of data protection laws across all the members of the EU. GDPR provides the general people to understand the use of their data and raise any complaints if required. The compatibility of the proposed principles and GDPR are outlined in Table 6 [78].

Our research is based in Australia, thus the compatibility of the proposed framework principles and Australian benchmark standard Australian Privacy Principles (APPs) have been accomplished. In addition, General Data Protection Regulation (EU) (GDPR) is broadly applicable, widely considered and comprehensive privacy legislation permitting the value of personal data globally. GDPR is a European Union ruling while has profound significance on all organizations worldwide. Both APPs and GDPR are the standards to be measured while collecting, processing and storing personal data, hence, our research considered both APPs and GDPR to measure compliance with the proposed framework. Based on the analysis shown in Table 5 and Table 6, we identified that our proposed principles have comprehensive compatibility with the two benchmark standards that supports us to guarantee maximum privacy as a result of achievement in patients' health records.

C. P3-IMPLEMENTATION PHASE

1) P 3.1 IMPLEMENTATION OF THE SELECTED REQUIREMENTS INTO THE HEALTHCARE SYSTEM

The healthcare principles (HPs), privacy design strategies, and privacy mechanisms extracted from the assessment phase are implemented into the PRMS to prevent privacy-invasive events before happening. We have particularly selected the Patient Registration Application (PRA) of the PRMS to determine the execution of the implementation phase. The data flow diagram in Fig. 4 illustrates the entire process involved between the 'user' and the 'database' in the PRA. The data flow diagram shows where the proposed healthcare principles (HPs) and privacy design patterns are implemented in PRA to collect user data with the user's consent and acceptance. The PRA has collected the necessary user registration details such as personal details, emergency contact, allergies, and medical information, insurance details, payment details, etc. Patient registration details are constructed as per the Client Registration Policy – Ministry of Health, NSW Australia [79].

Based on HP1, as the user enters into the registration page an agreement will be displayed providing a detailed

TABLE 5. Compatibility of the proposed principles and APPs.

	Australian Privacy Principles (APPs)	Purpose of APPs	Compatibility with the principles of the proposed framework
APP 1	Open and transparent management of personal information	This principle consists of an advanced and clearly expressed privacy policy to ensure that personal information is managed openly and transparently.	HP2
APP 2	Anonymity and pseudonymity	APP 2 provides individuals with the opportunity of not disclosing their identification and supports with anonymity and pseudonymity.	HP3, HP4
APP 3	Collection of solicited personal information	This principle ensures higher privacy while collecting the personal and sensitive information of an individual.	HP1
APP 4	Dealing with unsolicited personal information	This principle outlines how unsolicited personal information will be dealt with.	HP1
APP 5	Notification of the collection of personal information	APP 5 provides notification to an individual while collecting their personal information.	HP1
APP 6	Use or disclosure of personal information	APP 6 outlines the circumstances while using and disclosing personal information.	HP2
APP 7	Direct marketing	Organizations should ask permission from individuals while using or disclosing personal information for marketing purposes.	HP3
APP 8	Cross-border disclosure of personal information	APP 8 provides the stages that must take to protect while the information requires to disclose to overseas.	HP3
APP 9	Adoption, use or disclosure of government related identifiers	APP 9 outlines the conditions when government-related identifiers are assumed of an individual as its own or disclose or use of government-related identifiers.	HP2
APP 10	Quality of personal information	App 10 ensures with reasonable steps that the collected personal information is correct, up to date and complete. This principle also ensures the information it uses is correct, relevant and up to date.	HP4
APP 11	Security of personal information	This principle ensures personal information is protected from misuse, loss and unauthorized access or disclosure without the user's permission.	HP4
APP 12	Access to personal information	This principle outlines the obligations to provide access to individuals' requests to access personal information.	HP3
APP 13	Correction of personal information	App 13 provides obligations when it is necessary to correct individuals' personal information.	HP3, HP4

description of the data collection and usage policy. Based on the user's consent, upcoming web pages will be displayed or not displayed. The next page of the patient registration application uses HP2 measures to display ''just-in-time notices'' alongside specific data fields or attributes that require an extra layer of privacy while presented on the web pages. HP2 applies to specific attributes that will display pop-up notices to the users while collecting the information. All attributes with and without HP2 are mentioned in Fig. 4. At each step, as the user enters the data into the entry fields it is sent to temporary storage called ''cache memory''. After collecting all the required user details, the system is designed to apply HP3 that will allow users to manage their information by requesting user consent and acknowledgment. Obtaining 'user consent' is an important step in the data flow of the PRA because it will let the users know and manage the data collection, usage, sharing, and storage policy of the system. The user consent is authorized using a ''One-Time Password'' (OTP) that is sent to the mobile number provided by the user.

After successfully authorizing that the user has accepted the terms and conditions, the system will ask the user for 'acknowledgment' before sending the entered details into the 'cache memory'. Cache memory allows the system to store the entered details temporarily in the memory so that the footprint of the real data is not stored anywhere and can be removed easily after entering the database encrypted or hidden. HP4 measures are applied to the data that are presented in the cache memory. HP4 is used to apply Dynamic Data Masking (DDM) and Transparent Database Encryption (TDE) on the user data before storing it into the database to ensure privacy and security for the user data [80], [81]. After successfully storing the processed data into the database, the real data in the cache memory is removed forever, as observed in Fig. 4. If the user does not acknowledge the terms and conditions, the data present in the cache memory will be removed.

After collecting and storing the user-provided details in the cache memory, attribute splitting is performed to separate the real data in the cache memory into 'attributes for

TABLE 6. Compatibility of the proposed principles and GDPR.

	The General Data Protection Regulation (GDPR)	Purpose of GDPR	Compatibility with the principles of the proposed framework
1	Lawfulness, fairness and transparency	This principle provides full transparency for all EU data subjects when collected. The organizations must let the individual know about the collection, processing and disclosure of personal data in accordance with the law.	HP1, HP2
2	Purpose limitation	Personal information must be collected and processed for a legitimate reason. Without the consent of the individual, personal data must not be processed for any other reason. This principle ensures that personal data can only be used for a nominated purpose.	HP3, HP4
3	Data minimization	A minimum amount of data should be collected that is necessary for the purposes they are processed. This principle assures that only related, adequate and limited personal data should be collected and managed by the organizations.	HP4
4	Accuracy	The collected personal data must be accurate and up to date. The collected data should be reviewed in a timely manner and inaccurate data should be amended and if necessary, deleted by the responsible organizations. Individuals should have the right to rectify and erase their inaccurate and incomplete data to improve compliance and ensure up-to-date databases.	HP3
5	Storage limitation	An organization must delete the personal data if no longer needed for the purpose it was collected for. GDPR does not provide the time framework for holding personal data, it depends on the policy of the organization. Organizations should review the collected data to preserve the necessary and up-to-date data to ensure compliance.	HP4
6	Integrity and Confidentiality	This principle ensures that appropriate measures should be in place to secure the collected personal data from internal threats, e.g. accidental loss or damage, unauthorized use and external threats, e.g. malware, phishing. Organizations should provide appropriate levels of security to address the risks while processing personal data.	HP1, HP4
7	Accountability	This principle ensures that organizations must be in compliance with the other principles and take responsibility for the data they are managing with the necessary steps.	HP2, HP3

full masking', 'attributes for partial value blurring', 'email blurring', and 'attributes for random masking function' to apply the Dynamic Data Masking Methods before storing the processed data into the database, as shown in Fig. 4.

Fig. 5 shows the application of dynamic data masking on the real data attributes that are collected in the cache memory and transparent database encryption procedure to secure the database by creating certificates and privileges for the employees accessing the database. This allows the PRMS to protect the user data and to only provide access to people based on the decided policy measures [80], [82].

a: DYNAMIC DATA MASKING (DDM)

With the unprecedented increase in the collection of sensitive information from users, many organizations want to put security 'close to the data [81]. Security in terms of encryption, network firewalls, etc. This research has utilized the use of dynamic data masking methods to hide the data that is collected from the users, when storing it (data) in a database so that no unauthorized users can access the data. Dynamic data masking (DDM) allows the applications to simplify the design and coding of security [80], [83]. It also allows the data owners to decide 'how much data to reveal?' to the users based on their permissions. DDM method provides full masking, partial value blurring, email blurring, and random masking functions. These functions are used to mask the data in the database. With the implementation of DDM only designated users can access sensitive information [80].

After collecting the information from patients, as seen in Fig. 5, the collected attributes are split into 'attributes for full masking', 'attributes for partial value blurring'', 'email blurring', and 'attributes for random masking functions'.

2) i: ATTRIBUTES FOR FULL MASKING

Fig. 6 shows the attributes that are selected for full masking. The full masking function allows for masking of the attribute values according to the data types. It is a '*default*' function.

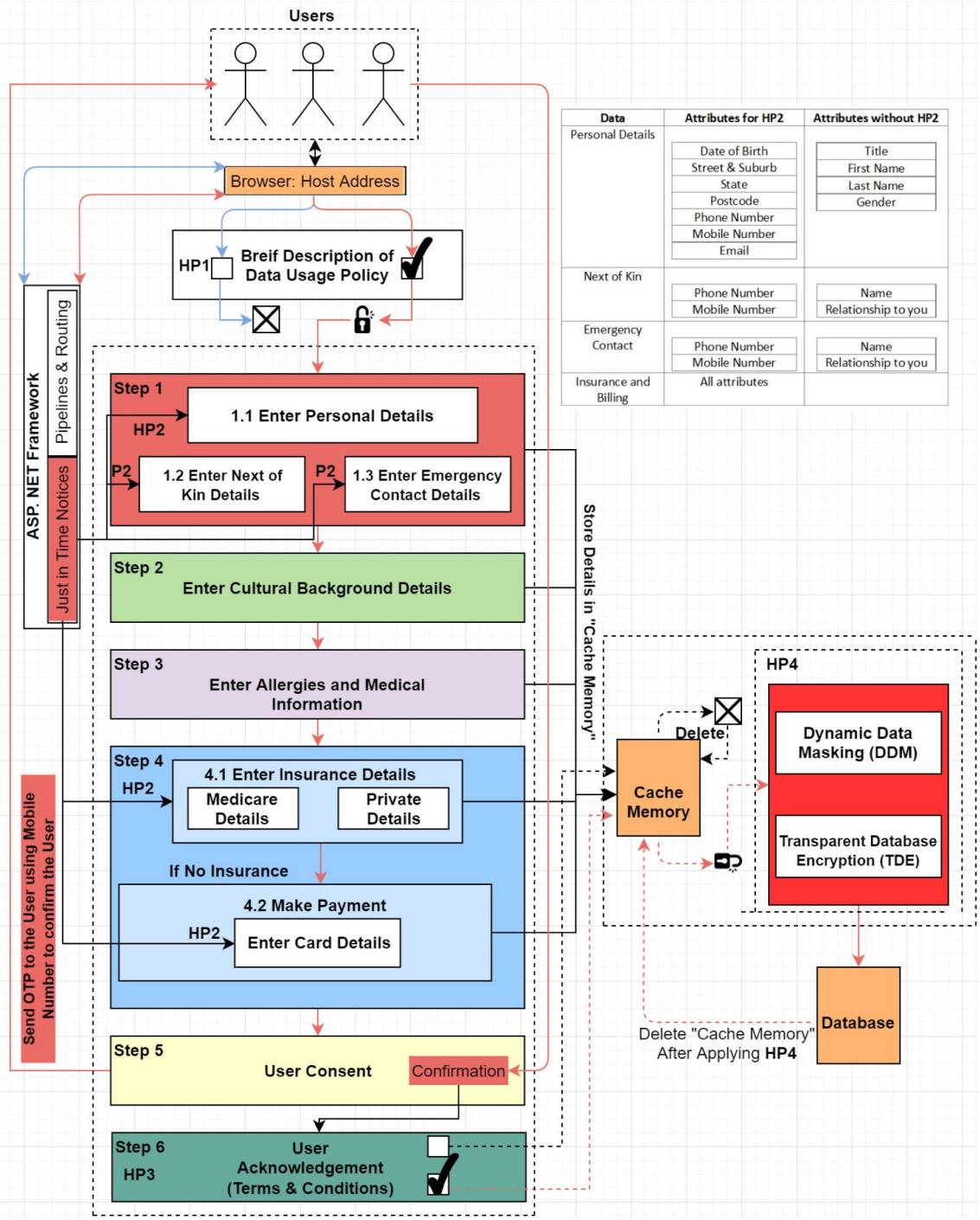

FIGURE 4. Dataflow of Patient Registration Compliance with Proposed HPs.

For string data types, the values are replaced with XXXX and for numeric data types, the values are replaced with Zeros.

Example SQL Syntax: **[First Name] [nvarchar](n) MASKED WITH (FUNCTION='default()') NOT NULL**

Using the above syntax applies the *default()* function on the attribute 'First Name' and fully mask the values with 'XXXX'. Similarly, all the attributes showcased in Fig. 6 are applied with *default()* function to fully mask them when storing them in the database. Table 7 provides examples of masking using the default () function.

3) ii: ATTRIBUTES FOR PARTIAL VALUE BLURRING

Fig. 7 shows the attributes that are selected for partial value blurring. Partial value blurring is applied using the *Custom String* function, a custom *padding string* can be added

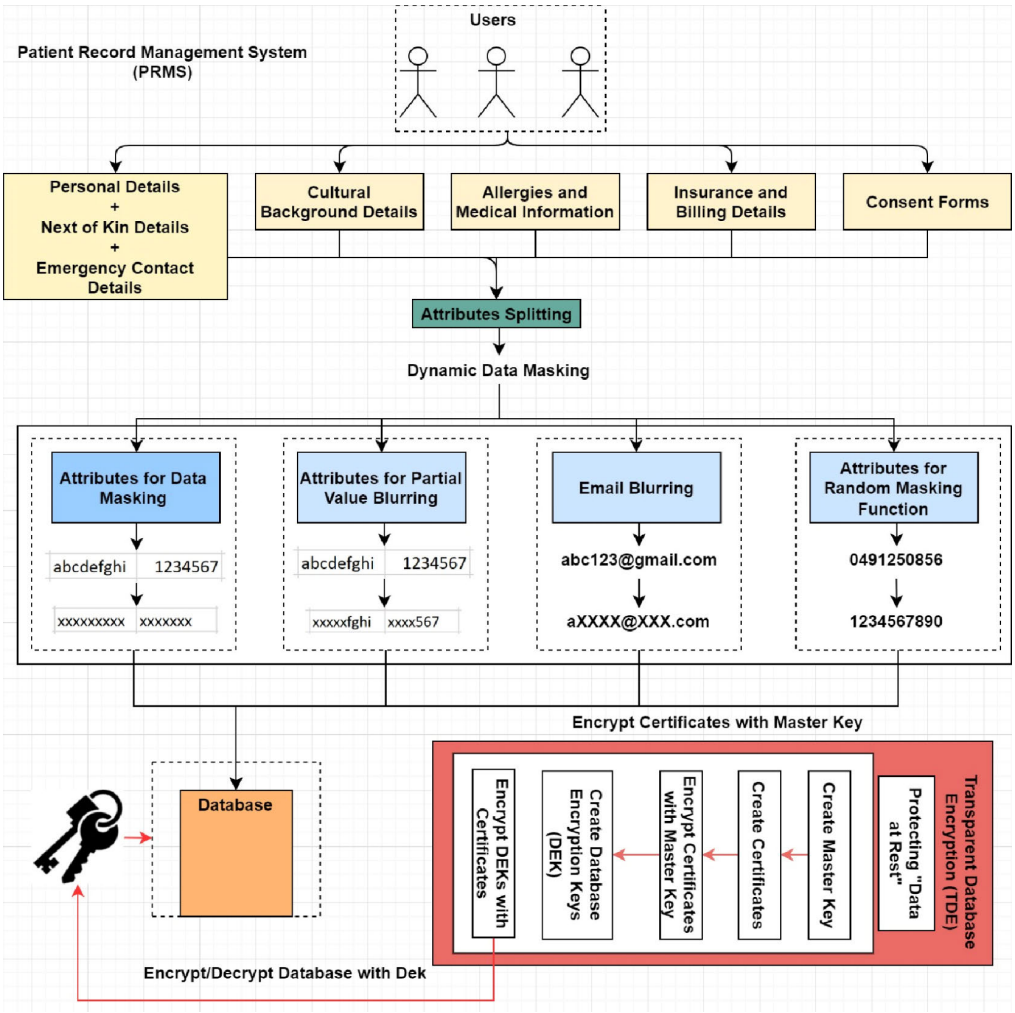

FIGURE 5. Application of Dynamic Data Masking (DDM) & Transparent Database Encryption (TDE).

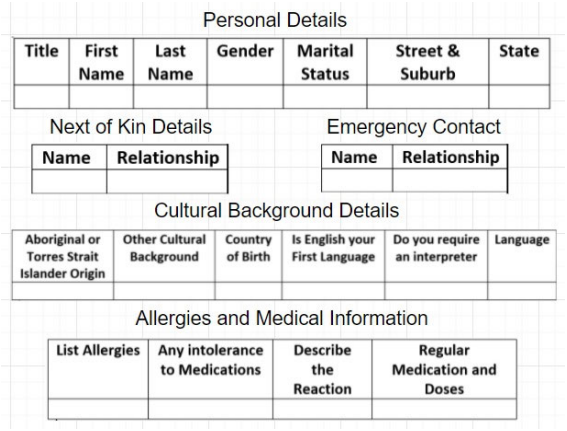

FIGURE 6. Attributes for Full Masking.

TABLE 7. Default() function example.

Function	Data Types	Examples
Default()	Works with all data types. String (char, nchar, varchar, nvarchar, text, ntext, etc)	ALTER COLUMN <First Name> ADD MASKED WITH(FUNCTION = 'default()') First Name - Joe (Joe – XXX)
	Numeric (bigint, int, decimal, real, float, etc)	Replace with '000'

between the prefix and suffix of a value, only exposing the first and last letters.

Example SQL Syntax: [Medicare Card No.] [varchar](n) MASKED WITH (FUNCTION='partial(prefix, ''XXXX'', suffix)') NOT NULL

Using the above syntax applies a *custom string* on the attributes selected for partial value blurring. This syntax only key keeps the prefix and suffix in the attribute value and replaces the middle part with XXXXX. Different custom strings can be created for different attributes. Table 8 provides

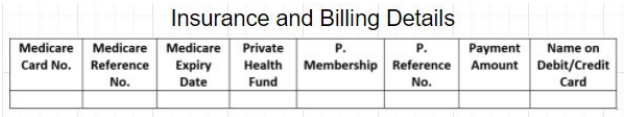

FIGURE 7. Attributes for Partial Value Blurring.

TABLE 8. Custom string function example.

Function	Data Types	Examples
Custom String	Supports String data types (char, nchar, varchar, nvarchar, text, etc)	ALTER COLUMN <Medicare Card No.> ADD MASKED WITH(FUNCTION='partial(1, "XXX", 2)') Medicare Card No. – 12342 (12342 – 1XXX2)

the example of *custom string* function used for partial value blurring.

4) iii: EMAIL BLURRING

Using the *Email* function, the email addresses can be masked directly. This function will only expose the first letter of the email and the constant suffix ".com" in the addresses.

Example SQL Syntax: [Email] [nvarchar](n) MASKED WITH (FUNCTION='email()') NOT NULL

This syntax by default will only expose the first letter and the suffix (i.e., aXXX@XXX.com).

5) IV: ATTRIBUTES FOR RANDOM MASKING FUNCTION

Fig. 8 shows the attributes that are used for 'random masking'. Random masking function works on only numeric data types. The function masks the original value with random values within a specified range.

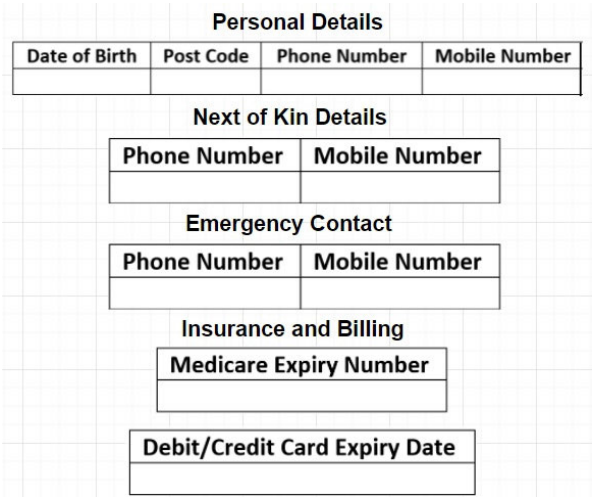

FIGURE 8. Attributes for Random Masking Function.

Example SQL Syntax: [Mobile Number] [bigint](10) MASKED WITH (FUNCTION='random([start range], [end range])') NOT NULL

This syntax allows for masking of the values present in the 'Mobile Number' attribute with random values within a specified range. Similarly, all the attributes selected for random masking are masked based on respective syntaxes and ranges. Table 9 provides an example of *random* function.

TABLE 9. Random function example.

Function	Data Types	Examples
Random	Supports Numeric data types (bigint, int, decimal, real, float, etc)	ALTER COLUMN <Mobile Number> ADD MASKED WITH(FUNCTION='random(0, 9)') Mobile Number – 0491250955 (0491250955 – 9865684485)

6) V: IMPLEMENTATION OF DYNAMIC DATA MASKING METHODS AND SETTING UP PERMISSIONS

After collecting the data and storing it in the cache memory, dynamic data masking is performed based on the attributes. The masked data is then stored in the database. Only the administrator can access the whole unmasked database. Other users need permission to unmask the masked data in the database. The following steps are required to implement dynamic data masking methods and set up permissions for the users:

Creating The Database

Pseudo Code 1 Creating the Database

```
USE [Admin]
GO
CREATE DATABASE [database name]
[CONTAINMENT= {NONE | PARTIAL | FULL}]
[ON
[PRIMARY]<filespec> [,.....n]
[, <filegroup> [,....n]]
[ LOG ON<filespec> [,....n]]
]
GO
```

Pseudo-code 1 is used to create the database by providing information related to the database specifications and groups. The argument *containment* is used to specify the containment status of the database (i.e., NONE = Non-Contained Database, PARTIAL = Partially Contained Database, FULL = Fully Contained Database). By providing the containment status for the database's elements, you may figure out which objects or features need to be replaced, altered, etc.

Creating Table With Proper Functions

The pseudo-code 2 is used to create functions (default(), partial(), random(), etc.) for various attributes in the table so that data can be processed and stored quickly in the database.

Granting Permissions to the Users

Setting up the permissions plays a crucial role in accessing the masked values. The database administrator can decide

Pseudo Code 2 Creating the Table With Proper Functions

```
USE [database name]
GO
CREATE TABLE [table name]
(
        [FirstName] [nvarchar](n) MASKED WITH
        (FUNCTION = 'default()') NOT NULL,
        ..
        [Medicare Card No.] [varchar] (n) MASKED
        WITH (FUNCTION = 'partial(prefix,
"XXXXXXX", suffix)')
        NOT NULL,
        ..
        [Email] [nvarchar](n) MASKED WITH
        (FUNCTION = 'email()') NOT NULL
        ..
        [Mobile Number] [varchar](n) MASKED WITH
        (FUNCTION = 'random()') NOT NULL
        ..
)
GO
```

who can unmask the data. Any unauthorized user cannot access the masked information without proper permission.

Pseudo Code 3 Granting Permission to Users (Public View)

```
CREATE USER [<Username1>] WITHOUT LOGIN;
GRANT SELECT ON [<Table Name>] TO
[<Username1>];
```

Pseudo Code 4 Granting Unmask Permission to Users

```
GRANT UNMASK TO [<Username1>];
SELECT * FROM [<Table Name];
REVERT;
```

SQL allows the administrator to grant various types of permissions to the users. The SELECT permission allows the user to see the table data with masked data in the masked columns. WITHOUT LOGIN allows the user to view the data without login. The public view can be created using this. The users can see the original values of only those data columns that are publicly available. Pseudocode 3 provides SQL code for granting SELECT permission to a user, whereas pseudo code 4 provides SQL code for granting UNMASK permission to a user. UNMASK allows the users to retrieve data from the database that is masked and then unmask it based on required accessibility. Permissions granted to users can be removed using REVOKE function (i.e., REVOKE UNMASK TO [<Username>]).

a: ENCRYPTION FOR THE WHOLE DATABASE

Encrypting the whole database will make the data in the database unreadable without proper keys for decryption. To encrypt the dataset, this research will be used Transparent Database Encryption (TDE) method to encrypt the ''data at rest'' in the database [84]. Fig. 5 illustrates the process involved in the TDE method to encrypt the database [45], [69]. To apply TDE to the database various 'certificates' will be created and encrypted with a 'master key'. These certificates will be created for various employees in the organization that will be accessing the database. Certificates will be used to set user privileges and control mechanisms for people accessing the database. After creating the certificates, Database Encryption Keys (DEKs) will be created for various users of the system to encrypt the entire database so that only users with the correct credentials can access the data in the database. The issued certificates will be used to encrypt the DEKs, so those different users can access different attributes in the database (Example: Doctors require access to different attributes/columns than the nurses and vice versa). Finally, the encrypted DEKs will be used to encrypt the database [70].

b: 3-TIER ARCHITECTURE (.NET FRAMEWORK, SQL SERVER, DATABASE)

To implement the proposed procedure discussed in the above sections this research will use .NET Core entity framework 4.5 [85], Visual Studio 2015 [86], C# and Entity Framework Database First [87], Bootstrap and MS SQL Server 2008 [88], [89]. Fig. 9 illustrates the functional process involved between the user, server, and the database. This research utilizes a 3-tier architecture to illustrate the functional process logic, data access and storage methods, and user interfaces used for the system design of the PRMS. The architecture consists of a presentation layer, business and service layer, and data access layer. These layers are used to pass the HTTP requests and responses. The presentation layer is built on top of the ASP.NET WebAPI framework to provide user interface and access to the application services for the users in the form of ASP.NET web forms, web user controls, and service gateways. The business and service layer accepts the HTTP requests made by the user and forwards them to the ASP.NET CORE components through the ASP.NET CORE web server. The accepted HTTP request is passed through the middleware and filter pipelines to extract the controllers and actions for invocation. The data access layer is independent of the presentation and business layers. It consists of an SQL Server and access to resources. SQL Server is used to communicate with the database and consists of resources such as HTML generators. Using the data generated from the database and the HTML page generated, an HTTP response is sent to the web browser of the user using the same path followed by the HTTP request.

The information validation will be compatible with the features of the.NET core framework if any external resources are required for PRMS. To keep track of the services, a microservice application will be an option to use to allow the schedule, monitoring, and performance review of PRMS. Developing the proposed system with.NET Core application can support

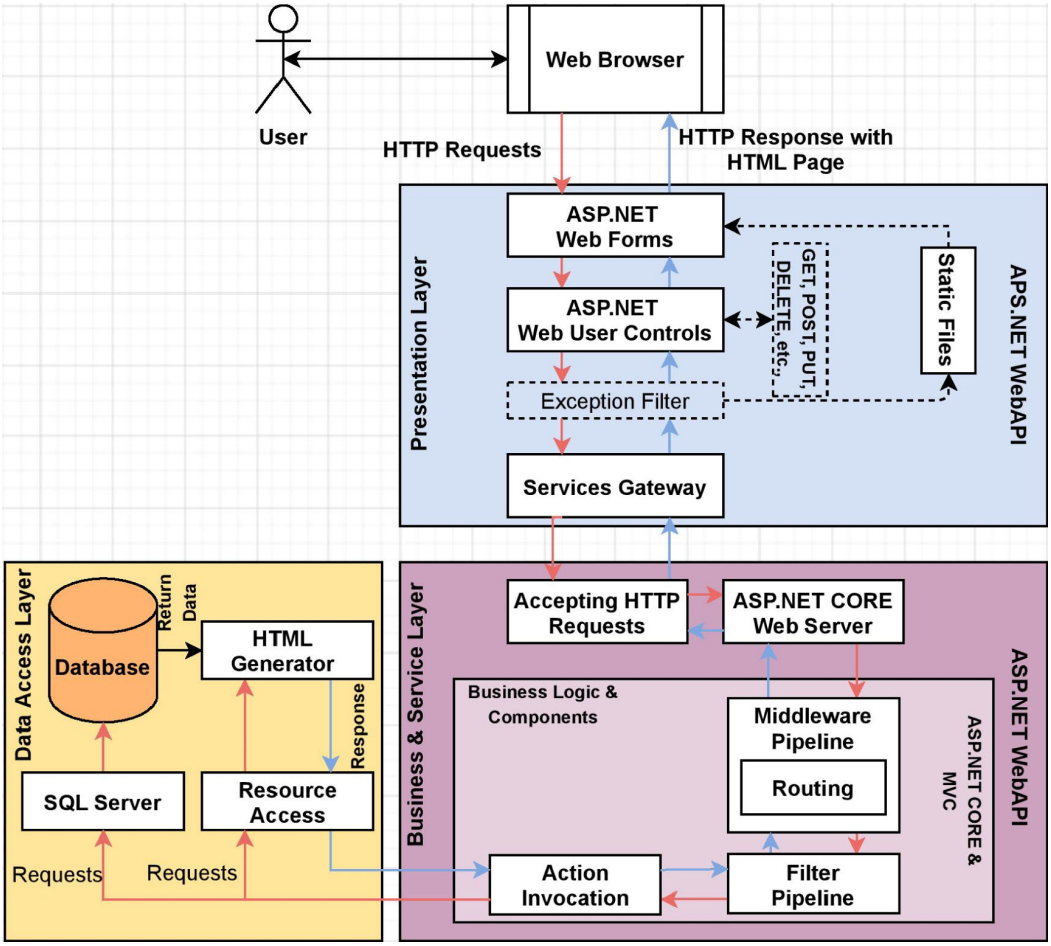

FIGURE 9. 3-Tier Architecture of Functional Process.

and improve health service features and external resources, e.g., additional applications, health check services, and middleware have capabilities to benefit from information validation. Besides, this framework provides a front-end application setup that will collect the personal information of healthcare system users [90]. Authentication and authorization are two key features of information protection that are built-in features within the.NET Core framework. Likewise, the user's credential validation approves the access to specific resources of PRMS that provides additional data protection by this framework [85], [91]

VI. CONCLUSION

The proposed framework is constructed with an accumulation of privacy by design fundamental principles, privacy design strategies, standards, and privacy impact assessment that deliver an extensive privacy-preserving environment in PRMS. The healthcare systems which employed the existing frameworks are behind to provide an entirely privacy-protected system, as desirable data privacy mechanisms are not properly consumed by the existing frameworks. A systematic activity is carried out in the proposed framework through three identified phases of system design named the planning phase, assessment phase, and implementation phase. The purpose of the proposed framework is to incorporate the necessary data privacy mechanisms in one place while collecting, managing, and storing personal information, thus the healthcare system can ensure maximum privacy to the personal data. Besides, the identified limitations that have been acknowledged in our work will be eliminated. The anticipated framework will ensure a sophisticated healthcare system incorporating privacy contexts compatible with the .NET Core framework. Implementing each of the proposed requirements will facilitate overcoming the gaps with complete privacy protection to achieve the desired outcome. The resulting framework will guarantee the integrity and confidentiality of PRMS while delivering high-level integration and allocation of personal data to decrease data breaches globally.

VII. FUTURE WORK

In our future endeavour, we intend to propose a PRMS by employing the proposed framework where patients' health data will be managed with maximum privacy assurance. The privacy by design framework produced an analysis of the core mechanisms in this study, which is immensely good,

but some degrees of risk are still there until we design the system to measure the potentiality of our framework. In this way we will have more chance and confidence to shield patients' information in the system, resulting in more consistent outcomes tailored to ensure the privacy of patients' health data. We will implement user testing to evaluate the potentiality of the proposed system. We will explore and analyse the privacy assurance of the users when interacting with the system [92], [93]. Moreover, we will incorporate necessary policies and mechanisms to assure data privacy for the distributed patient record management system and service delivery. This accumulation will provide scalability and flexibility of the PRMS in distributed environments where different healthcare organizations will collaborate for delivering perfect services by ensuring the privacy and security of the patients' sensitive data. Additionally, we plan to construct Security Incident Management (SIM) [94], [95] for information security management as this is one of the critical information security controls for organizations recommended by ISO/IEC 27001 [96], [97]. SIM will support the PRMS by notifying them of information security incidents or vulnerabilities. Besides, SIM will propose an immediate response to the vulnerabilities within a method that will protect affected users. Moreover, we will incorporate necessary policies, mechanisms to ensure patients' data privacy for the distributed patient record management system and service delivery.

REFERENCES

[1] A. Pika, M. T. Wynn, S. Budiono, A. H. M. ter Hofstede, W. M. P. van der Aalst, and H. A. Reijers, "Privacy-preserving process mining in healthcare," *Int. J. Environ. Res. Public Health*, vol. 17, no. 5, p. 1612, Mar. 2020, doi: 10.3390/ijerph17051612.

[2] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: Preserving security and privacy," *J. Big Data*, vol. 5, no. 1, pp. 1–18, Dec. 2018.

[3] V. Diamantopoulou, N. Argyropoulos, C. Kalloniatis, and S. Gritzalis, "Supporting the design of privacy-aware business processes via privacy process patterns," in *Proc. 11th Int. Conf. Res. Challenges Inf. Sci. (RCIS)*, May 2017, pp. 187–198.

[4] A. McLeod and D. Dolezel, "Cyber-analytics: Modeling factors associated with healthcare data breaches," *Decis. Support Syst.*, vol. 108, pp. 57–68, Apr. 2018.

[5] R. Taplin, *Managing Cyber Risk in the Financial Sector: Lessons From Asia, Europe and the USA*. Evanston, IL, USA: Routledge, 2016.

[6] F. H. Semantha, S. Azam, K. C. Yeo, and B. Shanmugam, "A systematic literature review on privacy by design in the healthcare sector," *Electronics*, vol. 9, no. 3, p. 452, Mar. 2020.

[7] OAIC. *Notifiable Data Breaches Report, Australian Government—Office of the Australian Information Commissioner*. Accessed: Jan. 25, 2021. [Online]. Available: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2020/

[8] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, and R. A. Khan, "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, p. 133, May 2020, doi: 10.3390/healthcare8020133.

[9] N. Whigham. *Health Sector Tops the List as Australians Hit by 300 Data Breaches Since February*. News.com.au. Accessed: Nov. 20, 2020. [Online]. Available: https://www.news.com.au/technology/online/hacking/health-sector-tops-the-list-as-australians-hit-by-300-data-breaches-since-february/news-story/5e95c47694418ad072bf34d872e22124

[10] H. Weisbaum. *The Total Cost of a Data Breach—Including Lost Business—Keeps Growing*. NBC News. Accessed: Mar. 15, 2021. [Online]. Available: https://www.nbcnews.com/business/consumer/total-cost-data-breach-including-lost-business-keeps-growing-n895826

[11] A. Cavoukian, "Privacy by design [leading edge]," *IEEE Technol. Soc. Mag.*, vol. 31, no. 4, pp. 18–19, Dec. 2012.

[12] J. Kirk. *Australia's Biggest Breach Offender: Healthcare Sector*. Bank Info Security. Accessed: Nov. 30, 2020. [Online]. Available: https://www.bankinfosecurity.com/australian-health-care-sector-reports-most-breaches-a-11267

[13] T. Micro. *Data Breaches 101: How They Happen, What Gets Stolen, and Where it all Goes*. Trend Micro. Accessed: Mar. 3, 2021. [Online]. Available: https://www.trendmicro.com/vinfo/ie/security/news/cyber-attacks/data-breach-101

[14] K. E. Emam and F. K. Dankar, "Protecting privacy using k-anonymity," *J. Amer. Med. Informat. Assoc.*, vol. 15, no. 5, pp. 627–637, 2008.

[15] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management—A consolidated proposal for terminology," Version v0.31, TU Dresden, Dresden, Germany, Tech. Rep., Feb. 2008.

[16] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019, doi: 10.3390/s19020326.

[17] J. Yang, M. M. H. Onik, N.-Y. Lee, M. Ahmed, and C.-S. Kim, "Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making," *Appl. Sci.*, vol. 9, no. 7, p. 1370, Apr. 2019.

[18] A. Iyengar, A. Kundu, and G. Pallis, "Healthcare informatics and privacy," *IEEE Internet Comput.*, vol. 22, no. 2, pp. 29–31, Mar. 2018.

[19] H. K. Patil and R. Seshadri, "Big data security and privacy issues in healthcare," in *Proc. IEEE Int. Congr. Big Data*, Jun. 2014, pp. 762–765.

[20] O. Adebisi, D. Oladosu, O. Busari, and Y. Oyewola, "Design and implementation of hospital management system," *Int. J. Eng. Innov. Technol.*, vol. 5, no. 1, pp. 1–5, 2015.

[21] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163–168, Feb. 2018.

[22] L. Bari and D. P. O'Neill, "Rethinking patient data privacy in the era of digital health," Health Aff Blog, Washington, DC, USA, Tech. Rep., 2019.

[23] A. Roehrs, C. A. da Costa, R. D. R. Righi, and K. S. F. de Oliveira, "Personal health records: A systematic literature review," *J. Med. Internet Res.*, vol. 19, no. 1, p. e13, Jan. 2017.

[24] D. A. Salleh. *Information Systems in Health Care*. Accessed: Feb. 17, 2021. [Online]. Available: https://drdollah.com/hospital-information-system-his/

[25] I. G. Cohen and M. M. Mello, "HIPAA and protecting health information in the 21st century," *Jama*, vol. 320, no. 3, pp. 231–232, 2018.

[26] S. Sharma, *Data Privacy and GDPR Handbook*. Hoboken, NJ, USA: Wiley, 2019.

[27] J. S. Baik, "Data privacy against innovation or against discrimination?: The case of the California consumer privacy act (CCPA)," *Telematics Informat.*, vol. 52, Sep. 2020, Art. no. 101431.

[28] C. Barrett, "Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection?" *Scitech Lawyer*, vol. 15, no. 3, pp. 24–29, 2019.

[29] M. A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab, M. A. Orgun, W. Iqbal, I. Rashid, and A. Yaseen, "Privacy preservation in e-healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2017.

[30] N. Thiranant, M. Sain, and H. J. Lee, "A design of security framework for data privacy in e-health system using web service," in *Proc. 16th Int. Conf. Adv. Commun. Technol.*, Feb. 2014, pp. 40–43.

[31] A. Shenoy and J. M. Appel, "Safeguarding confidentiality in electronic health records," *Cambridge Quart. Healthcare Ethics*, vol. 26, no. 2, pp. 337–341, Apr. 2017.

[32] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informat. J.*, vol. 22, no. 2, pp. 177–183, Jul. 2021.

[33] J. George and T. Bhila, "Security, confidentiality and privacy in health of healthcare data," *Int. J. Trend Sci. Res. Develop.*, vol. 3, no. 4, pp. 373–377, Jun. 2019.

[34] OVIC. (2019). *Privacy by Design: Effective Privacy Management in the Victorian Public Sector*. Office of the Victorian Information Commissioner. [Online]. Available: https://ovic.vic.gov.au/wp-content/uploads/2018/07/Privacy-by-Design-Background-Paper.pdf

[35] A. Cavoukian, "Operationalizing privacy by design: A guide to implementing strong privacy practices," Inf. Privacy Commissioner Ontario, ON, Canada, Tech. Rep., 2012.
[36] A. Cavoukian, "Understanding how to implement privacy by design, one step at a time," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 78–82, Mar. 2020.
[37] S. Moncrieff, S. Venkatesh, and G. West, "A framework for the design of privacy preserving pervasive healthcare," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jun. 2009, pp. 1696–1699.
[38] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in *Proc. 7th Int. Conf. Body Area Netw.*, 2012, pp. 269–275.
[39] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy preserving authentication and access control scheme for pervasive computing environments," *IEEE Trans. Veh. Technol.*, vol. 55, no. 4, pp. 1373–1384, Jul. 2006.
[40] A. Kung, A. C. Garcia, N. N. McDonnell, I. Kroener, D. Le Métayer, and C. Troncoso, "PReparing industry to privacy-by-design by supporting its application in REsearch," Eur. Commission, Brussels, Belgium, Tech. Rep., 2014.
[41] O. Drozd, "Privacy pattern catalogue: A tool for integrating privacy principles of ISO/IEC 29100 into the software development process," in *Proc. Int. Summer School Privacy Identity Manage. (IFIP)*. Cham, Switzerland: Springer, 2015, pp. 129–140.
[42] N. Notario, A. Crespo, Y.-S. Martin, J. M. Del Alamo, D. L. Metayer, T. Antignac, A. Kung, I. Kroener, and D. Wright, "PRIPARE: Integrating privacy best practices into a privacy engineering methodology," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 151–158.
[43] N. M. Shrestha, A. Alsadoon, P. W. C. Prasad, L. Hourany, and A. Elchouemi, "Enhanced e-health framework for security and privacy in healthcare system," in *Proc. 6th Int. Conf. Digit. Inf. Process. Commun. (ICDIPC)*, Apr. 2016, pp. 75–79.
[44] P. Mehndiratta, S. Sachdeva, and S. Kulshrestha, "A model of privacy and security for electronic health records," in *Proc. Int. Workshop Databases Netw. Inf. Syst.* Cham, Switzerland: Springer, 2014, pp. 202–213.
[45] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," *Int. J. Inf. Secur.*, vol. 14, no. 6, pp. 487–497, Nov. 2015.
[46] A. Samydurai, K. Revathi, P. Prema, D. Arulmozhiarasi, J. Jency, and S. Hemapriya, "Secured health care information exchange on cloud using attribute based encryption," in *Proc. 3rd Int. Conf. Signal Process., Commun. Netw. (ICSCN)*, Mar. 2015, pp. 1–5.
[47] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Privacy-by-design framework for assessing Internet of Things applications and platforms," in *Proc. 6th Int. Conf. Internet Things*, Nov. 2016, pp. 83–92.
[48] M. N. Hassan, M. R. Islam, F. Faisal, F. H. Semantha, A. H. Siddique, and M. Hasan, "An IoT based environment monitoring system," in *Proc. 3rd Int. Conf. Intell. Sustain. Syst. (ICISS)*, 2020, pp. 1119–1124.
[49] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.
[50] N. Foukia, D. Billard, and E. Solana, "PISCES: A framework for privacy by design in IoT," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Dec. 2016, pp. 706–713.
[51] R. H. Weber, "Internet of Things-new security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.
[52] O. Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. Copenhagen, Denmark: River, 2013.
[53] B. Chung, J. Kim, and Y. Jeon, "On-demand security configuration for IoT devices," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2016, pp. 1082–1084.
[54] B. Bagheri, M. Rezapoor, and J. Lee, "A unified data security framework for federated prognostics and health management in smart manufacturing," *Manuf. Lett.*, vol. 24, pp. 136–139, Apr. 2020.
[55] M. E. Morales-Trujillo and G. A. Garcia-Mireles, "Extending ISO/IEC 29110 basic profile with privacy-by-design approach: A case study in the health care sector," in *Proc. 11th Int. Conf. Quality Inf. Commun. Technol. (QUATIC)*, Sep. 2018, pp. 56–64.
[56] A. Cavoukian, "Privacy by design: The 7 foundational principles," *Inf. Privacy Commissioner Ontario, Canada*, vol. 5, p. 12, 2009.
[57] OVIC. *Privacy Impact Assessment Guide*. OVIC-Office of the Victorian Information Commissioner. Accessed: Jan. 10, 2021. [Online]. Available: https://ovic.vic.gov.au/privacy/for-agencies/privacy-impact-assessments/
[58] D. Gu, S. Deng, Q. Zheng, C. Liang, and J. Wu, "Impacts of case-based health knowledge system in hospital management: The mediating role of group effectiveness," *Inf. Manage.*, vol. 56, no. 8, Dec. 2019, Art. no. 103162.
[59] P. W. Handayani, A. N. Hidayanto, A. A. Pinem, I. C. Hapsari, P. I. Sandhyaduhita, and I. Budi, "Acceptance model of a hospital information system," *Int. J. Med. Informat.*, vol. 99, pp. 11–28, Mar. 2017.
[60] J. Zhang and W. Xu, "Web service-based healthcare information system (WSHIS): A case study for system interoperability concern in healthcare field," in *Proc. Int. Conf. Biomed. Pharmaceutical Eng.*, 2006, pp. 588–594.
[61] E. Freund, "ISO/IEC 15288:2002, systems engineering-system life-cycle processes," *Softw. Qual. Prof.*, vol. 8, no. 1, p. 42, 2005.
[62] R. Xue, C. Baron, and P. Esteban, "Optimising product development in industry by alignment of the ISO/IEC 15288 systems engineering standard and the PMBoK guide," *Int. J. Prod. Dev.*, vol. 22, no. 1, pp. 65–80, 2017.
[63] L. Yang, K. Cormican, and M. Yu, "An ontology model for systems engineering derived from ISO/IEC/IEEE 15288:2015: Systems and software engineering-system life cycle processes," *World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng*, vol. 11, no. 1, pp. 1–7, 2016.
[64] A. Cavoukian, A. Fisher, S. Killen, and D. A. Hoffman, "Remote home health care technologies: how to ensure privacy? build it in: Privacy by design," *Identity Inf. Soc.*, vol. 3, no. 2, pp. 363–378, Aug. 2010.
[65] J.-H. Hoepman, "Privacy design strategies," in *IFIP Int. Inf. Secur. Conf.* Berlin, Germany: Springer, 2014, pp. 446–459.
[66] N. Li, W. Qardaji, and D. Su, "On sampling, anonymization, and differential privacy or, k-anonymization meets differential privacy," in *Proc. 7th ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*, 2012, pp. 32–33.
[67] F. De Meyer, G. De Moor, and L. Reed-Fourquet, "Privacy protection through pseudonymisation in eHealth," *Stud. Health Technol. Informat.*, vol. 141, pp. 111–118, 2008.
[68] T. Neubauer and J. Heurix, "A methodology for the pseudonymization of medical data," *Int. J. Med. Inform.*, vol. 80, no. 3, pp. 190–204, 2011.
[69] Q. Huang and H. Li, "An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks," *Inf. Sci.*, vol. 403, pp. 1–14, Sep. 2017.
[70] L. Xu, C. Xu, J. K. Liu, C. Zuo, and P. Zhang, "Building a dynamic searchable encrypted medical database for multi-client," *Inf. Sci.*, vol. 527, pp. 394–405, Jul. 2020.
[71] G. Dhand and S. S. Tyagi, "Data aggregation techniques in WSN: Survey," *Proc. Comput. Sci.*, vol. 92, pp. 378–384, Jan. 2016.
[72] S. A. Yasin and P. P. Rao, "A framework for decision making and quality improvement by data aggregation techniques on private hospitals data," *ARPN J. Eng. Appl. Sci.*, vol. 13, no. 14, pp. 4337–4345, 2018.
[73] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronic medical records," in *Proc. ACM Workshop Cloud Comput. Secur. (CCSW)*, 2009, pp. 103–114.
[74] OAIC. *Guide to Undertaking Privacy Impact Assessments, Australian Government—Office of the Australian Information Commissioner*. Accessed: Dec. 28, 2020. [Online]. Available: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/
[75] A. S. Ahmadian, D. Strüber, V. Riediger, and J. Jürjens, "Supporting privacy impact assessment by model-based privacy analysis," in *Proc. 33rd Annu. ACM Symp. Appl. Comput.*, Apr. 2018, pp. 1467–1474.
[76] K. Vemou and M. Karyda, "An evaluation framework for privacy impact assessment methods," in *Proc. MCIS*, 2018, p. 5.
[77] OAIC. *Australian Privacy Principles*. Australian Government—Office of the Australian Information Commissioner. Accessed: Jul. 5, 2021. [Online]. Available: https://www.oaic.gov.au/privacy/australian-privacy-principles/
[78] D. A. Tamburri, "Design principles for the general data protection regulation (GDPR): A formal concept analysis and its evaluation," *Inf. Syst.*, vol. 91, Jul. 2020, Art. no. 101469.
[79] NSW-Health. *Client Registration Policy*. Ministry of Health. NSW. Accessed: Mar. 20, 2021. [Online]. Available: https://www1.health.nsw.gov.au/pds/ActivePDSDocuments/PD2007_094.pdf
[80] A. I. Baranchikov, A. Y. Gromov, V. S. Gurov, N. N. Grinchenko, and S. I. Babaev, "The technique of dynamic data masking in information systems," in *Proc. 5th Medit. Conf. Embedded Comput. (MECO)*, Jun. 2016, pp. 473–476.
[81] S. Mansfield-Devine, "Masking sensitive data," *Netw. Secur.*, vol. 2014, no. 10, pp. 17–20, Oct. 2014.

[82] Y. Ding and K. Klein, "Model-driven application-level encryption for the privacy of E-health data," in *Proc. Int. Conf. Availability, Rel. Secur.*, Feb. 2010, pp. 341–346.
[83] Microsoft. *Dynamic Data Masking*. Microsoft-SQL Docs. Accessed: Jun. 15, 2021. [Online]. Available: https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-ver15
[84] V. Sidorov and W. K. Ng, "Transparent data encryption for data-in-use and data-at-rest in a cloud-based database-as-a-service solution," in *Proc. IEEE World Congr. Services*, Jun. 2015, pp. 221–228.
[85] H. Schwichtenberg, "Introducing entity framework core," in *Modern Data Access With Entity Framework Core*. Berkeley, CA, USA: Springer, 2018, pp. 1–14.
[86] S. Amann, S. Proksch, S. Nadi, and M. Mezini, "A study of visual studio usage in practice," in *Proc. IEEE 23rd Int. Conf. Softw. Anal., Evol., Reeng. (SANER)*, vol. 1, Mar. 2016, pp. 124–134.
[87] K. Hule and Z. Shaikh, "Object relational mapping tool for C#.NET framework," *Int. J. Innov. Res. Sci., Eng. Technol.*, vol. 3, no. 8, pp. 15185–15191, Aug. 2014.
[88] Z. Aljazzaf, "Bootstrapping quality of web services," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 27, no. 3, pp. 323–333, Jul. 2015.
[89] H. S. Goswami, *Microsoft SQL Server 2008 High Availability*. Birmingham, U.K.: Packt, 2011.
[90] A. H. Thary Al-Ghrairi, A. A. Mohammed, and H. M. Saeed, "An application of web-based E-healthcare management system using ASP.Net," *Webology*, vol. 18, no. 1, pp. 285–298, Apr. 2021.
[91] A. Poudel, "A comparative study of project management system web applications built on ASP.Net core and laravel MVC frameworks," St. Cloud State Univ.-Repository St. Cloud State, St. Cloud, MN, USA, Tech. Rep., 2018.
[92] J. Abelson, K. Li, G. Wilson, K. Shields, C. Schneider, and S. Boesveld, "Supporting quality public and patient engagement in health system organizations: Development and usability testing of the public and patient engagement evaluation tool," *Health Expectations*, vol. 19, no. 4, pp. 817–827, 2016.
[93] I. Maramba, A. Chatterjee, and C. Newman, "Methods of usability testing in the development of eHealth applications: A scoping review," *Int. J. Med. Informat.*, vol. 126, pp. 95–104, Jun. 2019.
[94] M. Evans, Y. He, C. Luo, I. Yevseyeva, H. Janicke, E. Zamani, and L. A. Maglaras, "Real-time information security incident management: A case study using the IS-CHEC technique," *IEEE Access*, vol. 7, pp. 142147–142175, 2019.
[95] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Comput. Secur.*, vol. 45, pp. 42–57, Sep. 2014.
[96] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda," *TQM J.*, vol. 33, no. 7, pp. 76–105, Dec. 2021.
[97] M. Mirtsch, J. Kinne, and K. Blind, "Exploring the adoption of the international information security management system standard ISO/IEC 27001: A web mining-based analysis," *IEEE Trans. Eng. Manag.*, vol. 68, no. 1, pp. 87–100, Feb. 2021.

FARIDA HABIB SEMANTHA is currently a Ph.D. Researcher with the College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT, Australia. She has considerable experience working as an IT Professional with the Northern Territory Government, Australia. Her research interests include data privacy, cybersecurity, digital forensics, and ICT governance. She is currently researching privacy by design in the healthcare sector.

SAMI AZAM (Member, IEEE) is currently a Leading Researcher and a Senior Lecturer with the College of Engineering and IT, Charles Darwin University, Casuarina, NT, Australia. He has a number of publications in peer-reviewed journals and international conference proceedings. He is also actively involved in the research fields relating to computer vision, signal processing, artificial intelligence, and biomedical engineering.

BHARANIDHARAN SHANMUGAM is currently a Research-Intensive Lecturer with the College of Engineering and IT, Charles Darwin University, Australia. He has many publications in several journals and conference proceedings. His main research interest includes the field of cybersecurity.

KHENG CHER YEO is currently a Senior Lecturer in information technology with the College of Engineering, IT and Environment, Australia. He is passionate about teaching and has taught hardware, mathematics, networking, software engineering, and project management. He is also active in research and his research interests include the areas of intelligent signal processing and control, networking, and security and app development.

ABHIJITH REDDY BEERAVOLU is currently pursuing the M.S. degree in information systems and data science with Charles Darwin University, Casuarina, NT, Australia. He is also a Computer Science Enthusiast who is interested in anything related to computers. His research interests include reading books on History and making comparisons with the current world, to make sense of the reality and its progression. He is also interested in reading and analyzing information related to cognitive and behavioral psychology and trying to integrate them into various technological ideas.