# A FRAMEWORK TO EVALUATE CITIZENS' DATA PRIVACY IN HEALTH CARE SYSTEMS AND TRACING APPS USED DURING COVID-19


By

Shoaib Ul Hassan

Submitted to the Faculty of Department of Information Security
Military College of Signals, National University of Sciences and Technology,
Islamabad in partial fulfillment of the requirements for the degree of MS in
Information Security

FEBRUARY 2023

# THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Mr. Shoaib Ul Hassan**, Registration No. **00000328000**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfilment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor **Prof Dr. Haider Abbas, PhD**

Date: _____

Signature (HOD): _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

# A FRAMEWORK TO EVALUATE CITIZENS' DATA PRIVACY IN HEALTH CARE SYSTEMS AND TRACING APPS USED DURING COVID-19

Author
Shoaib Ul Hassan
Registration Number
00000328000

A thesis submitted in partial fulfillment of the requirements for the degree of
MS Information Security

Thesis Supervisor:
Prof Dr Haider Abbas, PhD

Thesis Supervisor's Signature: _____

Department of Information Security
Military College of Signals
National University of Sciences and Technology,
Islamabad
February 2023

# CERTIFICATE OF CORRECTNESS AND APPROVAL

It is certified that work contained in this thesis "**A Framework to Evaluate Citizens' Data Privacy in Health Care Systems and Tracing Apps used during COVID-19**", was carried out by Shoaib Ul Hassan under the supervision of Prof Dr. Haider Abbas, for partial fulfilment of Degree of Master of Information Security, is correct and approved. This thesis has been checked for Plagiarism. Turnitin report endorsed by Supervisor is attached.

Approved by

_____

(Prof Dr. Haider Abbas, PhD), HOD

Thesis Supervisor

Military College of Signals (MCS)

Dated: _____February 2023

# DECLARATION

I certify that this research work titled "**A Framework to Evaluate Citizens' Data Privacy in Health Care Systems and Tracing Apps used during COVID-19**" is my own work. No portion of this work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere. The material that has been used from other sources has been properly acknowledged / referred.

_____

Signature of Student

Shoaib Ul Hassan

00000328000

*This page is left intentionally blank.*

# ABSTRACT

Healthcare industry has seen rapid growth worldwide in recent years and many advance countries have shifted from manual records to computerised health care systems. Automated healthcare systems, mobile health apps, wearable gadgetries, and various types of sensors collect and stores individuals' data in electronic form. These steps have revolutionised the healthcare industry, however, raised serious data privacy concerns globally being privacy the fundamental human right. As health records are extremely valuable and are always subject to data breaches. To address this, countries all over the world are taking appropriate measures and tightening their data protection laws. In this research, initially health systems and use of medical data is discussed along with related privacy and security challenges. Then, the data privacy during pandemic and various data privacy preserving techniques have been presented. Then, popular data privacy legislations of key countries like HIPPA (US), GDPR (EU), PIPEDA (Canada) and PIPL (PRC) have been discussed along with regulations which cover citizen privacy in Pakistan. Based on best principles and practices of popular regulations, a framework has been proposed to evaluate citizens data privacy in Health care systems and Apps with Key Performance Indicators (KPIs). Finally, a case study has been presented in which tracing apps used to collect data during COVID-19 were analysed in detail and evaluated through proposed framework. At the end recommendations are made basing on privacy concerns found as result of evaluation.

# COPYRIGHT STATEMENT

# DEDICATION

**“**Are those equals, those who know and those who do not know.**”**

**(Chapter 39: Surah Az-'Zumar: Ayat 09)**

To my family and other loved ones,

To anyone who has shown me friendship and kindness during my research work,

&

To those who inspired me to pursue my dreams

# ACKNOWLEDGEMENT

First and foremost, I would like to praise and thank Allah Almighty for giving me strength to keep going on with this thesis, irrespective of job commitments and many other challenges.

I am indebted to my supervisor Professor Dr. Haider Abbas and co-supervisor Assistant Professor Dr. Shahzaib Tahir who supervised the thesis / research in a very encouraging and helpful manner. Similarly, I am grateful to my committee members Engr Sohaib Khan Niazi and Assistant Professor Dr. Imran Makhdoom who have always guided me with their profound and valuable support that has helped me in achieving my research aims.

Of course, I am also forever grateful to my family and kids, who have put up with my moaning and many weekends of work. I love you and promise I will cut down on weekend work to spend some more time with you!

Finally, I would like to express my appreciation to all the people who have provided valuable support to my study and whose names I couldn't bring to memory.

*This page is left intentionally blank.*

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# ACRONYMS

| | |
|---|---|
| Application Programming Interface | API |
| Clinical Document Architecture | CDA |
| Clinical Decision Support System | CDSS |
| Coronavirus Disease of 2019 | COVID-19 |
| Decentralized Privacy-Preserving Proximity Tracing | DP3T |
| Decision Support System | DSS |
| Electronic Health Record | EHR |
| European Union | EU |
| Fast Healthcare Interoperability Resources | FHIR |
| General Data Protection Regulation | GDPR |
| Hospital Document Architecture | HDA |
| Health Insurance Portability and Accountability Act | HIPAA |
| Health Information Technology for Economic and Clinical Health | HITECH |
| Health and Human Services | HHS |
| Institute of Electrical and Electronics Engineers | IEEE |
| Key Performance Indicators | KPIs |
| Ministry of Information Technology and Telecommunication | MoITT |
| Ministry of National Health Services Regulations and Coordination | MoNHSR&C |
| Micro Smart Lock Down | MSLD |
| National Database and Registration Authority | NADRA |
| National Command and Operation Center | NCOC |
| Non-Disclosure Agreement | NDA |
| National Institutes of Health | NIH |
| National Immunization Management System | NIMS |
| National Institute of Standards and Technology | NIST |
| National Information Technology Board | NITB |
| Prevention of Electronic Crimes Act | PECA |
| Personal Information Protection and Electronic Documents Act | PIPEDA |
| Smart Lock Down | SLD |
| Track, Trace and Quarantine | TTQ |
| United Nations General Assembly | UNGA |
| World Health Organization | WHO |

# *Chapter 1*

## INTRODUCTION

*"It's hard to beat a person who never gives up"*

*-Babe Ruth*

### 1.1 Overview

The revolution in IT industry has increased the importance of data manifold and therefore its being considered as Gold or as important as an Oil reservoir. However, its improper management has led to pilferage, misuse and resultantly raised citizen's privacy issues worldwide. To control this issue and enable citizens for exercising their rights, technologically advanced countries came up with strict data protection laws e.g., Health Insurance Portability and Accountability Act (HIPPA) [1] in United States and General Data Protection Regulation (GDPR) [2] in EU. With growing number of cyber-attacks, data leakage cases and privacy issues, Government of Pakistan has also issued its 1st National Cyber Security Policy in July 2021. One of the important objectives of National policy includes "To protect the online privacy of the citizens by provisioning the required support and system..."[3]. In line with National Policy, Ministry of National Health Services Regulations and Coordination has also issued National Digital Health Framework of Pakistan 2022-2030 in partnership with Provincial Health Departments which aims for digital health platforms with a view to promote the protection of health systems against cyber-attacks including fraud, exploitation, and monetization of health data [4]. In 2021, MoITT of Pakistan initiated a draft of Personal Data Protection Bill" due to increase used to technological tools during COIVD-19 [5] .Citizen's data warrants appropriate privacy, however, at the same time it is essentially required for secondary use and research purposes specially in the field of health to handle unprecedented situations like pandemics. In this regard, HIPPA, GDPR, PIPEDA, PIPL and WHO regulations also show flexibility for the common good [6].

To control the disease spread, various technological solutions were adopted worldwide including use of multipurpose tracing apps to monitor patients 'movement, enforcing quarantine, identity cluster with high disease areas and generating alerts. Although the apps played an important part in limiting the virus spread, however, due to data collection without

consent raised privacy concerns like increased surveillance, taxation, identification etc in various parts of the world.

## 1.2 Motivation

The world has just faced and is still suffering from a pandemic named COVID-19. To handle the destructive disease, health experts of various countries collected and used citizens' data in various forms for necessary assessments. e.g., local and international disease trends, disease variants, mortality rates, efficacy of various vaccines in various zones and age groups, disease re-infection rate etc. As proactive approach, systems like Track, Trace, and Quarantine (TTQ) for the infected and potentially infected patients were adopted by gathering citizens' data after taking necessary consent. With geo tagged data of highly infected areas, hotspot clusters were created which helped in imposing Smart Lock Downs (SLDs) and even Micro Smart Lock Downs (MSLDs) to street level [7]. IT apps were also used to facilitate the passengers and efficient management of the inbound travel to lower the risk of imported disease [8].

During COVID-19 personal data related to citizens was collected, stored, and processed to mitigate the risk of pandemic under the relations provided by privacy laws as it was required and used for the common good. However, the government and heath care authorities must ensure that only minimum and required data is collected and processed. In such situations, it should be ensured by government and health authorities that citizens personal data is only used for required purposes and not shared or used for secondary purposes without justifiable reason. IT solutions used during such situations require comprehensive privacy evaluation before deployment at large scale to minimize the risk of privacy breaches.

## 1.3 Problem Statement

The pandemic named COVID-19 caught everyone with surprise, especially healthcare authorities who were not prepared to handle it through traditional healthcare systems. To control the fast spread of virus, various technological approaches were adopted by governments and healthcare authorities including tracing apps. The global legislative structures have special clauses and provide relaxation in collection and processing of personal data during special conditions without the consent of person. However, lack of transparency and explicit policies raised privacy concerns in public. Due to the existing breach incidents and challenges of electronic health records, people were concerned with

collection, storage, and processing of their data through hastily developed apps. Considering the public privacy concerns vis-à-vis benefits accrued from such tools, a dire need is felt to evaluate such systems, apps and tools used to monitor and track patients during pandemic in the light of popular regulations followed in various regions.

### 1.4 Research Objectives

The main objectives of thesis are:

a. Discuss privacy issues associated with Health Systems, EHR and its secondary use.
b. Analyze the global legislative structures under which citizens' data processing is performed.
c. Analyzing contact tracing apps developed and used worldwide for tracking covid patients along with data privacy concerns.
d. Propose framework to evaluate privacy concerns of tracing apps.

### 1.5 Contribution

This thesis will contribute in the following ways:

a. In this study EHR has been discussed along with its numerous secondary uses wrt to data privacy.
b. This thesis has systematically analysed global legislative structures including GDPR, HIPAA, PIPEDA and PIPL and linked their applicability during covid and various technological solutions. Moreover, privacy related regulations and frameworks published in Pakistan have also been discussed.
c. Comprehensive analysis of tracing apps used worldwide and their serious privacy issues have been discussed in detail with respect to privacy of individual personal data.
d. Basing on important privacy principles and practices of popular regulations, a framework has been proposed which will help to evaluate tracing apps privacy compliance wrt citizens data.

## 1.6 Thesis Outline

The basic outline of the thesis is:

Chapter 1: The study aims, objectives, motivation, research issues, and contributions are all presented in Chapter 1. The introduction describes the motives for performing this research, as well as why it is important.

Chapter 2: This chapter presents healthcare systems, evolution of EHR, healthcare system of Pakistan, data privacy and security challenges including privacy during COVID-19.

Chapter 3: This chapter explains few important global data privacy regulations including HIPPA, GDPR, PIPEDA and PIPL which are being used by technologically advanced countries and also covers the privacy landscape of Pakistan.

Chapter 4: In this chapter, several privacy-preserving techniques are presented.

Chapter 5: To evaluate the privacy compliance of apps, a framework has been proposed inferred from the best principles of best global regulations.

Chapter 6: In this chapter analysis of apps has been carried out which were used during COVID-19. The analysis includes types of models, developing technologies, techniques, app features and data privacy concerns. At the end privacy of Tracing Apps has been evaluated through proposed framework as test and results have been attained in the form privacy concerns ranging from low to high levels.

Chapter 7: This chapter incorporates the thesis's main conclusions as well as future research directions.

# *Chapter 2*

## LITERATURE REVIEW

Citizen's data is sensitive information and dealt with extreme care in most of the world regions especially in the technologically advanced countries as it can lead to financial losses, create social and health issues in case of leakage [9]. In health care systems, especially during the pandemic, massive amount of citizens' data including clinical and personal details was generated daily and shared with various stakeholders for various purposes particularly research [10]. This data enabled healthcare institutions to ascertain disease trends in different aspects including age brackets, gender based etc. The record was collected and shared with consent and sometime without taking consent. The citizens data, healthcare systems and its usage are so important that regulations are required to ensure privacy and exercise discipline. To address the citizen's data privacy issues, there are many regulations which not only guide but also apply to ensure safety of private and sensitive information. HIPAA and the GDPR are amongst the well-known and considered as most comprehensive regulations [11]. The relaxing clauses of world regulations and new amendments during pandemic provided opportunity to governments and health official to collect and process personal data without the user consent which raised serious privacy concerns worldwide.

The objective of this literature research is to discuss citizens data privacy in health systems, examine popular international privacy regulations, privacy preserving techniques and propose privacy evaluation framework to evaluate privacy compliance of tracing apps and health care systems used during COVID-19.

### 2.1 Health Systems

It is a collection of resources including workforce, infrastructure, facilities, and technology and resource put in place to provide healthcare services to society [12].

#### 2.1.1 Health Information System (HIS)

Apps which collect, store, and process data related to health are considered as health information systems. Since the 1960s, computer-based healthcare information systems are being utilized. During the period between 1960-1980, scope of apps was departmental like

laboratory management [13]. Later it moved to patient centric data processing. Currently, the focus is on maintaining electronic health records including provision of variety of services related to health. These include management of resources finance, and departments [14].

### 2.1.2 Medical Record

It's the record of treatment maintained manually and utilized for further visits and stored in cabinets in an organized way. This method is still practiced in various parts of the world where technology has not grown much. However, issues like record tracing, redundancy, compilation time, misplacement, and forgery lead to evolution of health information systems and collection, storage and processing and sharing of health records through IT systems. It is the foundation of electronic medical records [15].

### 2.1.3 Electronic Health Record (EHR)

Mostly, in advanced countries, manual paper-based medical records have been digitized. Computerized records having patients' complete information and their treatment record is called EHR. Murphy, Waters and Amotegacul defined EHR as: -

> *"... any information relating to the past, present, or future physical / mental health or condition of an individual which resides in an electronic system(s) used to capture, storage, retrieve, link, and manipulate data for the primarily purpose of providing health care and related* services."[16]

As per the definition, ownership of data is not determinate, and purpose has not been limited thus can be used for multiple purposes. As per International Standard Organization (ISO), EHR can be defined as under: -

> *"Electronic Health Record is a repository of information regarding the health status of a subject of care in a computer processable form, storage and transmitted securely, and accessible by multiple authorized users. It has a standardized or commonly agreed information model, which is independent of the EHR system. Its primary purpose is the support of continuing, efficient and quality integrated health care and it contains information, which is retrospective, concurrent, and prospective."*[17]

In above mentioned definition, access control and secure transmission of health information is implied.

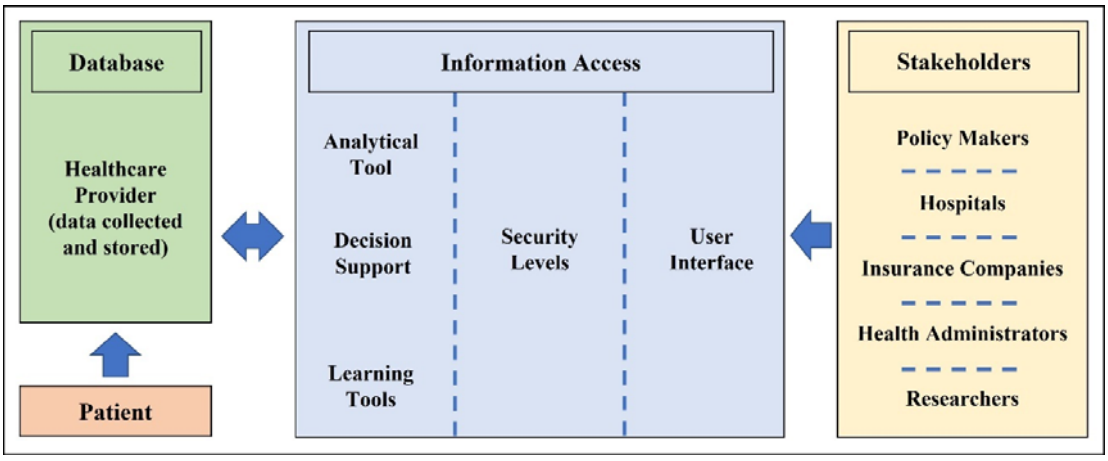


Figure 2.1 A conceptual overview of EHR Systems

Clinical data stored as EHR can be easily shared amongst numerous stakeholders [11] like hospitals (primary, secondary, tertiary care hospitals), labs, pharmacies, dispensaries as per requirement for effective and efficient utilization (described in Figure 2.1) [18]. Following advantages can be gained from EHR as compared to manual health records:

a. Comprehensive medical data of patients can be stored, structured and in encrypted form [19].
b. Live and updated data on dashboards through decision support systems (DSS) can facilitate decision making at multiple tiers and overall improve healthcare systems [20].
c. Health forecasts, resource planning, requirement gathering and its distribution, clinical studies, medical insurances, clinical auditing [21]Disease surveillance, its analysis in various ways. If connected to different clinical databases, future trends can be predicted [22]
d. Readily available information access to paramedic staff (specialists, physicians, nurses etc) / departments can provide better medical support in an efficient way [23].
e. It is important to highlight that most of the citizens only share their information for treatment purposes and may not like its secondary uses. So, using citizens data without their consent will definitely disturb their privacy e.g. collection of Covid19 positive cases through various android apps across the world.

The use of EHR brought many benefits in healthcare field but having complete health and personal information in the form of EHR, which is highly accessible if not handled appropriately raises many concerns regarding data protection and privacy of citizens, few are as under:

a. Its unauthorize access can lead to many serious problems and can be life threatening as well [22]. This warrants serious protective measures of central data bank where patients' data is residing so that it should not land into unauthorized hands.
b. The data can also be stolen when in transition across the network or at rest when stored on distributed cloud servers [18].
c. In case of disclosure, it can be used for several purposes other than healthcare delivery.

### 2.1.4 Protected Health Information (PHI)

Any type of data or information that can be utilized to identify an individual in called PHI. It includes name, date of birth, picture, address, contact number, national identity number or social security number, biometrics (like fingerprints, voice, and retina), medical history (clinical notes, tests, X-rays, laboratory results etc) driving license numbers, vehicle details etc. It can be digital (stored in computers / databases) or manual record (paper files) of an individual. PHI is used in healthcare facilities for treatment and billing purposes [24].

### 2.1.5 Personally Identifiable Information (PII)

The importance of PII in privacy regulations is very high and considered very seriously. As per Department of Homeland Security (DHS) PII is "any information which can be used to infer the identity of an individual directly or indirectly" [25]. It also categorized sensitive PII as "the PII disclosed, lost or compromised without consent resulting into inconvenience, harm, embarrassment or unfairness to a person" [25]. NIST defines it as "information that can be used to distinguish or trace an individual's identity" [26], and "it can alone or combined with other information that is linked or linkable" [26].

### 2.1.6 Health Information Systems in Pakistan

In 1992, Pakistan deployed its first health management information system. Later in 2005, a new system was developed and rolled out countrywide at different tiers including national, provincial, district to sub-district level, however, faces integration issues. Data is

collected both through manual and electronic means and entered into the system at different levels [27]. Figure 2.2 (Source: http://www.nhsrc.pk) shows the national level dashboard being handled by the Ministry of National Health Services Regulations & Coordination in which various systems are feeding data directly or through APIs.

Apart from it several isolated systems both in public and private sectors at various levels are being used, however, they are not integrated with each other due to various issues like technology used, development platform and lack of data sharing mechanisms. Moreover, the isolated systems are generally limited in scope like disease specific (e.g. Polio, Dengue monitoring etc) or program specific (e.g. Vaccination Programs) and other category include hospital management (e.g. HMS used in Shoukat Khanum Memorial Hospital etc).

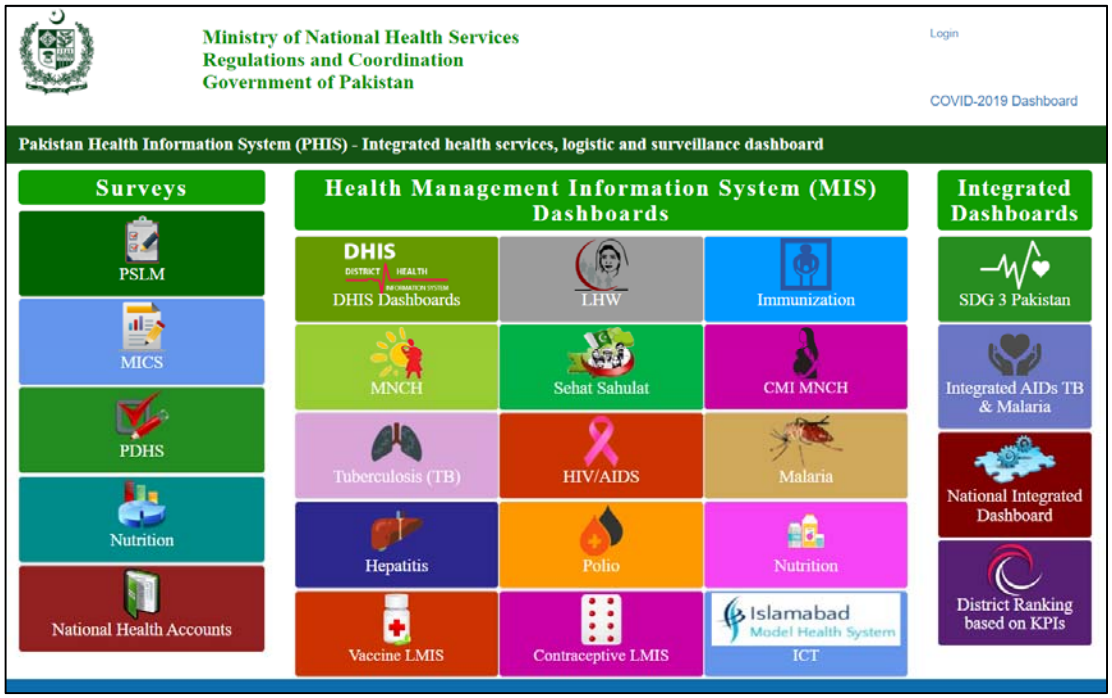


Figure 2.2 Pakistan Health Information System Dashboard

## 2.2 Secondary Use of Data

In this section, analysis of numerous secondary uses of data will be carried out with respect to patient's privacy. Mostly secondary data analysis is done to generate new clinical evidence as it provides insights of clinical practices.

a. **Administrative Purposes**. It is basically collected for billing and administrative purposes; however, some have the capacity to be used for gaps identification in services, administration and to improve health procedures[28].
b. **Clinical Research**. The growing population, increase in types of diseases and behavioral change in existing diseases have posed serious challenges for healthcare professionals. They are required to provide best drugs in short span of time to tackle hard pressed medical issue. Therefore, to identify causes of diseases, to understand response of new drugs and figure out its frequency of use, secondary use of data has a lot of importance for clinical trials. Recently, during covid-19, disease trend and efficacy of vaccine is much relevant example for secondary use of data and its importance in clinical research. Clinical research may include demographic based data, daily habits, labs result to investigate disease origin of diseases and efficacy of various drugs etc [29]
c. **Public Health Surveillance**. Data related to specific diseases like epidemics and pandemics is collected, processed, and analyzed to assess and administer overall public health including emergency preparedness.[10] In third world countries data is collected through manual means, however, in advance countries analysis is performed in EHRs and results are shared with general public for awareness and control the spread of diseases which are likely to harm large populations and spread in communities [30].
d. **Industrial Purpose**. To identify revenue streams and do targeted marketing, data is gathered and analyzed. Data helps to find medical services requirements in various ways like geographic location, gender, age brackets, specific disease etc. Accordingly, industry related to medial services, specially pharmaceutical industry plan their business activities [31].

EHR has been found beneficial in healthcare both in primary and secondary use of data, however, at the same time it poses many security and privacy challenges.

### 2.2.1 Security Challenges

Heath care is considered as one of the major industries and most valued as EHR contains a huge information, only in US it valued $5 trillion dollars [32]. Moreover, compromise of healthcare system can affect a large no of population. Therefore, it's always an attractive target for hackers to get ransom or sell stolen data in black market to get

financial gains. Fixed identifiers in EHR data are most vulnerable and are helpful to access patient's bank account. For example, in the USA, approximately 4.5 million patients were affected due to data breaches [33] and over 80 million suffered when a health insurance company Anthem BC/BS lost PHI in 2014 [34].

Heath systems are mostly online and internet-based systems which share EHR for various purposes including healthcare, billing and administration. Similarly, various kinds of data are collected through simple mobile apps, medical devices and wearable sensors for various diseases. These advancements are beneficial but increase the existing security risk, therefore, securing such data is a great challenge.

With the growth of e-health solutions, cloud services have been adopted worldwide to handle mass amount of data. Access to multiple authorized users from different geographic locations has opened another door to hackers and the threat to access large amount of data has increase manifold.

As per literature, many efforts have been made to safeguard EHR data. To access EHR data securely, many privacy-preserving and access control methods have been adopted [35], [36], however, still it remains a challenging task. Although advanced encryption methods are used but health systems hosted on cloud and EHR are still vulnerable to breaches [37] such as access to own database administrators who are authorized users to access massive data. Moreover, threats like key managers cannot be disregarded and less spending on system protections left many doors open and as well. To overcome this issue, healthcare sectors have started adopting blockchain technology in which patient's private key is used to decrypt the encrypted EHR [10], [38], [39]

### 2.2.2 Privacy Challenges

As per UNGA's universal declaration of human rights, "privacy is a fundamental human right" [40], however, its interpretation and implementation ways vary from country to country [41]. Generally, privacy concerns are raised once the patient's data collected for healthcare is used for different purposes without its consent and knowledge. Most importantly, in recent era various types of patient's data is collected without approval and knowledge with the help of various apps and sensors. With regards to privacy, various healthcare organizations are of the view that data jointly belongs to patients, physicians, and

healthcare organizations. [42]. However, it's not easy to ascertain ownership and who is owner of which part, and the issue needs detailed research.

Security issues also result in privacy issues and the same is the case with health systems and EHR. Data breaches can occur due to numerous reasons and can affect patients' privacy. Leakage and disclosure of patient's sensitive information can have ethical repercussions like impact on an individual's reputation in society. It can also lead to financial losses through access to bank accounts and in terms of medical insurance etc. Research shows that many patients avoid sharing or try concealing their sensitive information due to privacy as they have little trust in the security of healthcare system. Patients' mistrust on medical staff have also increased due to various data disclosure events. For example, in 2013, patients' medical information was sold by a medical technician of a US hospital [43]. Similarly, many cases of data hacking and stealing of medical records have happened worldwide [44].This privacy mistrust can lead to inappropriate medical care for patients and create disasters in healthcare.

### 2.3 Privacy During COVID-19 Pandemic

WHO declared the spread of "COVID-19 virus as pandemic" on 11 Mar 2020 [45]. In the information age, the world has witnessed the health emergency due to the rapid escalation of pandemic. The pandemic challenged the governments, public health authorities and privacy experts that were dealing with protection of personal health information.

#### 2.3.1 Surveillance Approaches

To trace covid infected persons, governments and healthcare authorities adopted various approaches including tracking through mobile networks, Bluetooth, GPS, video surveillance, credit card transactions as per details mentioned in Table 1. Mobile apps played and vital role in technological approaches and they were instrumental in augmenting traditional public health procedures to handle pandemics. Apps were used to collect symptoms, tracing contacts to infected persons, enforcing quarantine, generating disease clusters by mapping population movement and various analysis basing on collected information.

The main purpose of using such tools during the pandemic was to mitigate the risk and prevent the virus widely in larger communities. Tracing tools were used to measure

proximity and track interaction between users. Mobile phones helped through alerts once infected person came in proximity and health authorities were able to provide necessary care[46]. This also resulted in a reduction of virus transmission due to timely alerts.

Table 1 Region Wise Surveillance Approaches

| Region | Country | GPS | Credit Card Transaction | Video Surveillance | Bluetooth | Mobile Network |
|---|---|---|---|---|---|---|
| Asia | Bangladesh | | | ✓ | | |
| | China | ✓ | | ✓ | | |
| | Hong Kong | ✓ | | | | |
| | India | ✓ | | ✓ | | |
| | Pakistan | ✓ | | ✓ | | |
| | Singapore | | | | ✓ | |
| | South Korea | ✓ | ✓ | ✓ | | |
| | Taiwan | | | | | ✓ |
| Middle East | Iran | | | | ✓ | |
| | Israel | | | | | ✓ |
| | Saudi Arabia | ✓ | | | | |
| | Qatar | ✓ | | | ✓ | |
| EU | Belgium | ✓ | | | | |
| | Bulgaria | | | | | ✓ |
| | France | | | ✓ | ✓ | |
| | Germany | ✓ | | | ✓ | |
| | Italy | ✓ | | | ✓ | |
| | Poland | | | | ✓ | |
| | Turkiya | | | | ✓ | |
| | UK | | | | ✓ | |
| Africa | Ghana | ✓ | | | | |
| | Kenya | ✓ | | | ✓ | |
| | South Africa | | | | | ✓ |
| American | Canada | | | | ✓ | |
| | Colombia | ✓ | | | | |
| | Mexico | ✓ | | | | |
| | United States | ✓ | | | | |

### 2.3.2 Public Concerns

Although healthcare authorities were able to mitigate pandemic through this technology driven programs. However, the digital footprint at global level raised great privacy concerns worldwide. Discussion on relevant authorities is not possible in detail here, but elements of concerns have been highlighted.

As per Singer and Sang-Hun, in many countries the tracking and surveillance apps are launched by partnership of governments, healthcare providers and private sectors. Collection of data and tracking through cell phones, license plates readers, drones and facial recognition apps have threatened individuals' privacy [47].

Less adoption of apps was observed in United States due to privacy. Limit of data sharing was the most debated question across the country and public officials [48]. Privacy advocates that collected information individual rights even after covid as privacy rights relinquished are rarely regained. In March 2020, Congress wrote letter to US president and urged to protect the location and health data for privacy of US citizens. Recommendation by Congress includes data destruction and restoration of privacy standards after the pandemic is over [49]

Location trails covid positive cases was published online by South Korea. Though this helped the public regarding exposure to infected areas, however, it is considered as significant privacy breach as combining patterns of movement through location trails can easily be de-anonymized to retrieve information like home addresses.

To track suspected cases in China, consent from citizens was not sought to track their data through their mobile phones [50]. Taiwan government merged immigration system with health system to immediately trace record of outbound passengers [51]. Government plans to retain location data collected from tracking app which illustrates failure to consider personal data privacy.

According to polls conducted regarding app usage, 68% of the participants showed willingness for app usage that shares covid results with health officials, 50% were willing to use app which generate proximity alert, however, 45% were willing to share such data with health officials [52].

Based on the opinions and surveys, it is stated that people are of the view that pandemic situation will be used by political and corporate players to justify for maximum type of data collection for the future use.

### 2.3.3 Types of Privacy Concerns

a. **Personal Data**. Most of the tracing apps requests users to enter details through registration form which is further uploaded on server. Requests include to provide personal sensitive data which comes under protected information as per many privacy regulations:
   - Names & Surname. Most of the tracing apps request to enter names and surnames that are linked with mobile owner or app user. It is privacy-intrusive and can help to uniquely identify the person.
   - National ID Number. By providing it, citizens can be uniquely identified.
   - Cell Number. It is generally requested for two factor authentication through user interface and can also be retrieved programmatically.
   - Email. Email requested by tracing apps are mostly linked with corresponding cell phone and can lead to other information disclosure.

b. **Geolocation**. It is collected from mobile phones through GPS coordinates or network-based positioning through WiFi. The retrieved information is highly sensitive, including user habits, religious beliefs, address, and workplace data. Most of the privacy regulations consider this information as protected.

c. **Contacts**. Data of contacts came in close proximity to patient is collected which can reveal persons 'social circle and relatives' details which can further lead to identification of protected information like name, email, address etc.

d. **Travelling Information**. To control the spread and monitor virus transmission including its variants, countries also mandated to enter certain details for inbound and outbound passengers. For instance, the India mandated the use of Aarogya Setu app is to access public transport and airports. Similarly, Singapore made TraceTogether mandatory for migrant employees. Details of travelling also raised public privacy concerns regarding surveillance.

### 2.3.4 Relaxation of Privacy Laws

Most of the privacy regulations followed worldwide allow personal data processing without getting permission and knowledge of the person during special circumstances like

epidemics, where public health is in danger or in time of crises. However, this may require added safeguards. For example, EU's GDPR has existing clause for emergency Article 9: -

> *"Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy"* [2].

Privacy also provides relaxation in data sharing during imminent danger without the explicit permission of the patient. Under Civil Rights, the law permits sharing of protected health information without consent with *"anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public"* [1], however, covered entities are needed to share merely required information to accomplish the purpose of disclosing protected data.

Few countries have enacted new laws to handle covid emergencies which allow collection of public health data [2]. For example, Slovakia has passed a law allowing health authorities to collect location data through cellular companies to track movement of positive cases to ensure quarantine enforcement [53]. Others have standing committees that enable the data collection for use and enforcement of health specific orders.

### 2.3.5 Online Working & Education

To control virus transmission and during lockdowns, 'work-from-home' and 'online-studies' were adopted worldwide. This led to a spike in online traffic, more interaction with websites and high usage of apps like Zoom which had 300 million daily meeting participants [54], thus resulting in more hacking opportunities and privacy breaches.

a. **Online Working**. Official data which was handled in closed and protected environments got more prone to breaches once transmitted over internet [55].
b. **Online Education**. Multiple types of student's data were collected, and parents showed concerns regarding privacy as well during online activities [56],[57].

### 2.3.6 Home Monitoring Technologies, Telehealth, Telemedicine

Reliance on home monitoring technologies increased to a greater extent due to restrictions as an alternative, however, many security and privacy problems emerged. As per available literature, collection and online transmission of health data and fraudulent medical devices are the main privacy concerns of public and health authorities [58]–[60]

### 2.3.7 IT Initiatives of Pakistan during Pandemic and Data Privacy

Pakistan is amongst the very few countries which handled the pandemic amicably by establishing National Command and Operation Centre (NCOC). To monitor, analyze and control the disease, data of positive / suspect cases was required including their movement. As there was no centralized EHR System at national level for record keeping of covid patients and immunization, therefore, various IT solutions were developed and deployed in short period of time mainly with the help of NADRA, NIH and NITB and integrated with existing health systems of MoH and Provinces through APIs. Few examples are as under: -

a. **Pak Neghayban App**. The app provided features like positive declaration on voluntarily basis and positive cases zones [61]. It provided real time visibility of covid hospitals on vicinity basis with beds and oxygen availability. No personal data without user consent was collected and processed.

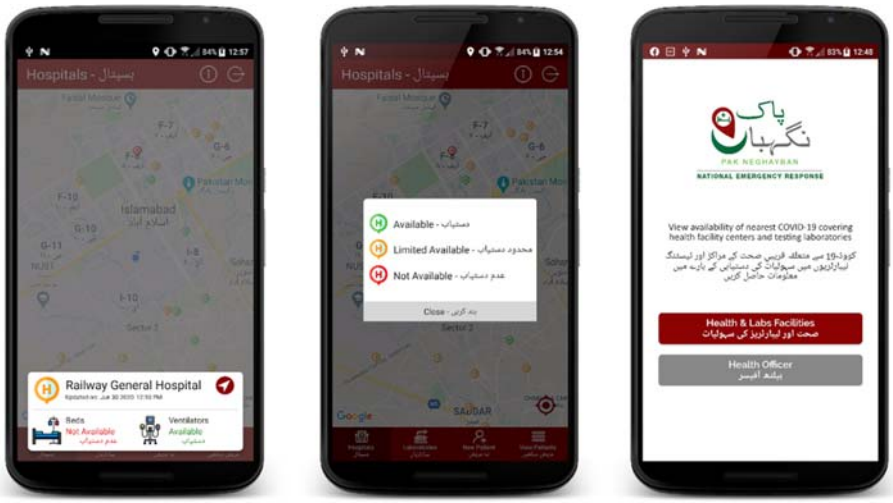


Figure 2.3 Pak Neghayban App

b. **Pass Track App**. The app was used to collect data of inbound passengers for quarantine enforcement, however, raised certain privacy concerns by citizens regarding collection of travelling details [62].

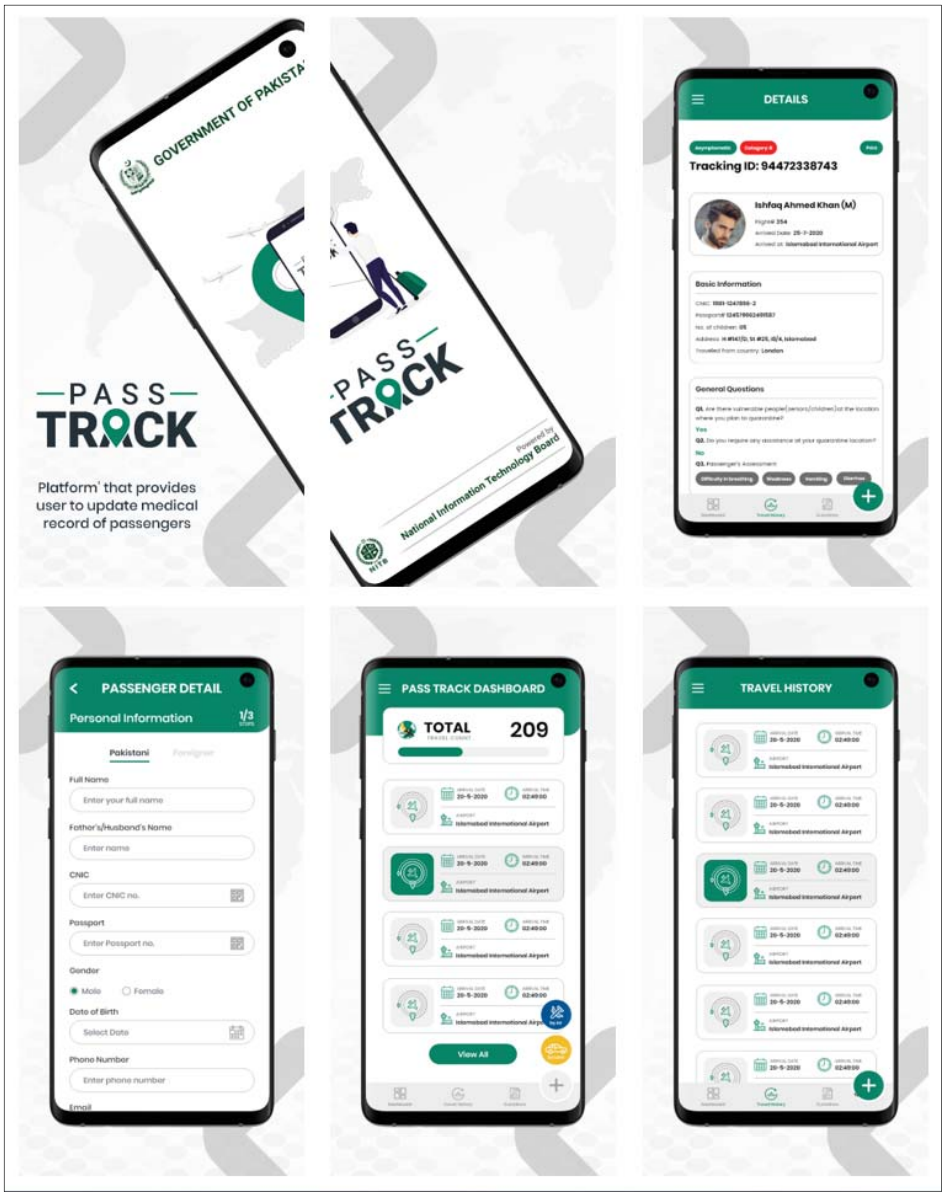


Figure 2.4 Pass Track App

c. **NIMS**. It was used to record immunization details of citizens based on CNIC. It was automated vaccine administration system built under the supervision of NCOC and MoNHR&C in collaboration with NADRA and EPI [63]. Although sensitive identifiers like CNIC, mobile numbers etc were used for phased vaccination of citizens, however, due to strict privacy protocols no major concern has been noted.


Figure 2.5 Sample Immunization Certificate – NIMS

In Pakistan, NADRA is custodian of the citizen's central data repository, therefore, systems developed and utilized during pandemic mainly revolved around the main database of NADRA. So far, no major concern in the country has been raised regarding data privacy during the pandemic because of public trust built on NADRA over the period. However, it endures huge responsibility of data recording and its protection as any lapse or leakage of data have severe consequences.

# *Chapter 3*

## GLOBAL LEGISLATIVE STRUCTURES

With evolving technologies in the digital era, unprecedented challenges and threats to data privacy are arising. To counter these threats, continuously effort have been made to improve privacy and security laws against evolving threats. Citizens' privacy is protected through various laws, regulations and accords in different regions of the world as shown in Figure 3.1 including HIPAA in the US [1], GDPR in Europe [2], and PIPL [64] in China. These standards are largely territorial whereas technological advancements and challenges are global. Important privacy regulations will be discussed including their challenges and scope of discussion will remain health care systems and privacy of citizen data.

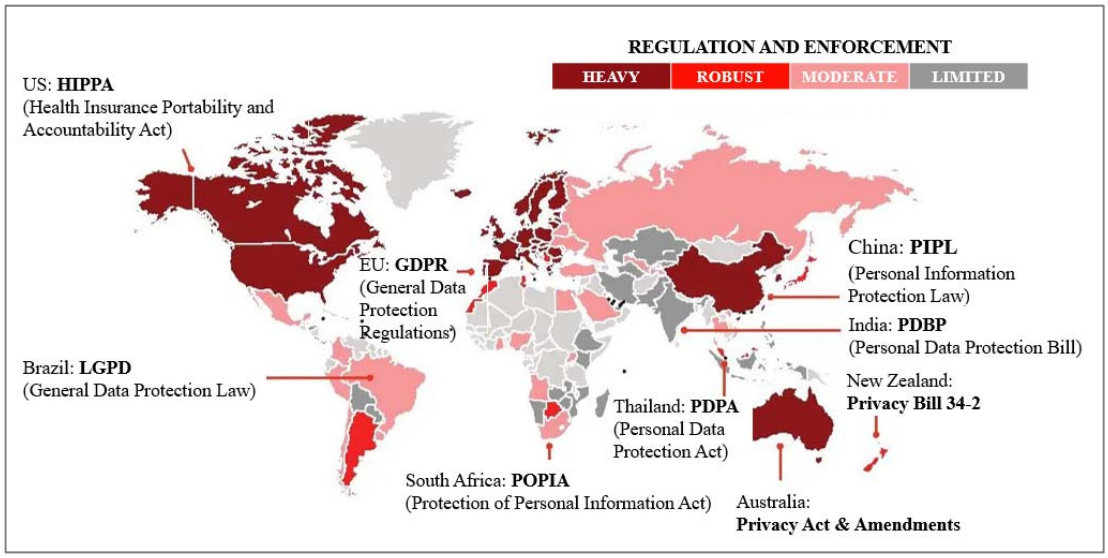


Figure 3.1 Global Data Protection and Privacy Regulation

### 3.1 Health Insurance Portability and Accountability Act

United States approved HIPPA law in 1996 with the aim to protect medical records in healthcare industry (includes healthcare employees, students, healthcare providers, insurance companies, billing companies, business associates) [65]. As per HIPPA, medical records are considered as PHI which can be used directly or indirectly to identify a person. Names, address, social security number, date of birth, contact number etc are considered as PHI. It includes written, spoken, or electronic data that is recorded on papers or stored in

computers and the data in transit. HIPPA comprises of five sections called ‘titles’ as shown in Figure 3.2, which are comprehensive, voluminous, and complex.


Figure 3.2 HIPPA SECTIONS (TITLES)

With the surge in medical records and unprecedented challenges, changes in HIPPA were made and additional standards and rules were introduced which further strengthened the law and significantly reduced the privacy breach incidents [8]. Few important rules are explained as under: -

### 3.1.1 Privacy Rule

The rule sets minimum standards to ensure that patients’ private medical data must remain private and confidential. The HIPAA privacy rule is applicable to “covered entities” which includes health care providers, billing houses and their business associates etc.

a. **Relative Disclosure**. It imposes constraints on the allowable uses and disclosures of PHI, specifying when, with whom, and under what circumstances, PHI could be shared [24]. As per disclosure clause, Hospitals may not reveal information of admitted patients over the telephone. However, this has resulted in problems for relative for locating patients in case of accidents.
b. **Right to Access**. It provides patients the right to request their own health related information when requested in writing. By law, the provider must provide the requested PHI (hard copy or electronic form as requested) within 30 days after such a request [1].

### 3.1.2 Exceptions to the Privacy Rule

HIPPA provides relaxations legally in certain conditions when health care providers can share PHI without consent of the patient, however, they are required to make sure that only minimum needed information is shared on need-to-know basis to accomplish the purpose of the request: -

a. Gunshot, stab injury or injuries sustained during a crime.
b. Health care operations, payments, treatments.
c. During a natural disasters or public health emergency declaration.
d. Suspected Child / Elderly abuse or neglect.
e. In case of court orders to do so.
f. Public health safety such as prevention from infectious and communicable diseases.

### 3.1.3 Security Rule

It introduces procedures designed to ensure that health records are appropriately secured and safeguarded from unauthored access. It complements privacy by implementing three types of security safeguards: -

a. **Administrative Safeguards**. These are policies and procedures meant to be adhered by employees. These may include access policies, sanction policies, audits, security awareness trainings for employees, contingency planning & data backup plans in case of disasters and cyber-attacks etc.
b. **Physical Safeguards**. These are designed to control physical access to PHI. It includes controlling and monitoring the access to offices, building, hardware, systems, physical files etc and scanning and inspection of incoming and outgoing equipment from the office building. Moreover, restriction on entry of terminated individuals.
c. **Technical Safeguards**. It includes protection of computer systems where PHI is stored and secure communication network over which its being transmitted. It must be protected from unauthorised viewing, copying, intrusion, alteration, and deletion. Procedures, hardware and software are required to be in place for incorporating encryption & decryption, backups, restoration and safe transmission.

### 3.1.4 Unique Identifiers Rule

In standard transactions, HIPPA covered entities are required to use a unique 10 digits number with the last digit a checksum - may be alphanumeric called National Provider Identifier (NPI).

### 3.1.5 Breach Notification Rule

According to breach notification rule, patients are required to be notified once their PHI is accessed in an unauthorized way [66]. This provides protection to patients from fraud and theft.

### 3.1.6 Transactions and Code Sets Rule

As per HIPPA, under standardized health care transactions, medical providers claim reimbursements electronically.

### 3.1.7 HITECH Act - 2009

` HITECH was introduced to with aim to nationwide implantation of EHRs and integrate health data. Significant change involves defining business associates (sub-contractors etc) in addition to covered entities that are subject to the HIPPA ruling. It offered incentives and subsidies to encourage the use of EHR by health care providers. On the other side it imposed penalties on those who were eligible but avoid implementation and prosecution at the state level in case of violations. HITECH also mandated public breach notification (discussed above) when PHI is revealed or utilised for an unlawfully [67].

### 3.1.8 Omnibus Rule Update - 2013

To further enhance privacy and protection of health information, a set of rules was issued by US Department of HHS. It includes amendments in Privacy and Security Rules of HIPPA, HITECH, Breach Notification Rule, and Enforcement Rules. It also classified genetic information as PHI by making amendment in Genetic Information Non-discrimination Act [68]. The important regulations included in Omnibus rule are as under: -

a. It expanded rights of patients to get electronic copy of their health record, if maintained on systems. Moreover, individual can request health care provider for transmission of health record to another person directly.

b. It brings more clarity to breach "the impermissible use or disclosure of PHI is presumed to be a breach unless a covered entity or business associate can demonstrate, through a factor-based risk assessment, that there is a low probability that the PHI has been compromised" [68].

c. Removal of the limited data sets exception.

d. Broadened the definition of a business associate by including their subcontractors which will also be required to comply with HIPPA and be liable for their own breaches.

e. Usage of PHI for fundraising and marketing by organizations.

f. Provided flexibility for PHI of deceased individuals. Protection period reduced to 50 years after death.

g. Relaxation during a natural disaster.

HIPPA rules have significant impact on the functioning of healthcare organizations in terms of adherence to complex regulations, financial penalties for violations and implementation cost to ensure compliance. It has been noted that it effected clinical health occasionally once healthcare providers refused to share life-saving information during critical time. The reasons behind this includes lack of knowledge of healthcare providers about the regulations and their responsibilities and risk of stiff penalties.

It is believed by many researchers that HIPAA has a substantial negative impact on healthcare research. According to *Edemekong, Peter F, Pavan Annamaraju, and Micelle J. Haydel*, patients follow-up surveys have been dropped by 95% drop due to HIPPA privacy laws [69]. As per *O'Herrin JK, Fost N, Kudsk KA*, HIPAA seems to hinder research in the field of medical and it has increased workload for researchers being unable to meet the governing HIPPA requirements. The researchers are discouraged due to substantial penalties and abandoned the studies because of regulatory obstacles. Although there is provision for researchers to carryout research on de-identified data without patient permission, however, 31% data was lost once identifiers were removed, which includes vital information required to carry out research [65].

## 3.2 General Data Protection Regulation

It is a set of rules written by policy makers and lawyers regarding data protection and privacy, came into force in 2018 [2], which aimed to standardize data privacy regulations across EU countries. The regulations provide greater protection to individuals' data thus reducing and avoiding the risk of wrongful processing of data. It is established on the idea that "privacy is a fundamental human right" in line with Charter of EU Rights. The law is imposed through software systems which are supposed to keep personal data safe so that it may not be used for direct or indirect identification [70]. It is considered as the world's strongest data privacy rule which contains 11 chapters and 99 articles.

### 3.2.1 Scope

a. **Temporal Scope**. Processing started after the application of GDPR (i.e. 25 May 2018) falls under temporal scope, if it meets the obligations of material and territorial scope.
b. **Material Scope**. It applies to organizations (public and private) for processing of personal data. Four categories (personal, special types of personal data, pseudonymous and anonymous data) are used by GDPR to explain legal obligation for its processing.
c. **Territorial Scope**. Under Article 3, it applies to organizations established within the EU irrespective of whether they perform processing operations within EU or not. It is also applicable to organizations which are established outside EU; however, they carryout data processing within EU including imported datasets. It also becomes applicable as per public international law. In simple words, the transmission of personal data from EU to other countries is not allowed except limited lawful exemptions (Adequacy decision, Binding Corporate Rules, Explicit Consent and Derogations).

### 3.2.2 Personal Data Under GDPR

It is applicable to electronically stored information, signs or indications related to an individual. Few types of data which could be processed or used to distinctively identify an individual are categorized as sensitive personal data and need greater protections. These include person's name, location data (addresses), ID number, online identifiers (such as IP

address and cookies), pictures, demographic information, political opinions, religious faiths, genetic and biometric data, health information etc as shown in (Figure 3.3) [2].

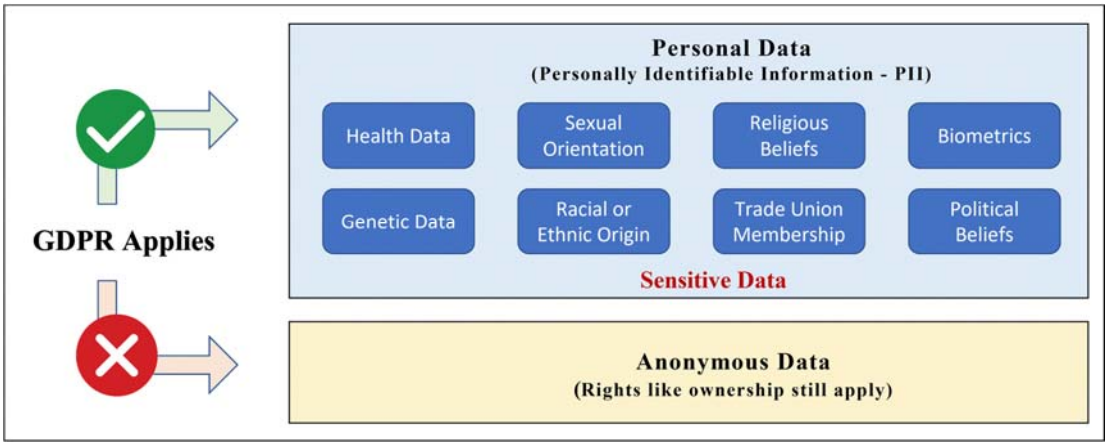


Figure 3.3 GDPR Application

### 3.2.3 GDPR Application

GDPR applies to the owner of personal data and anyone who is processing or controlling its processing [71].

a. **Subject.** Personal data owner is called as subject.

b. **Controller**. Data controllers are individual or organizations which overall exercise control on processing of personal data.

c. **Processors.** The individual (natural person) or organizations which carry out processing of personal data on behalf of controller.

### 3.2.4 Key Principles

As per article 5 of the GDPR, seven data protection principles are laid out to guide lawful processing of data. These are not hard rules, however, act as overarching framework to layout the broad purpose: -

a. **Lawfulness, fairness, and transparency**. Usage of data must be clearly communicated to the subject.

b. **Purpose limitation**. Collection of data must be carried out as per defined purposes and should not be used for other than defined purposes.

c. **Data minimization**. Only the minimum amount of data required for specific purpose be collected by organizations.
d. **Accuracy**. Organizations must take reasonable steps to ensure that collected data is accurate and up to date. Data must be deleted or changed when a data subject makes such a request.
e. **Storage limitation**. Collected data should not be retained longer than necessary.
f. **Integrity and confidentiality**. Appropriate protection measures must be applied to personal data to ensure its secure and protected against breaches.
g. **Accountability**. Data collectors are responsible for ensuring compliance with the regulation. Organizations that process large amounts of sensitive personal data are required to appoint a data protection officer (DPO).

### 3.2.5 Privacy by Design

GDPR instils Privacy by Design model and based on the realisation that the conditions for data processing are fundamentally being set by the software and hardware used [Article 25]. This core principle is supported by transparency and accountability. To ensure transparency, businesses are required to provide full information to individuals in accessible manner and understandable language. Accountability requires that businesses consider users' data privacy in their systems by placing appropriate technical and organizational measures. Developers must keep in mind factors likes risk management, data minimization, pseudonymisation within software and incorporate features which complies with regulations. Moreover, user consent to be the essential component of software and must be explicit in the case of data collection and its processing for any purpose. Individuals must be provided details about data recipients, time for data retention as per individual rights provided by GDPR [72][73]

### 3.2.6 Privacy by Default

It protects the individuals against the practice of maximum data collection by the organizations. By default, only minimum required personal data shall be collected. To achieve privacy by default, data controllers and processors working on their behalf are required to take measures regarding data collection, limits of processing and retention period. Less complex and privacy friendly default settings be adopted in software incorporating user consent to obtain minimum personal data for processing (article 25, section2).

### 3.2.7 Data Subject Fundamental Rights

GDPR has empowered citizens by giving them new rights (article 13, 14, 15, 16, 17, 18, 20, 21, 22) related to their personal data as shown in Figure 3.4.

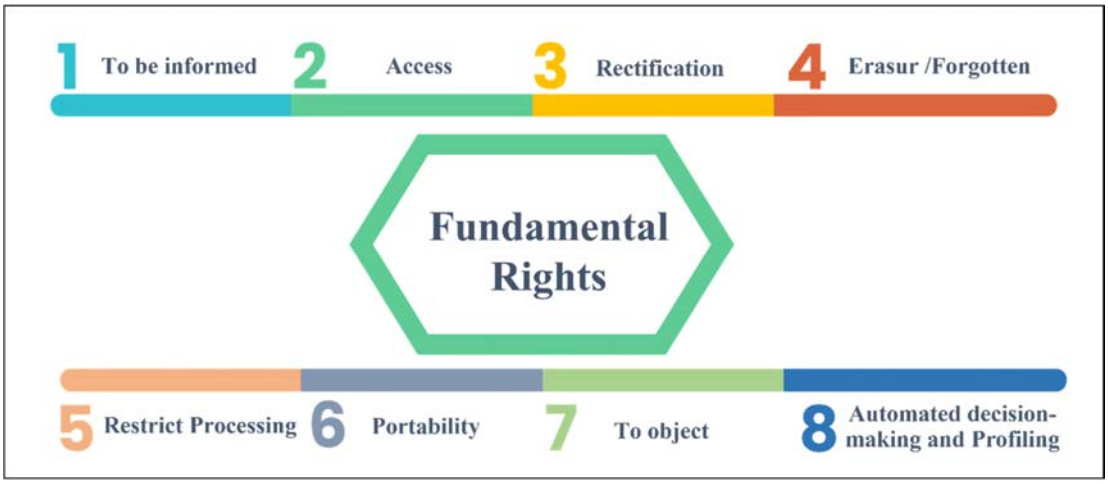


Figure 3.4 Fundamental Rights

### 3.2.8 Lawful Processing of Health Data

In article 9, GDPR has provided additional protection to health data especially personal genetic data, biometric data including photographs (Recital 51 GDPR) as its use including processing and transmission is sensitive. So, to process such information, number of requirements are required to be met as per regulations [74]. Even this data is inferred through further processing of non-special category data held, in that case, processing must still meet the Article 9 requirement which includes explicit consent of data subject.

### 3.2.9 GDPR Breaches and Fines

As per Article 4, regulation is applicable to all types of breaches including accidental regarding data loss, unlawful disclosure, unauthorized access, and processing of transmission.

GDPR regulates businesses for compliance through heavy fines and severe penalties. In case of breach or non-compliance, GDR can impose fines up to €20 million or 4% of a firm's global turnover; whichever is greater. A Portuguese Hospital was fined €400,000 for 'deficient' account management practices. Other heavy fines include Google - €50 million

(biggest fine so far), British Airways - €200 million and Marriot Hotels - €100 million [75],[76].

### 3.2.10 Major Compliance Concerns

As per survey carried out by Ovum, 68% are of the view that cost of doing business in Europe will increase and 52% believe that more fines will be imposed on compliance to GDPR [77].

According to Veritas GDPR Report 2017 [78], the responses received from more than 900 businesses (based in various countries including UK, Germany, Australia, USA, France, Japan, Singapore, and South Korea) showed multiple concerns regarding the GDPR which are reflected in Figure 3.5.

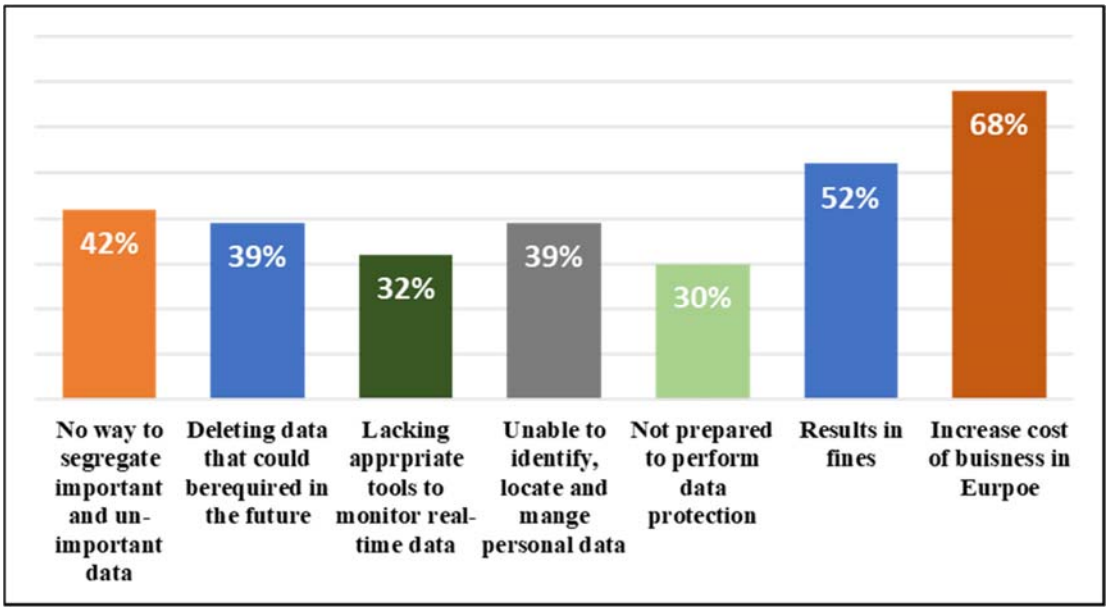


Figure 3.5 Major Compliance Concerns

## 3.3 Personal Information Protection Law

In China, there are currently ten different privacy laws. Apart from laws, there are five national and nine administrative standards to impose privacy protection. These mainly include PIPL, Civil Code and Data Security Laws. PIPL was passed and adopted in 2021 and it brought significant improvement regarding data protection in China [79]. It recognised and categorised health data as 'sensitive information' and is subject to legal protection [80]. As per PIPL Article 28, the processing is only allowed with specific purpose and sufficient necessity (minimum one legal ground required) and under strict protective measures. As per

PIPL Article 13, several legal grounds have been provided by PIPL for processing of personal information are as under: -

a. Obtaining individuals' consent.
b. Performance of the contract or management of human resource.
c. To fulfil legal requirement.
d. During public health emergencies, life safety, health, and property of individuals in case of disasters.
e. For public interest including news reporting.
f. In case personal information of individuals has already been revealed publicly.
g. Where otherwise allowed by laws or regulations.

### 3.4 Personal Information Protection and Electronic Documents Act

PIPEDA is privacy law of Canada which started in 2000 and implemented in 2004. It regulates the collection of personal information, its usage and disclosure. Fundamental principles of PIPEDA covers accountability, identified purpose for data collection, use of individual consent, purpose limitation, data accuracy, safeguards against data thefts, openness of privacy policies and should allow individual to access his data. Moreover, right to challenge an organization that does not comply [81]. As of October 2018, privacy laws like The Personal Health Information Protection Acts for health sectors have been declared by various provinces of Canada in line with the PIPEDA [82].

### 3.5 Data Privacy Regulations - Pakistan

There is no comprehensive data protection regulation regarding privacy of citizens data specially for healthcare systems.

a. **Constitution.** Article 14(1) of the Constitution of the Islamic Republic of Pakistan accords the right to privacy as a fundamental right [83]; however, certain exceptions also exist in the constitution.
b. **National Cyber Security Policy - 2021**. One of the objectives of policy is "*To protect the online privacy of the citizens by provisioning the required support and system to all the concerned institutions and organizations that are dealing with citizens' data-related matters be more equipped and able to render their services, accordingly*" [3]. Apart from this no specific privacy point pertaining to privacy of health care data is mentioned.

c. **National Digital Health Framework of Pakistan (2022-2030)** [4]. The framework issued by Ministry of National Health Services Regulations and Coordination has in partnership with Provincial Health Departments aims for digital health platforms with a view to promote the protection of health systems against cyber-attacks including fraud, exploitation, and monetization of health data.

d. **Pakistan Health Information System Action Plan & Provincial Action Plan 2020-2024.** Terms of Reference of National HIS Technical Sub-Committee includes the task of "*Recommend and oversee implementation of standards to maintain privacy and confidentiality of data*"[27].

e. **PECA 2016**. Currently PECA is the main legislation regarding data protection with respect to information systems in Pakistan. However, citizens data privacy with respect to health care systems is not covered specifically [84].

f. **Pakistan Personal Data Protection Bill - 2021 (draft)**. It has been proposed by MoITT [5], however, it's not clear when the Bill will be enacted. The Bill has been drafted mostly in line the European GDPR and covers following: -

- Scope. Application of the Bill in whole Pakistan.
- Data Protection Authority / Regulatory Authority in the form of Commission (within the six months) after the approval of Bill which will issue guidelines and act as protection and regulatory authority.
- Legal bases which include consent and matters like public safety.
- Principles for lawful processing.
- Various controller and processor obligations including notifications, transfers of data, appointment of data protection officer, data retention period, impact assessment and contracts.
- Data subject rights of informed, access, rectification, erasure, object, data portability, automated decision making and other.
- Penalties on unlawful processing up to PKR 15 million and subsequently up to PKR 25 million.

### 3.6 Comparison of Data Protection Regulations

After discussing important data protection regulations, following differences were found regarding regulating healthcare information in USA, EU and China (Table 2).

Table 2 Comparison of Global Legislative Structures Regulating Healthcare Information

| | **US - HIPPA** | **EU - GDPR** | **China - PIPL** |
|---|---|---|---|
| **Adoption** | HIPPA was strictly enforced since 2003 to protect patients' data and privacy | GDPR was enforced in May 2018 with objective to standardise data privacy laws across EU countries regarding protection of EU citizens data privacy | PIPL was enforced in November 2021 and aim to regulate issues related personal information protection. |
| **Territorial Scope** | Applies to covered entities, business associates, individuals, organizations residing or operating in the US. | Applies to EU based companies but and to those who collect data of citizens of EU countries even residing outside EU. (GDPR Article 3) | Applies within China for processing of protected information, however, may be appliable outside on occurrence of special event or special circumstances. (PIPL Art. 3.) |
| **Definition** | **Individually identifiable health Information**. It include demographic information or data which can be used to identify an individual. It ca be related to historical health record, health care provision or its payment details. | **Personal data**. Information through which an individual can be identified directly or indirectly. Identifiers which can be used to reveal information include name, address, genetic information, demographic identity. (GDPR, Article 4) | **Sensitive personal information**. It includes basic information about an individual and individuals' medical health data. (PIPL, Article 28, Paragraph 1) |

| | | | |
|---|---|---|---|
| | Common identifiers include name, email or residence address, date of birth, and national identity number). (45 C.F.R. § 160.103) | | |
| **Considered Elements** | - Name<br>- Email addresses<br>- Social Security Number<br>- Dates<br>- Phone numbers<br>- Fax numbers<br>- Account number<br>- Vehicle number<br>- URLs<br>- IP Addresses<br>- Biometric data<br>- Face photo<br>- Any unique code | - Names<br>- Identification number<br>- Location data<br>- Online identifier<br>- Any specific identifier related to the physical, psychological, mental, genetic, cultural, economic, or social identity of the person.<br>- Social media posts<br>- Pictures<br>- Lifestyle preferences<br>- Transactions data<br>- IP addresses<br>- Racial & Ethnic data<br>- Political opinions<br>- Sexual orientation | - Biometric characteristics<br>- Religious beliefs<br>- Specific identity<br>- Medical health<br>- Financial accounts<br>- Individual location tracking etc |
| **Consent Model** | Individual authorization consent should be in writing. (45 C.F.R. § 164.508) | In writing (including electronic) or oral statement<br><br>(GDPR introduction, Article 32) | Written consent should be obtained<br><br>(PIPL, Article 29) |
| **Exceptions to Consent** | - Health care operations, | - Clinical or preventive purpose | - Public health emergency |

| | | | |
|---|---|---|---|
| | payments, treatments.<br>- During a natural disasters or public health emergency declaration.<br>- Suspected Child / Elderly abuse or neglect.<br>- In case of court orders to do so.<br>- Public health safety such as prevention from infectious and communicable diseases.<br>(45 C.F.R. 64.502(a)(1)) | - For the interest of public health.<br>- Work capacity assessment at jobs<br><br>(GDPR, Article 9, Paragraph 2) | - Life protection during emergency<br><br>(PIPL, Article 13) |
| **Withdrawal of Consent** | Individual can revoke the granted authorization through in writing revoke request.<br><br>(45 C.F.R. § 164.508(b)(5)) | Subject can **withdraw** the consent for data processing.<br><br>(GDPR, Article 7, Paragraph 3) | Processing based on authorized consent can be withdrawn. Moreover, individuals to be provided convenient ways of withdrawn consent by data processor.<br><br>(PIPL, Article 15) |
| **Data Protection Officers (DPO)** | Designate privacy officer with responsibility of developing and implementing | DPO must be appointed in case of processing of the data include public authorities and | Personal information protection officers to be designated who should |

| | | | |
|---|---|---|---|
| | privacy policies for covered entities. (45 C.F.R. § 164.530(a)) | organization processing large-scale sensitive personal data. (GDPR, Article 37) | supervise personal information processing and adopt data protection measures. (PIPL, Article 52) |
| **Fines** | $100 to $50,000 per violation with $1.5 million per year as maximum penalty | Up to 20 million Euro or 4% of annual revenues (GDPR, Article 83) | Up to 50 million RMB or 5% of the previous year's turnover, and other operational sanctions (PIPL Article. 66) |
| **Marketing** | Using or disclosing PHI is prohibited unless a specific authorization form | Authorization should be expressly and explicitly to the individual and required to be presented clearly and separately from any other information. | |

# *Chapter 4*

## Privacy Preserving Techniques

There are numerous data preservation techniques available in the literature which are used to make data secure and ensure its privacy. However, these can be categorized mainly in two groups. First group covers randomization and anonymization methods for privacy preservation. Second group cover different cryptography algorithms for data privacy and third method covers the identity and access management.

### 4.1 Anonymization and Randomization Techniques

Most of the data preservation techniques are centred at anonymization of data. Some of them are discussed with reference to the big data security and privacy. Anonymization of data are normally achieved through shuffling, suppuration, and redaction. Shuffling is the method of scrambling the data within column in such a way to disassociate its original attributes. Suppuration is achieved by removing the sensitive data from dataset. Whereas redaction is the process of hiding some part of the data from the whole column's values. Some of the popular techniques of anonymization are discussed in this section [85].

#### 4.1.1 K anonymity

K anonymization is a technique to muggle up data using suppression and generalization in a fashion that de-identification of data is not easily possible. K anonymization is specially designed to address the issue of re-identification of the anonymized data. However, k anonymization is prone to background knowledge attack and homogeneity attack. Some benefits of K diversity are preservation of identity, less cost as compared to other anonymity techniques like cryptography [86],[85].

#### 4.1.2 L Diversity

It is an extension of K anonymity and was introduced to address the issue of homogeneity attack. In this method sensitive data is made limited by greater distribution methodology. However, it is not always possible to implement L diversity due to the variety of data. This mechanism is also based on K anonymity but protects attribute disclosure and produce better performance as compared to its predecessors. L diversity is prone to similarity and skewness attacks in some cases [86], [87].

### 4.1.3 T Closeness

This technique is an advance version of L diversity based on the anonymization which preserves the privacy by decreasing the granularity of the data set. This method protects against background knowledge and homogeneity attack. It overcomes the drawback of L diversity by identification of semantic closeness of attributes [86].

### 4.1.4 Randomization Technique

Randomization is an effective method of achieving privacy. It can be achieved by a probability distribution, which is the process of adding noise to the data. Randomization is normally accomplished during pre-processing and data-collection phase and is best suited for sentiment analysis and surveys. However, randomization on a large dataset is not effective due to reason like data utility and time complexity [85].

## 4.2 Cryptographic Technique

Cryptography is the knowledge of encryption and decryption used for securing data from unauthorized access. As obvious from the name, Crypto means hidden, and graph means writing which cumulatively means the security of data from fraud and unauthorized access. There are multiple techniques used for privacy preservation of data in the literature, some of the popular techniques are discussed as follows.

### 4.2.1 Encryption Algorithms

Encryption is a process of securing data by converting it mathematically such that it cannot be translated by an unauthorized person. It can also be described as the conversion of data from readable (plain text) format to a form that cannot be easily understood (cipher text). There are multiple encryption algorithms available in literature that are used for privacy preservation like AES, Triple DES, RSA, Blowfish, Twofish etc [88].

### 4.2.2 Hash Functions

It converts a variable numeric data into a fixed length value of numeric data output. Due to the preimage resistance property of the hash function (it is computationally difficult to reverse hashed data). Hash table techniques are vastly used for privacy preservation. Popular hash function are Message Digest (MD) variants like MD2, MD4, MD5 and MD6, Secure Hash Function (SHA) variants "SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512" and RIPEMD and its different variants [89].

### 4.2.3 Homomorphic Encryption

It is a new version of encryption techniques used for privacy preservation of data. This method allows us to perform computations over the encrypted data without compromising encrypted data. Single homomorphic encryption has the characteristic of addition or multiplication whereas fully homomorphic encryption has the property of addition and multiplication as well. Homomorphic encryptions are computationally slow [90].

## 4.3 Identity and Access Management Techniques

It is a framework of technologies that ensures the right users have legitimate access to data and technologies. Identity and access management is not a tool for privacy preservation but can provide a mechanism for ensuring the privacy preservation of data. Coupling identity and access mechanisms with other privacy preservation techniques can ensure the privacy of data by limiting access to legitimate users [91].

## 4.4 Service Level Agreement (SLA)

Service-level agreements do not preserve privacy but provide assurance that the data or services should not be misused. SLAs ensure through heavy fines and other disciplinary consequences that data and services be used as per the clauses of the agreement and do not deviate from policy and agreements [92].

# *Chapter 5*

## Proposed Framework

After literature review of health information systems and global regulations regarding the privacy, it has been concluded that almost all legislation, laws and acts provide various principles to ensure user data privacy. Privacy is generally assessed by doing compliance check. However, to evaluate the privacy compliance of apps with respect to various privacy principles, a framework has been proposed in which privacy principles have been incorporated mainly inferred from best privacy regulations discussion in Chapter 3. In addition to privacy principles, other components which are required for app evaluation have also been incorporated into the framework based on best practices.

### 5.1 Privacy Evaluation Areas

To evaluate the privacy various principles and standards exist around the globe. However, following evaluation areas based on the principles and components of renowned regulations (Figure *5.1*) have been selected for the proposed framework: -

a. App Privacy Policy
b. Lawfulness
c. Fairness
d. Transparency
e. Purpose Limitation
f. Data Minimization
g. Retention
h. Integrity & Confidentiality
i. Accountability
j. Data Transfer & Sharing
k. Architecture
l. Tracing Method
m. Development Sponsorship
n. Usage

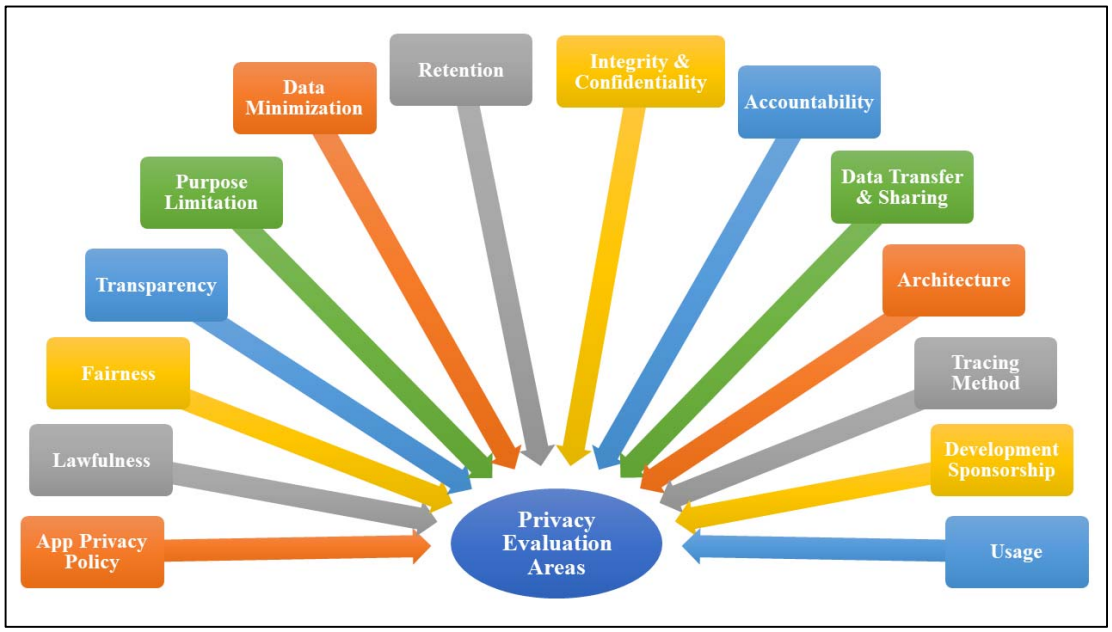


Figure 5.1 Privacy Evaluation Areas

## 5.2 Evaluation Areas and KPIs

After finalising the privacy evaluation areas, key performance indicators (KPIs) have been proposed against the each as shown in Table 3. The KPI will help to evaluate the key areas with respect to privacy in each category of privacy areas.

Table 3 Privacy Areas and KPIs

| Privacy Areas | Key Performance Indicators (KPIs) |
|---|---|
| **Privacy policy** | Privacy Policy is Available? |
| | Is it comprehensive? |
| | Is it clear and understandable? |
| **Lawfulness** | Seeking Consent in clear and understandable language? |
| | Does regulations allow use of tracing apps? |
| | Legislation for Tracing Apps? |
| **Fairness** | Only adequate, relevant and limited data is collected? |
| | Kept no longer than required |
| **Transparency** | User rights |
| | Does the apps mentioned purpose of processing other than required? |
| | Lawful basis |

| | |
|---|---|
| | Public interest |
| | Notifications |
| **Purpose limitation** | Specify the purpose(s) for which personal information is collected, processed and stored. |
| **Data Minimization** | Collect only what is required. |
| **Retention** | Data Deletion Timeline (indefinite period, time limit or until action completed) |
| | Can user request the data deletion? |
| | Decommissioning of App |
| **Integrity and confidentiality** | Data encryption and Anonymity |
| | Access Control |
| **Accountability** | Audits |
| **Data Transfer and Sharing** | Data Sharing |
| | Third Party API's |
| | Secondary Use |
| **Architecture** | Centralised |
| | De-centralised |
| | Hybrid |
| **Tracing Method** | Location Data Collection |
| | Proximity |
| | Mobile Operators |
| **Development Sponsorship** | Government |
| | Private |
| | Multi-stakeholders |
| **Usage** | Mandatory |
| | Voluntary (Opt-in/ Opt-Out) |

### 5.3 Grading Criteria

The input of apps statistics and performance against the key performance indicators, apps will be graded based on values. Following grading criteria has been devised based on the value system from 0 - 3, where 3 will be for full implementation and compliance and 0 for situation where principles are not considered nor applied as show in Table 4.

Table 4 Grading Criteria

| Privacy Principles Implementation & Compliance | Value |
|---|---|
| Privacy principles were implemented and complied. | 3 |
| Privacy principles were partially implemented and complied. | 2 |
| Privacy principles were weakly implemented and complied. | 1 |
| Privacy principles were not considered nor applied. | 0 |

## 5.4 Privacy Concerns Level

Based on the value assigned through grading carried out with reference to the privacy principles and their compliance against key performance indicators, four levels of privacy concerns have been proposed as show in in Table 5.

Table 5 Privacy Concerns Level

| |
|---|
| **Normal** |
| **Low** |
| **Medium** |
| **High** |

## 5.5 Proposed Framework

Apps values will be entered against Privacy areas and their corresponding key performance indicators. Same will be graded as per criteria discussed above. After the grading privacy concern will be evaluated. A diagrammatic depiction of framework has been shown in Figure 5.2.

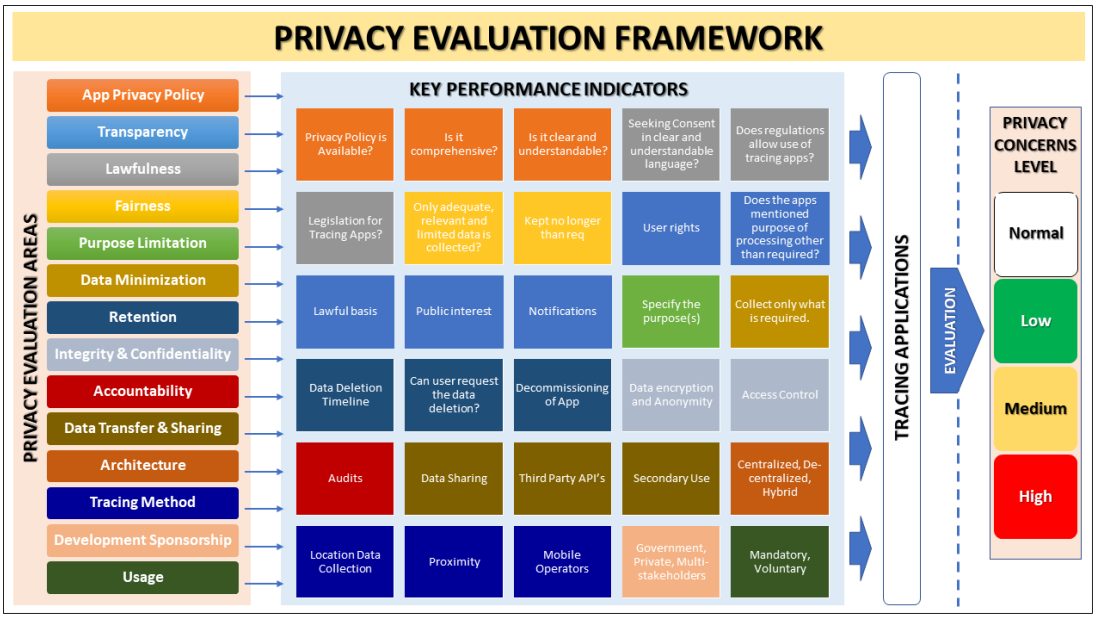


Figure 5.2 Proposed Privacy Evaluation Framework for Tracing Apps

## 5.6 Benefits

The framework will help to evaluate apps privacy status and will provide concern areas as output. Accordingly, governments, healthcare authorities, developers and other concerned authorities will be able to address privacy concerns.

# *Chapter 6*

## Case Study - Tracing Apps and Privacy during Covid19

### 6.1 Context

Contact tracing apps have been commonly known to public due to their use during COVID-19 pandemic. Most of the countries developed their own mobile apps to collect data of covid infected patients and used it for surveillance of infected patients, identifying high infected areas and to counter covid spread. These apps proved to be highly beneficial, however, this data-driven innovation raised the privacy concerns around the globe.

### 6.2 Objective

To analyse contact tracing application used during COVID-19 and verify compliance to data privacy regulations with a view to recommend suitable measures for adoption in future to ensure protection of individuals data.

### 6.3 Study design

Multiple application analysis used in covid for contact tracing.

### 6.4 The cases

Contact tracing apps used in 62 countries sponsored by governments, private organizations and multi-stakeholders, which offered multiple features like tracking patients, enforcing quarantine and generating disease cluster.

### 6.5 Data collection

Research papers, books, journals, news items identified from local and national websites, health websites.

### 6.6 Analysis

The COVID-19 pandemic severely affected the population globally and claimed millions of lives. After analysing the disease spread pattern, it was established by WHO and healthcare professionals that contact with covid positive patients is prime reason of virus transmission. Contact was defined by WHO as "*Being in face-to-face contact within one meter for more than 15 minutes with a COVID-19 patient or having direct physical contact with a patient*" [93]. Now to undertake tracing of persons (potentially infected with covid)

who came in close proximity of covid positive case, manual tracking strategy was adopted for testing, quarantine, and care purpose. However, to match covid spread speed and, various technologies (GPS, Bluetooth etc, discussed in subsequent paragraph) and surveillance approaches were adopted for effective contact tracing and reduce transmission [94]. WHO mentioned in its guidelines for covid contact tracing that collected data to be protected from identification and harmful disclosure; to be used for safety of public health only, not for punitive or security measures, safeguards must be in place for privacy as per legal framework of respective countries, data handlers to follow ethical principles and digital tools must be assessed for data protection before use by countries [93].

Though WHO asserted for personal data privacy during contact tracing but at same time various countries flexed their regulations for effective contact tracing and public safety.

Tracing apps (discussed below) were developed globally in short span of time as complementary response to quickly perform contact tracing, however, it resulted into mass violations of privacy of public data, and this resulted into decrease of public trust on their governments [94]. The other technological methods like GPS based monitoring including cauterised data collection models also raised concerns about data privacy [95]. The privacy concerns lead to less usage of tracing apps due public hesitancy worldwide which impacted disease spread monitoring and impeded quarantine and care process.

This case study presents a detailed analysis of tracing apps developed and used by various countries in the context of user data privacy.

### 6.6.1 Scope of Apps

The apps were developed with varied scope in each country including contact tracing, health reporting, alerting, quarantine enforcement, self-diagnostic as shown in Figure *6.1*, information related to covid and covid facilities like available of oxygen bedded hospitals in near vicinity etc.

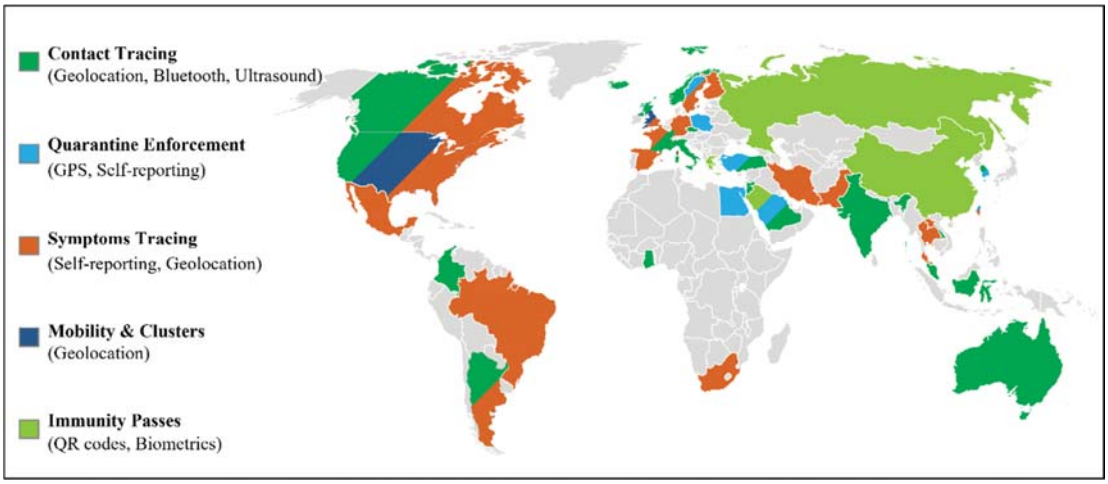


Figure 6.1 Worldwide Mobile Surveillance Programs

### 6.6.2 Architecture

Centralised, decentralised and hybrid architectures were commonly used for development of tracing apps during covid as shown in Figure *6.2*.

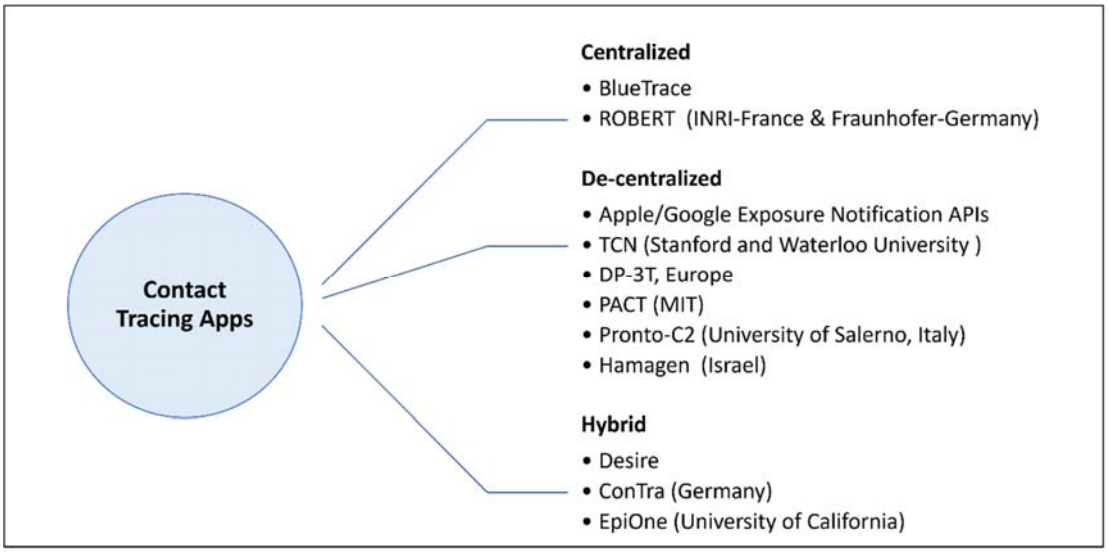


Figure 6.2 Protocols based on Architectures

#### 6.6.2.1 Centralised

Gathered user data is uploaded and managed on a central server. The identifiers are generated through central server. The diagnosed user uploads the list of identifiers sensed in predefined time period to central server. The other users regularly check from the server whether they were in proximity. Various models have used which includes networked based location tracing, mobile device tracking, card transactions and contact logs uploading when in proximity of other users. Generally, BlueTrace and Pan-European privacy-preserving

proximity tracing (PEPPPT/PEPP) protocols have been followed for centralised model [96]. The model provides direct and better oversight of user data, however, access to raw location data through centralised model has significant potential of privacy breach [97][46]. Steps involved (Figure 6.3) are discussed below: -

a. **Registration**. User installs the tracing app and get registered by proving details like name, mobile no, data of birth and post code.
b. **Generation of Unique ID**. Server verifies the legitimate user by sending OTP through SMS to mobile number. After verification servers generates and transmits the Unique_ID along with expiry time.
c. **Exchange of Encounters Messages**. Encounter message (encrypted Unique_ID, phone model and transmit power) is exchanged with other app users though Bluetooth once come in close contact and devices record timestamp of message delivery and Received Signal Strength Indicator (RSSI).
d. **Encounters Data Upload**. This data is uploaded on central server on voluntary basis. If user tests positive, the health official marks it positive in server. The server generates OTP, and data is uploaded on verification.
e. **Exposure Notification**. Server decrypts Unique_ID and uses RSSI and transmit power to calculate proximity. Accordingly, alerts are sent to users from central server who remained in proximity and had likely exposure to positive case.

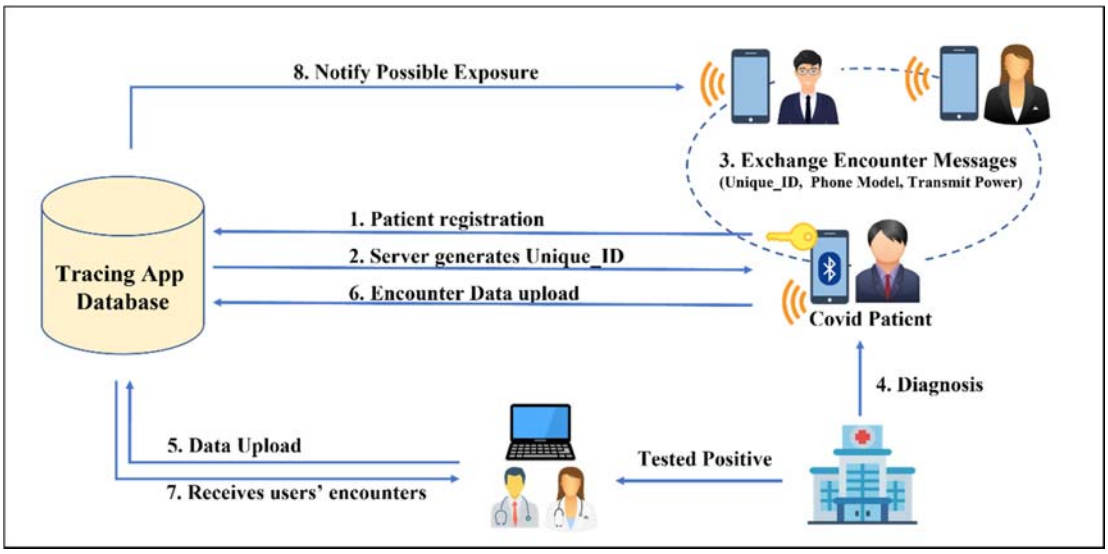


Figure 6.3 Centralised Architecture of Covid Tracing Apps

#### 6.6.2.2 Decentralized

In this model, user data is generated, stored and managed locally on user devices and not shared with central server. The identifiers are exchanged between devices locally by apps installed on user mobile phone. Once the user diagnosed positive, the app sends list of seen identifiers to the server which notifies the devices who were in proximity. Apps used protocols like Temporary Contact Number (TCN), MIT Media Lab's SafePaths, DP3T or Google/Apple exposure notification framework [98]. As the processing is performed at user end, therefore, devices with high computation powers are required. The model provides better privacy, however, vulnerable to eavesdropping and false alerts attack [99], [100]. Steps involved (Figure 6.4) are discussed below: -

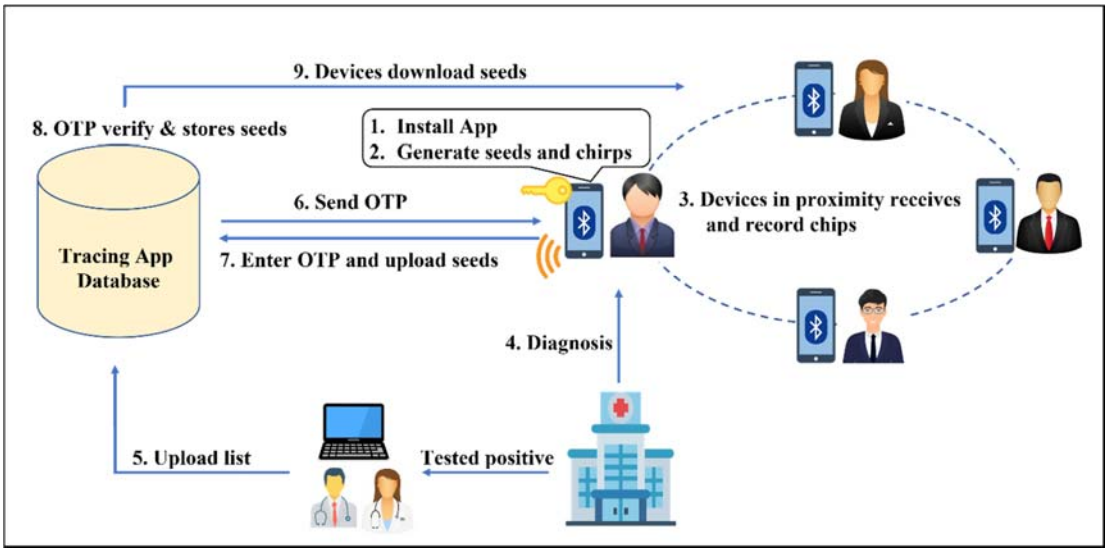


Figure 6.4 Decentralized Architecture of Covid Tracing Apps

a. **Installation of App**. Generally, registration process is not required like centralised model. Apps deploy seed generation algorithm on user mobile phone after installation.
b. **Seed and Chirps Generation**. In this model, seed are generated by user mobile phone. Then a pseudorandom function generates chirps from seeds and current time. These anonymous chirps are broadcasted via Bluetooth. The receiving devices stores chirps, RSSI and time stamps.
c. **Encounters Data Upload**. Once tested positive, the health authorities provide Unique ID to authorise data upload of all seeds, however, data of single user is uploaded as compared to complete list in case of centralised model.

d. **Contact Tracing**. The app contact server generally once in a day and download any seed updated by positive case. Then the app performs lookup in local chirp log to identify any infected person in proximity.

#### 6.6.2.3 Hybrid

In this model, load is balanced between user device and server. The divided functionalities improve privacy preservation as well. Steps involved are discussed below: -

a. **App Installation & Registration**. Two step authentication is performed in this model. Servers verifies the mobile number by sending the OTP and app by authorization token. Then it assigns a Unique_ID and sends encrypted key. Both the phone number and encrypted keys are not retained by the server.
b. **Generating and Exchanging of Ephemeral IDs**. Devices generates Ephemeral IDs using Diffie Hellman key exchange mechanism and start broadcasting through Bluetooth. The app maintains query and upload tables.
c. **Uploading Encounter Data**. Once uploads data with consent once tested positive.
d. **Contact Tracing**. User uploads query table record to server once wants to check exposure. Server matches the values with infected users data using time and duration values and accordingly generate notifies the user.

### 6.6.3 Technologies Adopted

Mainly tracking is carried out on location basis through GPS navigation system and proximity based via Bluetooth LE radio signals. GPS based tracing has more privacy issues as compared to Bluetooth due to its limited range. Other techniques include WiFi for indoor environment, geofencing technology using wristbands, check-in QR codes at contact points, digital contact tracing with IoT and cameras [101], [102].

### 6.6.4 Methods of Tracing

Contact tracing was performed by adopting following methods (Figure 6.5): -

a. **Location**. Mobile apps provide geo-location using GPS and other location sensors like network-based positioning by using WiFi.
b. **Proximity**. Mobile apps use Bluetooth and GPS to sense neighbouring devices and proximity estimation.

c. **Mobile Operators**. Contact tracing is performed using base-station level information provided by cellular companies.

d. **Hybrid solution**. Any combination of at least two of above-mentioned methods.

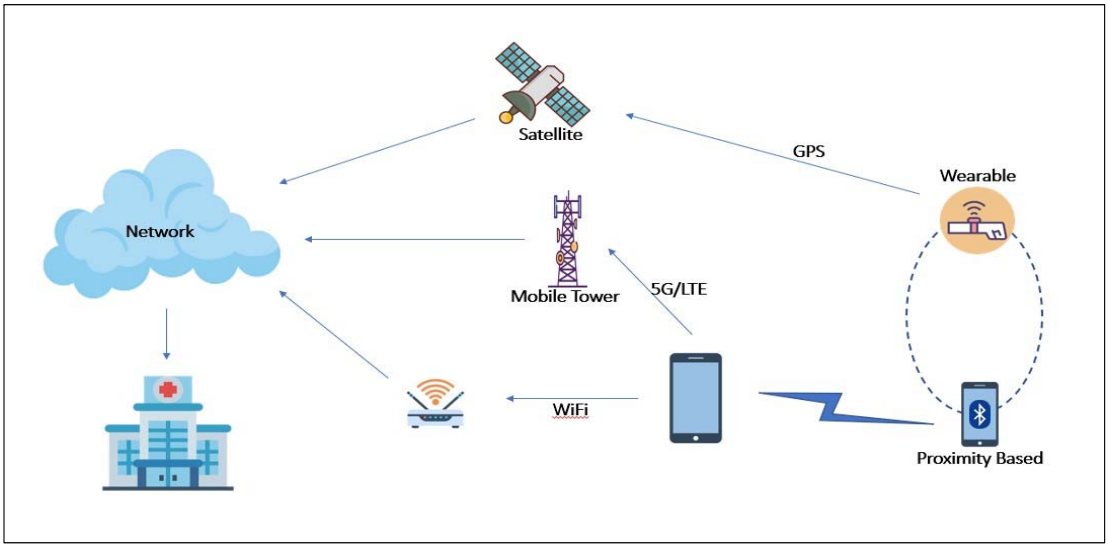


Figure 6.5 Tracing Methods Used

### 6.6.5 Sponsorship

Apps were either sponsored by Governments, public and private sectors, or the combination of above. Moreover, Apple, Google and Amazon set the limit on addition of apps to stores only through official and trustable organizations.

### 6.6.6 Usage

Installation of apps and their usage was made mandatory by a few countries during high spread of covid, however, it was voluntary in some countries. Few countries used mix policy of mandatory / voluntary like they make it mandatory at some public locations and during quarantine period as safety measures. Mandatory usage has higher privacy concerns as compared to voluntary where users are provided rights to select or opt-out the specific permissions [103], [104].

### 6.6.7 Data Collection

WHO provided minimum information parameters [93] for data collection during contact tracing (Table *6*) and data related to location and health status was collected mostly with consent and notifications. However, most of the researchers are of the view that additional data than requirement was also collected without consent and informing the public [96].

Table 6 Type of Information Collected by Tracing Apps

| **Information Type** | **Details** |
|---|---|
| Contact identification | - Contact ID<br>- Identification number<br>- Complete name<br>- Contact number (mobile, landline) and list<br>- Pictures (immunization certificates)<br>- Address/lat-long<br>- Passport number |
| Demographic details | - Association with the source positive contact<br>- Date of birth<br>- Age Categories (Senior, Adults, Youth, Children)<br>- Gender (M/F/T)<br>- Occupation<br>- Linguistic details |
| Contact Type | - Type<br>- Date<br>- Duration<br>- Factors |
| Health Symptoms | - Breathing problem, Fever or Chills, Cough, Fever, Diarrhoea, Fatigue, Headache, Loss of smell or taste<br>- Any other issue |
| Miscellaneous Details | - Covid test time<br>- New or Quarantine location |
| Immunization Details | - Vaccination Details<br>- Types of Vaccine<br>- Data of Vaccination<br>- Location / Health Centre of Vaccination |

### 6.6.8 Integration with EHRs

The tracing apps were also integrated with health care systems in various countries. Exchange of data (e.g. immunization record, testing results etc) was done through APIs based on identifiers. Although it helped in analytics and research like effects of particular vaccine wrt demographics, re-infection rate after immunization and re-infection based on type of vaccine but at the same time is a serious privacy issue.

### 6.6.9 Privacy and Security Concerns

According to a John Hopkins study, 82% of US citizens reported that they would use a tracing app which is accurate and ensures privacy. Only 24% - 26% would want an app with less chances of data leakage [105]. As per a cross country survey with approximately 6000 participants, it was observed that people generally support tracing app, however, US citizens were found less supportive mainly due to lack of interest in government [106]. In Ireland, people who were not using app responded that its due to privacy concerns. 42% mentioned surveillance concern, 35% mentioned cybersecurity, however, 74.8% would use and opt-in app [107]. In Jordan, 37.8% used app, however, privacy was general concern of the participants [108]. Privacy-preserving is claimed by many apps which means that their identity and location will not be revealed without explicit user consent. Another concern is that apps might be re-purposed to track users after pandemic.

## 6.7 Country Wise Analysis of Tracing Apps

Table *7* presents detailed analysis of various COVID-19 tracing apps have been developed worldwide. It discusses specifically privacy-related features of COVID-19 apps in numerous countries and includes the origin County of app, app name, developed or sponsored by (Government, public, private), its usage (mandatory, voluntary opt-in or opt-out options), feature and architecture (centralized/decentralized/hybrid). It is evident from the table that most of the apps used centralized model thus leading to privacy breaches. After analyzing each app, it has been noted that few apps are mandatory during quarantine period and in highly infected zones including public points like hotels, airports, and railway stations etc, however, user can opt-out after where it’s not mandated.

Table 7 List of County Wise COVID-19 Apps

| **Country** | **App Name** | **Origin (Governmental /Multistakeholder/private)** | **GPS/ Bluetooth/ other** | **Mandatory (Yes/No)** | **Key Features** | **Architecture (centralised/ decentralised /hybrid)** |
|---|---|---|---|---|---|---|
| Austria | Stopp Corona | Governmental/ Private | Bluetooth, DP-3T, Google/Apple | No | Contact tracing, Medical Reporting | Decentralized |
| Australia | COVIDSafe, Coronavirus Australia | Governmental | Bluetooth | No | Contact tracing, Quarantine enforcement | Hybrid |
| Azerbaijan | e-Tabib | Governmental | NA | NA | Information | NA |
| Bahrain | BeAware | Governmental | Bluetooth, GPS | Yes | Contact tracing, Quarantine enforcement, Alerts | Centralized |
| Bangladesh | Corona Tracer BD | Governmental | NA | NA | Contact tracing, Information | NA |
| Brazil | Tô de Olho | Governmental/ Private | NA | No | Contact tracing, Medical Reporting | NA |
| Belgium | Belgium's app | Governmental/ Private | Bluetooth, Google/Apple | No | Contact tracing, Medical Reporting | NA |
| Bulgaria | ViruSafe | Governmental | GPS | No | Contact tracing, Symptoms | Centralized |
| Canada | Covid Shield, ABTraceTogether, COVID Alert | Governmental | Bluetooth, Google/Apple | No | Contact tracing, Self-diagnostic, Information | Centralized |
| Chili | CoronApp | Governmental | NA | NA | Self-diagnostic, Information, Reporting | NA |
| China | Alipay &WeChat. HealthCode | Private | GPS, QR code | Yes/No | Contact tracing, Symptoms | Centralized |
| Colombia | CoronApp | Governmental | NA | No | Contact tracing, Demographics, Symptoms, Action taken | Centralized |
| Croatia | Stop COVID-19 | Governmental | NA | NA | NA | NA |

| Country | App Name | Origin (Governmental /Multistakeholder/private) | GPS/ Bluetooth/ other | Mandatory (Yes/No) | Key Features | Architecture (centralised/ decentralised /hybrid) |
|---|---|---|---|---|---|---|
| Cyprus | CovTracer | Governmental/ private | GPS | No | Contact tracing | Centralized |
| Czech Republic | eRouška (eFacemask) & Mapy.cz | Governmental | Bluetooth | No | Contact tracing | Centralized |
| Denmark | Smittestop | Governmental | Bluetooth | No | Contact tracing | NA |
| Estonia | HOIA | Governmental | Bluetooth, DP-3T, Google/Apple | No | Contact tracing | NA |
| Fiji | careFIJI | Governmental | Bluetooth | NA | NA | NA |
| Finland | Koronavilkku, Ketju | Governmental/ Private | Bluetooth, DP-3T | No | NA | Decentralized |
| France | Alertano, StopCovid, uTakeCare | Private/Governmental/Multistakeholder | Bluetooth, PEPP-PT/ROBERT | NA | Contact tracing | Hybrid |
| Georgia | StopCovid | Governmental | PEPP-PT | NA | Contact tracing | Hybrid |
| Germany | Corona-Warn-App | Governmental/ Multistakeholder | Bluetooth, Google/Apple, TCN | No | Contact tracing, Medical Information | Hybrid |
| Ghana | GH COVID-19, Tracker, OHIOH, Ito | Governmental | GPS | No | Contact tracing, Action taken | Centralized |
| Greece | DOCANDU Covid Checker | Multistakeholder | NA | NA | Self-diagnostic, Information | NA |
| Hong Kong | StayHomeSafe, LeaveHomeSafe | Governmental | QR code | Yes | Contact tracing, Quarantine enforcement | NA |
| Hungary | VírusRadar | Governmental | Bluetooth | No | Contact tracing | NA |
| Iceland | Rakning C-19 | Governmental | GPS | No | Contact tracing | Centralized |
| India | Rakning C-19, Corona Watch, Quarantine Watch, Mahakavach, COVA Punjab, Aarogya Setu,Saiyam, COVID-19 Quarantine Monitor | Governmental | Bluetooth, GPS | Yes | Contact tracing, Quarantine enforcement, Medical Reporting, Self-diagnostic, , Action taken | Centralized |

| Country | App Name | Origin (Governmental /Multistakeholder/private) | GPS/ Bluetooth/ other | Mandatory (Yes/No) | Key Features | Architecture (centralised/ decentralised /hybrid) |
|---|---|---|---|---|---|---|
| Indonesia | Care Protect, PeduliLindungi | Governmental | TBD | Yes | Contact tracing | Centralized |
| Ireland | HSE Covid-19 App | Governmental | Bluetooth, Google/Apple | No | Contact tracing | Decentralized |
| Israel | HaMagen & Track Virus | Governmental/ Private | GPS | No | Contact tracing | Centralized |
| Italy | alertaLOM, Covid Community Alert, diAry, Rintarricia dei contatti, SM_COVID19, Immuni | Governmental | Bluetooth, Google/Apple, GPS, TCN, RecoVer | No | Contact tracing, Self-diagnostic, Alerts, Medical Reporting | Decentralized |
| Japan | COCOA | Governmental | Google/Apple | No | NA | NA |
| Jordan | AMAN | Governmental | NA | NA | Contact tracing | NA |
| Kuwait | Shlonik | Governmental | NA | NA | Self-diagnostic | NA |
| Kyrgyzstan | Stop COVID-19 KG | Governmental | NA | NA | | Centralized |
| Latvia | Apturi Covid application | Governmental | NA | NA | Contact tracing | NA |
| Malaysia | MySejahtera, Gerak, MyTrace | Governmental | Bluetooth, Google/Apple | No | Contact tracing, border crossing | NA |
| Mexico | Covid-19MX, Plan Jalisco | Governmental | NA | NA | Contact tracing | NA |
| Morocco | Wiqaytna | Governmental | NA | NA | Contact tracing | NA |
| Nepal | COVIRA app | Private | NA | NA | Information | NA |
| Nederland | CoronaMelder | Governmental | QR code, DP-3T | NA | Contact tracing | Decentralized |
| New Zealand | NZ COVID Tracer | Governmental | QR code | No | Contact tracing | NA |
| North Macedonia | StopKorona! | Governmental | Bluetooth | No | Contact tracing | Centralized |
| Norway | Smittestopp | Governmental | Bluetooth, GPS | No | Contact tracing | Decentralized |
| Pakistan | COVID-19 Gov PK | Governmental | GPS | No | Contact tracing, Information, Self-diagnostic | Centralized |
| Philippines (Cebu) | Staysafe | Governmental/ private | Bluetooth | No | Contact tracing | Centralized |
| Poland | Kwarantanna domowa, ProteGO-Safe | Governmental/ Multistakeholder | Bluetooth | Yes | Contact tracing, Quarantine enforcement, Symptoms, Action taken | Decentralized |

| Country | App Name | Origin (Governmental /Multistakehol der/private) | GPS/ Bluetooth/ other | Mandatory (Yes/No) | Key Features | Architecture (centralised/ decentralised /hybrid) |
|---|---|---|---|---|---|---|
| Portugal | Stayaway | Governmental | NA | NA | Contact tracing | NA |
| Qatar | Ehteraz, COVI | Private | Bluetooth, GPS | Yes | Information | NA |
| Russia | Social Monitoring | Private | NA | Yes | Contact tracing | NA |
| Saudi Arabia | Tawakkalna and Rest Assured | Governmental | TBD | Yes | Contact tracing, Symptoms | Centralized |
| Scotland | Protect Scotland | Governmental | NA | NA | Contact tracing (later disabled) | NA |
| Singapore | SafeEntry, TraceTogether | Governmental | Bluetooth | Yes | Contact tracing | Hybrid |
| Slovak Republic | ZostanZdravy | Private | NA | NA | Contact tracing, Action taken | Centralized |
| South Africa | Covi-ID, AlertSA | Governmental | NA | NA | Contact tracing | NA |
| South Korea | Corona 100m, Self-Isolator Safety Protection | Private | GPS | Yes | Contact tracing, Quarantine enforcement, Demographics | Centralized |
| Spain | Radar COVID, CononaMadrid, Covid19.eus | Governmental | DP-3T | No | Contact tracing, Symptoms, Information | Centralized |
| Slovenia | ZVem | Governmental | NA | NA | NA | NA |
| Sri Lanka | MyHealth Sri, Lanka, Self Shield | Governmental | NA | No | Contact tracing, Quarantine enforcement | Centralized |
| Switzerland | SwissCovid | Governmental/ Multistakehol der | Bluetooth, DP-3T, Google/Apple | No | Contact tracing | Decentralized |
| Taiwan | Taiwan Social Distancing | Governmental/ Private | NA | NA | Contact tracing | NA |
| Thailand | Mor Chana | Governmental | Bluetooth, GPS | No | Contact tracing | Centralized |
| Turkey | Korona Önlem, Hayat Eve Sığar | Governmental | Bluetooth, GPS | Yes | Contact tracing, Symptoms | Centralized |
| UAE | TraceCovid, Tawakkalna (Covid-19 KSA) | Governmental | Bluetooth | NA | Contact tracing, Quarantine enforcement | NA |
| Ukraine | Act at home | Governmental | NA | No | Contact tracing | Centralized |

| Country | App Name | Origin (Governmental /Multistakeholder/private) | GPS/ Bluetooth/ other | Mandatory (Yes/No) | Key Features | Architecture (centralised/ decentralised /hybrid) |
|---|---|---|---|---|---|---|
| UK | NHS COVID-19 | Governmental | Bluetooth, Google/Apple | No | Contact tracing | Decentralized |
| USA | Coalition App, covid safe, Covid watch, NOVID, Private kit: SafePaths | Private/Multistakeholder | Whisper Tracing Protocol, TCN | No | Contact tracing, Self-diagnostic, Medical Reporting | Decentralized |

### 6.8 Results based on Country Wise Comparison

After analysing the available data and features of various apps in various countries, following results were drawn: -

a. 72% of the apps were sponsored by the governments, 9% were developed by the private sector and 19% were developed by the partnership of multi stakeholders as shown in Figure *6.6*.

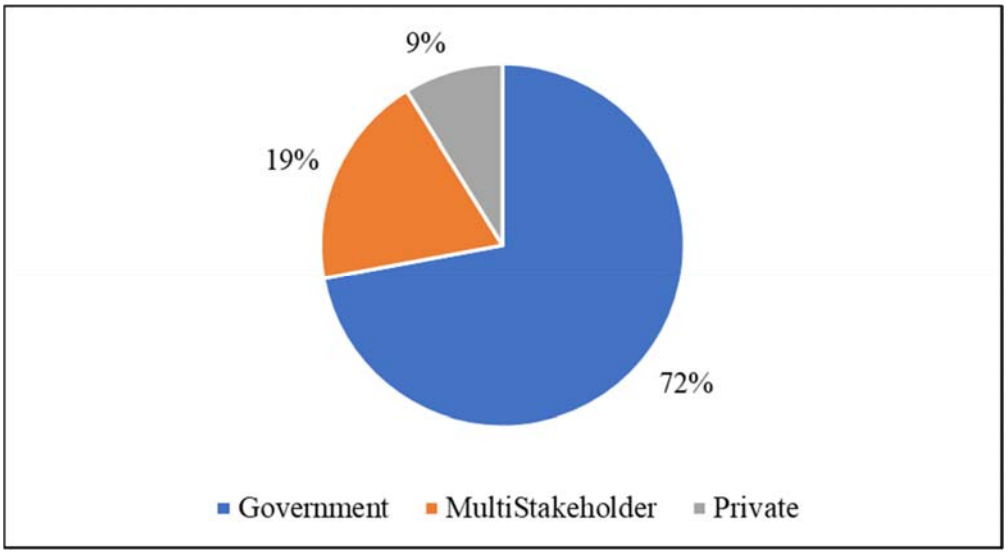


Figure 6.6 Development Sponsorship of Tracing Apps

b. Various technologies / protocols have been used; however, Bluetooth is mostly utilised with 37% followed by GPS i.e. 15%. Utilization of remaining is reflected in Figure *6.7*.

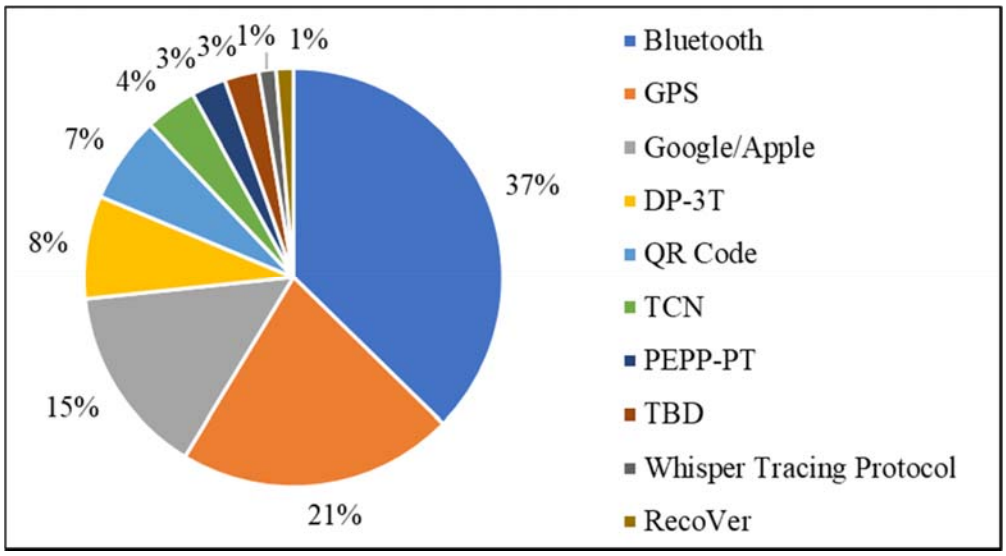


Figure 6.7 Technology Used by Tracing Apps

c. Few countries enforced mandatory used of tracing app during covid peaks; however, same was converted to voluntary later. As per available data, 74% countries made it voluntary and only 26% as mandatory as shown in Figure *6.8*.

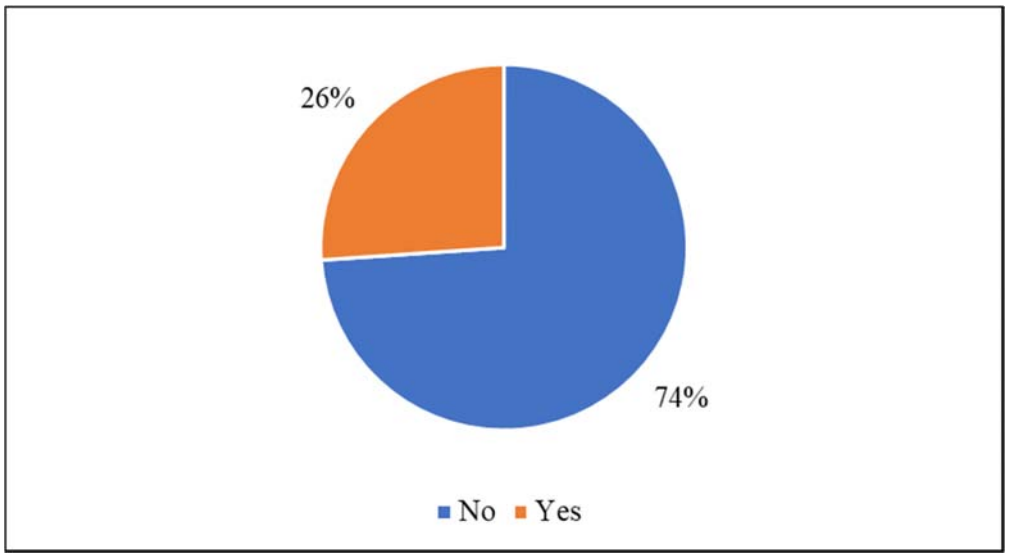


Figure 6.8 Mandatory / Voluntary Usage of Tracing App

d. 52% apps were used for tracing purposes. 9% provided feature of information related to covid. Other major purposes include Quarantine enforcement, self-diagnostic, medical reporting, covid symptoms, action taken etc as reflected in Figure *6.9*.

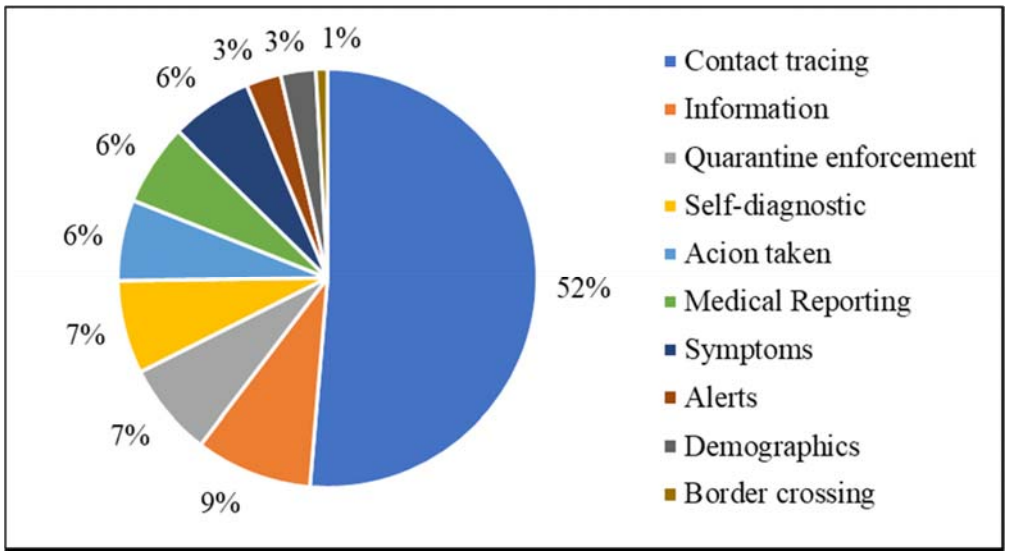


Figure 6.9 Features Used by Tracing Apps

e. As per available data, 61% apps utilised central architecture, 26% decentralised and 13% followed hybrid model as shown in Figure *6.10*.

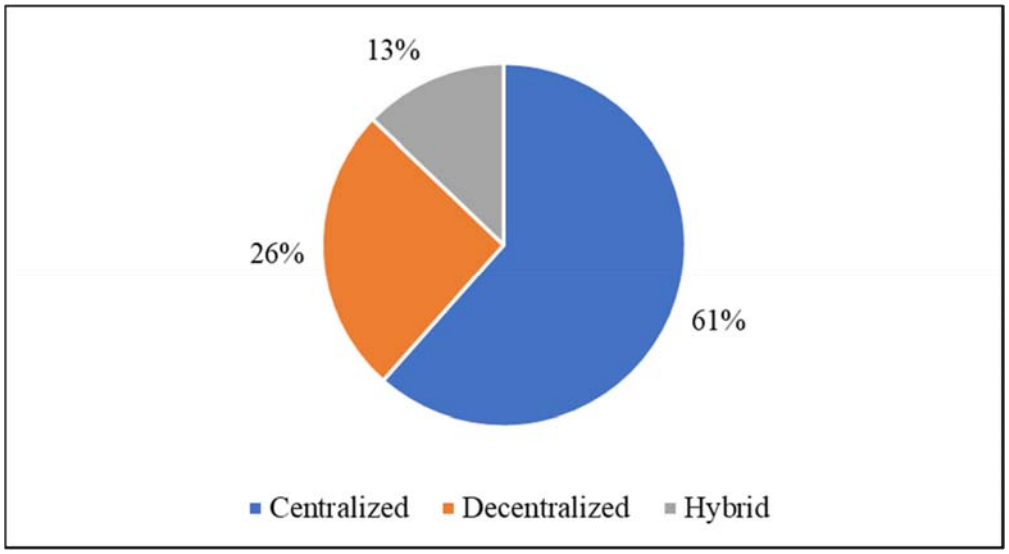


Figure 6.10 Tracing App Architecture Used Worldwide

## 6.9 Evaluation of Tracing Apps based on Proposed Framework

Basing on the results drawn from various tracing apps worldwide, now their evaluation will be carried out based in proposed framework.

| Evaluation Areas | Key Performance Indicators (KPIs) | Apps Compliance Description | Grading Value | Privacy Concern |
|---|---|---|---|---|
| Privacy policy | Privacy Policy is Available? | Most of the app have not mentioned any privacy policy in App Stores. Few apps deleted the provided policies after some time. | 2 | **Low** |
| | Is it comprehensive? | Mostly data privacy part is not covered comprehensively. | | |
| | Is it clear and understandable? | Few have mentioned clearly, however, in many apps its not clear for common person. | | |
| Lawfulness | Seeking Consent in clear and understandable language? | It has been observed that people were not given the free choice in apps over the data. Both under the privacy regulations and ethically, what kind of data will be collected, which data is shared, with whom and when and for how long. Mostly default settings were to share everything, all the time. | 2 | **Low** |
| | Does regulations allow use of tracing apps? | Bills and resolution adopted worldwide regarding Apps to comply with existing regulations. | | |
| | Legislation for Tracing Apps? | Most of global legislative structures like HIPPA, GDPR and WHO allow use of digital tools during emergency. | | |
| Fairness | Only adequate, relevant and limited data is collected? | Personal information (like name, mobile number, email, location, gender, date of birth etc) was collected and shared with 3rd parties.<br>Information can help to uniquely identify any person. | 1 | **Medium** |
| | Kept no longer than req | Varied results found regarding data deletion and retention in each country. | | |

| | | | | |
|---|---|---|---|---|
| Transparency | User rights | The apps provided either limited or no access to user for controlling their data. Whereas most of the international regulations provide various rights to users regarding privacy e.g. as per GDPR, individual has the rights to access personal data. Additionally, they have the right to know or being informed that how their data is being collected, used, stored, processed, and being shared with whom. | 1 | **Medium** |
| | Does the apps mentioned purpose of processing other than required? | The apps claimed that data will be used for public health safety. | | |
| | Lawful basis | Most of the apps specially GPS-based tracked, captured location data, time of contact with positive case and broadcasted as well, which invades individuals' privacy. The continuous tracking including international travelling was criticised worldwide as it was taken as an attempt by the governments to regulate public lives and privacy breach of fundamental rights | | |
| | Public interest | Apps were developed in public interest. | | |
| | Notifications | Partially implemented. | | |
| Purpose limitation | Specify the purpose(s) for which personal information is collected, processed and stored. | Mentioned purpose of tracing positive cases, identify suspect in proximity and analyse disease trends. | 3 | **Normal** |
| Data Minimization | Collect only what is required. | During the installation and registration process, the apps asked for personal information (like name, mobile number, email, location, gender, date of birth etc) and also asked for permissions to GPS, camera, microphone, Bluetooth etc. Access to this information can | 1 | **Medium** |

| | | | | |
|---|---|---|---|---|
| | | help to uniquely identify any person which is a high concern of individual's privacy. Although WHO instructed to collect minimum data for use of public health only while ensuring privacy, however, same was truly adhered. | | |
| Retention | Data Deletion Timeline (indefinite period, time limit or until action completed) | In most of the apps there is no mention of data retention period and deletion after use at the end of pandemic. | 0 | **High** |
| | Can user request the data deletion? | GDPR gives user right to be forgotten under which their data may be deleted. Similarly, user can withdraw consent regarding data usage. Limited apps provided data deletion option; however, it was not transparent. | | |
| | Decommissioning of App | Few apps have been removed from the app stores, however, decommissioning procedure was lacking. | | |
| Integrity and confidentiality | Data encryption and Anonymity | Few apps claimed that data is encrypted and transferred over a secure connection. However, there is no evidence that identifiers were removed during the data processing or sharing, and data was completely anonymised as per privacy laws | 1 | **Medium** |
| | Access Control | As per survey and analysis of models used by various apps, it has been noted that centralised architecture has been adopted mostly. However, single database is not only more vulnerable to breaches but access to complete data to authorities is also matter of high privacy concerns | | |
| Accountability | Audits | No audit mechanism was mentioned regarding the collected data, its processing and storage. | 0 | **High** |

| | | | | |
|---|---|---|---|---|
| Data Transfer and Sharing | Data Sharing | Appropriate security and privacy measures were not in place for data transmission from user to databases.<br>Moreover, in most of the apps, users have not been informed that with whom their data is being shared and for what purpose. Under international privacy laws users must be informed about once their data is shared.<br>Moreover, there was no assurance like data is only being shared and processed to control the pandemic and will not be used for any other purpose.<br>Few apps mentioned that data will be shared with private setups, however, further details were missing. | 1 | **Medium** |
| | Third Party API's | Another privacy concern is using of third-party APIs by apps as they may reach the data.<br>Personal information access from Google and Apple API's also raised privacy concerns.<br>Mentioning of governance processes to ensure data protection while sharing with 3rd parties was missing. | | |
| | Secondary Use | Clarity regarding data sharing for clinical research, public health Surveillance, industrial or administrative purpose was missing. | | |
| Architecture | Centralised | As per available data, 61% Apps used centralised model where data was managed on central server. | 2 | **Low** |
| | De-centralised | 26% apps were designed on decentralised model where processing and storage was carried out on users' mobile device. | | |
| | Hybrid | Only 13% used Hybrid Model. | | |
| Tracing Method | Location Data Collection | 21% apps used GPS to collect location data which was used to track positive cases, identify | 1 | **Medium** |

| | | | | |
|---|---|---|---|---|
| | | covid clusters and movement profiles. | | |
| | Proximity | 37% apps used Bluetooth protocol to to sense neighbouring devices and proximity estimation. | | |
| | Mobile Operators | No verified data is available, however as per available literature there are incidents where contact tracing was performed using base-station level information provided by cellular companies. | | |
| Development Sponsorship | Government | As per the available data, 72% of the Apps were sponsored by the Governments. | 1 | **Medium** |
| | Private | 9% Apps were developed by private developers. | | |
| | Multi-stakeholders | 19% were developed with the effort of multi stakeholders. | | |
| Usage | Mandatory | Out of available data, 26% countries made the usage of app mandatory, however, few made voluntary at later stage. | 2 | **Low** |
| | Voluntary (Opt-in/ Opt-Out) | 74% countries made usage of app on voluntary bases and provided Opt-In and Opt-Out options to users. | | |

## 6.10 Recommendations

### 6.10.1 Mandatory Data Privacy Policy

International regulations, WHO, governments and relevant health authorities must make data privacy policies mandatory for such apps. Appropriate measures must be taken to ensure that it is available to public on app store in easy and understandable language. App stores may also made apps available once the fulfil the requirement.

### 6.10.2 Consent Withdrawal

It enables the user to stop participating in data sharing. Under regulations, it also provides surety that users can delete their data whenever they want. Therefore, all tracing apps must incorporate electronic consent withdrawal feature which should enable the user to withdraw consent during data collection stage and later on after uploading on server.

### 6.10.3 Lawfulness, Fairness and Transparency

The privacy concerns raised by public are very genuine regarding the type of data being collected from the mobile phones and its utilization including further sharing with various parties. This warrants lawful data handling and taking measure to make it transparent. To achieve this, options like making source code open can be considered. It will not only help to improve the code through analysis and scrutiny by researchers but also raise public trust. Other useful options include periodic reviews of apps by independent test and verification committees and third-party audits for compliance testing. Legislative guarantees against the misuse of collected data by authorities and complete transparency can increase the adoption rate significantly.

### 6.10.4 Data Minimization

As per Article 25(2) of GDPR, only necessary data for a particular purpose should be collected and used, and there must be limits on data processing and retention period. Therefore, special safeguards must be in place to ensure that only minimum data is collected which is essentially required to handle any disaster and should not be used outside the realm of public health.

### 6.10.5 Decommissioning of Apps

Authorities must put in place a review and exit strategy to decommission apps which are no more required. In disasters like COVID-19, basing on circumstances WHO can also issue advisory for decommissioning of all tracing apps after the pandemic is over. Moreover,

independent committees can also establish data deletion timelines after which users' data be removed from the servers.

### 6.10.6 Privacy-Preserving

Blockchain technology has surfaced which maintain anonymity and immutability thus proved as reliable an immutable ledger. Moreover, pseudonymization must become the default for all such projects. Cryptographic processes be used to generate pseudonymous identifiers, which can be exchanged through Bluetooth across the users' device. Risk like physical tracking and linkage attacks can be reduced by time-bound renewal.

### 6.10.7 Decentralised Architecture

It has been noted that every architecture certain benefits and issue as well. However, research on decentralized models to enable privacy-preserving data sharing between user devices should be pursued. However, in case centralised models are adopted than data protection by design and data minimization should be greatly considered without user identification and inferring information about it.

### 6.10.8 Data Access and Control Policies

In the centralised model adopted by most of the countries, a central trusted server is responsible for storing personal information of uses and managing security keys for encryption/decryption of TempIDs. However, in case of compromise, this design has implied risk of data theft. To ensure security and privacy, proper authentication and access control mechanisms must be in place. All type of information shared between the server, user's mobile phones and health care officials should be transmitted though secure medium and accessible to authorised only.

### 6.10.9 Secondary Use

Privacy policies must explicitly and directly address the concern. Public must be informed about the secondary use of their data by researchers, health care authorities along with purpose. However, data access and control policies, anonymization and de-identification of data merit special attention by governments and health care authorities. This complete process will bring transparency and build public trust. Wide public awareness campaigns through suitable organizations regarding benefits of secondary use of data can pay back as well.

### 6.10.10 Privacy by Design

The range of privacy concerns raised by users can be addressed if governments, public health authorities, policy makers and app developers adopt privacy by design for such apps. It can be achieved by applying certain design strategies like data minimization (only minimal necessary personal information is collected), hiding (data confidentiality by encryption, pseudonymisation or anonymising the data in transit or in storage), separation (storage and processing of personal information in a distributed way), transparency (informing user which data is being collected and processed and for what purpose), user control (user should be able to access, alter and delete personal data), and compliance to piracy policies.

### 6.10.11 Formulation of Independent Committees

Independent committees with representatives from government, health authorities, legal and IT experts (including privacy specialist) be formed to monitor the process from design, development and deployment including data governance.

### 6.10.12 Roles of Stakeholders

a. **State**. Governments and concerned authorities must ensure that privacy regulations are adhered in all aspects and privacy of citizens is respected.

b. **Healthcare Authorities**. Ensure transparency in data processing. Develop proactive strategies to handle disasters through less privacy evasion approaches.

c. **User**. Guard against privacy infringements and advocate for personal privacy protection at all forums.

# *Chapter 7*

## CONCLUSION AND FUTURE WORK

### 7.1 Conclusion

COVID-19 affected everyone's way of life worldwide. The technological solutions played vital role in countering COVID-19 through quick tracing of infected individuals, analysing spread trend, identifying cluster and in many other ways. This research presented health systems and linked privacy challenges. This research also elucidates global regulations regarding user data privacy including their application, rights provided to users, and comprehensive discussion on keys areas regarding privacy. Additionally, an overview of privacy preserving techniques was presented, which can be effectively utilised to protect user data from breaches. Finally, approaches adopted globally to handle the pandemic were discussed. Case study of tracing apps is presented which include their scope, technologies (Bluetooth, GPS etc) used for tracking data, architectures adopted (centralised, decentralised and hybrid), government and private sponsorships, methods used, and types of data collected and concerns raised by public regarding privacy.

This research will help researchers to understand electronic health records and its challenges including in unprecedented situation like pandemics. It also provides privacy perspective of various legislative structures and help to understand various technological and privacy aspects of tracing apps used during COVID-19.

### 7.2 Future Work

- Identification of mobile phone vulnerabilities exploited for data collection by various apps used during covid.
- Operating system permissions for tracing apps.
- Open-source suitable tracing app architecture.

## BIBLIOGRPAHY


[1] US Government, “Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996),” Aug. 1996, [Online]. Available: https://www.govinfo.gov/app/details/PLAW-104publ191

[2] EUROPEAN PARLIAMENT AND OF THE COUNCIL, “EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.,” Apr. 2016.

[3] Ministry of Information Technology and Telecommunication, “Government of Pakistan National Cyber Security Policy 2021,” 2021.

[4] R. and C. Health Planning System Strengthening & Information Analysis Unit (HPSIU)- Ministry of National Health Services, “Pakistan: National Digital Health Framework (2022-2030),” 2021. [Online]. Available: http://nhsrc.pk

[5] Ministry of Information Technology and Telecommunication, “PERSONAL DATA PROTECTION BILL 2021 (DRAFT),” 2021.

[6] W. H. Organization. R. O. for Europe, “The protection of personal data in health information systems- principles and processes for public health,” World Health Organization. Regional Office for Europe, 2021.

[7] N. Akber Pradhan, A. Shahil Feroz, and S. Mairajuddin Shah, “Health Systems Approach to Ensure Quality and Safety Amid COVID-19 Pandemic in Pakistan,” *Journal of the College of Physicians and Surgeons Pakistan*, vol. 31, pp. 38–41, 2021, doi: 10.29271/jcpsp.2021.Supp.S38.

[8] R. Zakar, S. Iqbal, M. Z. Zakar, and F. Fischer, “COVID-19 and health information seeking behavior: Digital health literacy survey amongst university students in Pakistan,” *Int J Environ Res Public Health*, vol. 18, no. 8, Apr. 2021, doi: 10.3390/ijerph18084009.

[9] I. S. Rubinstein, “Big Data: The End of Privacy or a New Beginning?” [Online]. Available: http://idpl.oxfordjournals.org/

[10] S. M. Shah and R. A. Khan, “Secondary use of electronic health record: Opportunities and challenges,” *IEEE Access*, vol. 8, pp. 136947–136965, 2020, doi: 10.1109/ACCESS.2020.3011099.

[11] M. Shuaib, S. Alam, M. Shabbir Alam, and M. Shahnawaz Nasir, “Compliance with HIPAA and GDPR in blockchain-based electronic health record,” *Mater Today Proc*, Mar. 2021, doi: 10.1016/j.matpr.2021.03.059.

[12] “WHO EMRO | Health information system.”

[13] R. Haux, “Health information systems – past, present, future,” *Int J Med Inform*, vol. 75, no. 3–4, pp. 268–281, Mar. 2006, doi: 10.1016/j.ijmedinf.2005.08.002.

[14] N. Menachemi and T. H. Collum, “Benefits and drawbacks of electronic health record systems,” *Risk Manag Healthc Policy*, vol. 4, pp. 47–55, 2011, doi: 10.2147/RMHP.S12985.

[15] W. Scholarship, N. Hamade, S. Amardeep Thind, O. Joint Supervisor Amanda Terry, and G. Program in Epidemiology, “Improving the Use of Electronic Medical Records in Primary Health Care: A Systematic Review and Meta-Analysis,” 2017. [Online]. Available: https://ir.lib.uwo.ca/etdhttps://ir.lib.uwo.ca/etd/4420

[16] D. R. Posircaru and L. Dan Serbanati, “Integrating legacy medical applications in a standardized Electronic Health Record platform,” in *2015 E-Health and Bioengineering Conference (EHB)*, Nov. 2015, pp. 1–4. doi: 10.1109/EHB.2015.7391401.

[17] A. S. (Shvo), “Electronic Health Record,” in *Encyclopedia of Database Systems*, New York, NY: Springer New York, 2017, pp. 1–6. doi: 10.1007/978-1-4899-7993-3_48-3.

[18] B. Kaplan, “How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales,” *Cambridge Quarterly of Healthcare Ethics*, vol. 25, no. 2, pp. 312–329, Mar. 2016, doi: 10.1017/S0963180115000614.

[19] C. T. Lye, H. P. Forman, J. G. Daniel, and H. M. Krumholz, “The 21st Century Cures Act and electronic health records one year later: Will patients see the benefits?,” *Journal of the American Medical Informatics Association*, vol. 25, no. 9. Oxford University Press, pp. 1218–1220, Sep. 01, 2018. doi: 10.1093/jamia/ocy065.

[20] K. R. Simpson, “Electronic health records,” *MCN The American Journal of Maternal/Child Nursing*, vol. 40, no. 1. Lippincott Williams and Wilkins, p. 68, Dec. 20, 2015. doi: 10.1097/NMC.0000000000000089.

[21] J. Hemerly, “Public Policy Considerations for Data-Driven Innovation,” *Computer (Long Beach Calif)*, vol. 46, no. 6, pp. 25–31, Jun. 2013, doi: 10.1109/MC.2013.186.

[22] P. Pereira Rodrigues *et al.*, *Proceedings of CBMS 2013 Porto : 26th IEEE International Symposium on Computer-Based Medical Systems, Portugal : 20-22 June University of Porto*.

[23] G. W. Beeler, “HL7 Version 3—An object-oriented methodology for collaborative standards development1Presented at the International Medical Informatics Association Working Group 16 Conference on Standardisation in Medical Informatics—Towards International Consensus and Cooperation, Bermuda, 12 September, 1997.1,” *Int J Med Inform*, vol. 48, no. 1–3, pp. 151–161, Feb. 1998, doi: 10.1016/S1386-5056(97)00121-4.

[24] W. Moore and S. Frye, “Review of HIPAA, Part 1: History, protected health information, and privacy and security rules,” *J Nucl Med Technol*, vol. 47, no. 4, pp. 269–272, Dec. 2019, doi: 10.2967/JNMT.119.227819.

[25] M. E. Callahan, “Handbook for Safeguarding Sensitive PII Contents,” 2012. [Online]. Available: www.dhs.gov/privacywww.dhs.gov/privacy

[26] S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeau, “An introduction to privacy engineering and risk management in federal systems,” Gaithersburg, MD, Jan. 2017. doi: 10.6028/NIST.IR.8062.

[27] R. and C. Health Planning System Strengthening & Information Analysis Unit (HPSIU)- Ministry of National Health Services, “Pakistan : National Health Information System Action Plan & Provincial Roadmaps (2020-24),” 2019, [Online]. Available: http://phkh.nhsrc.pk/

[28] S. M. Cadarette and L. Wong, “An Introduction to Health Care Administrative Data,” *Can J Hosp Pharm*, vol. 68, no. 3, Jun. 2015, doi: 10.4212/cjhp.v68i3.1457.

[29] P. Coorevits *et al.*, “Electronic health records: new opportunities for clinical research,” *J Intern Med*, vol. 274, no. 6, pp. 547–560, Dec. 2013, doi: 10.1111/joim.12119.

[30] M. E. Sips, M. J. M. Bonten, and M. S. M. van Mourik, “Automated surveillance of healthcare-associated infections,” *Curr Opin Infect Dis*, vol. 30, no. 4, pp. 425–431, Aug. 2017, doi: 10.1097/QCO.0000000000000376.

[31] S. Dash, S. K. Shakyawar, M. Sharma, and S. Kaushik, “Big data in healthcare: management, analysis and future prospects,” *J Big Data*, vol. 6, no. 1, p. 54, Dec. 2019, doi: 10.1186/s40537-019-0217-0.

[32] D. Mohammed, “U.S. Healthcare Industry: Cybersecurity Regulatory and Compliance Issues,” *Journal of Research in Business, Economics and Management*, 2017, [Online]. Available: www.scitecresearch.com/journals/index.php/jrbem

[33] M. R. Fuentes, “Cybercrime and Other Threats Faced by the Healthcare Industry.”

[34] B. Edwards, S. Hofmeyr, and S. Forrest, “Hype and Heavy Tails: A Closer Look at Data Breaches.” [Online]. Available: http://docs.scipy.org/doc/scipy/reference/stats.

[35] S. Chenthara, H. Wang, and K. Ahmed, “Security and Privacy in Big Data Environment,” in *Encyclopedia of Big Data Technologies*, Cham: Springer International Publishing, 2018, pp. 1–9. doi: 10.1007/978-3-319-63962-8_245-1.

[36] U. Premarathne *et al.*, “Hybrid Cryptographic Access Control for Cloud-Based EHR Systems,” *IEEE Cloud Computing*, vol. 3, no. 4, pp. 58–64, Jul. 2016, doi: 10.1109/MCC.2016.76.

[37] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, “Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing,” *IEEE Access*, vol. 7, pp. 74361–74382, 2019, doi: 10.1109/ACCESS.2019.2919982.

[38] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, “Blockchain based searchable encryption for electronic health record sharing,” *Future Generation Computer Systems*, vol. 95, pp. 420–429, Jun. 2019, doi: 10.1016/j.future.2019.01.018.

[39] F. A. Reegu, S. Mohd, Z. Hakami, K. K. Reegu, and S. Alam, “Towards Trustworthiness of Electronic Health Record system using Blockchain,” 2021. [Online]. Available: http://annalsofrscb.ro2425

[40] U. N. G. Assembly and others, “Universal declaration of human rights,” *UN General Assembly*, vol. 302, no. 2, pp. 14–25, 1948.

[41] MehmetKayaalp, “Patient Privacy in the Era of Big Data,” *Journal*, vol. 35, no. 1, pp. 8–17, 2018.

[42] M. Meingast, T. Roosta, and S. Sastry, “Security and Privacy Issues with Health Care Information Technology,” in *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, Aug. 2006, pp. 5453–5458. doi: 10.1109/IEMBS.2006.260060.

[43] U.S. Attorney’s Office, “Former Howard University Hospital Employee Pleads Guilty to Selling Personal Information About Patients,” *District of Columbia, (202) 252-6933*, Jun. 12, 2012.

[44] N. Jamshed, F. Ozair, A. Sharma, and P. Aggarwal, “Ethical issues in electronic health records: A general overview,” *Perspect Clin Res*, vol. 6, no. 2, p. 73, 2015, doi: 10.4103/2229-3485.153997.

[45] “WHO Director-General’s opening remarks at the media briefing on COVID-19 - 11 March 2020,” Mar. 11, 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020 (accessed Jan. 07, 2023).

[46] N. Ahmed *et al.*, “A Survey of COVID-19 Contact Tracing Apps,” *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 134577–134601, 2020. doi: 10.1109/ACCESS.2020.3010226.

[47] A. R. Brough and K. D. Martin, “Consumer Privacy During (and After) the COVID-19 Pandemic,” *Journal of Public Policy & Marketing*, vol. 40, no. 1, pp. 108–110, Jan. 2021, doi: 10.1177/0743915620929999.

[48] Matt Richtel, “W.H.O. Fights a Pandemic Besides Coronavirus: An ‘Infodemic,’” *https://www.nytimes.com/2020/02/06/health/coronavirus-misinformation-social-media.html*, Feb. 06, 2020.

[49] A. R. Brough and K. D. Martin, “Consumer Privacy During (and After) the COVID-19 Pandemic,” *Journal of Public Policy & Marketing*, vol. 40, no. 1, pp. 108–110, Jan. 2021, doi: 10.1177/0743915620929999.

[50] L. Lin, I. Singapore, and T. W. Martin In Seoul, “How Coronavirus Is Eroding Privacy wsj.com/articles/coronavirus-paves-way-for-new-age-of-digital-surveillance-11586963028,” 2020. [Online]. Available: https://www.wsj.com/articles/coronavirus-paves-way-for-new-age-of-digital-surveillance-11586963028

[51] C. Lin *et al.*, “Policy Decisions and Use of Information Technology to Fight Coronavirus Disease, Taiwan,” *Emerg Infect Dis*, vol. 26, no. 7, pp. 1506–1512, Jul. 2020, doi: 10.3201/eid2607.200574.

[52] J. Labs and S. Terry, “Privacy in the Coronavirus Era,” *Genetic Testing and Molecular Biomarkers*, vol. 24, no. 9. Mary Ann Liebert Inc., pp. 535–536, Sep. 01, 2020. doi: 10.1089/gtmb.2020.29055.sjt.

[53] F. Jenny, “Economic Resilience, Globalization and Market Governance: Facing the COVID-19 Test,” *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3563076.

[54] A. Ukani, A. Mirian, and A. C. Snoeren, “Locked-in during lock-down,” in *Proceedings of the 21st ACM Internet Measurement Conference*, Nov. 2021, pp. 480–486. doi: 10.1145/3487552.3487828.

[55] M. A. Agus Purwanto Mochammad Fahlevi Abdul Mufid Eva Agistiawati Yoyok Cahyono Popong Suryani, “Impact of Work From Home (WFH) on Indonesian Teachers Performance During the Covid-19 Pandemic : An Exploratory Study,” *International Journal of Advanced Science and Technology*, vol. 29, no. 05, pp. 6235–6244, May 2020, [Online]. Available: http://sersc.org/journals/index.php/IJAST/article/view/15627

[56] A. C. L. C. B. L. Y. L. J. R. A.-M. S. A. W. Helen Beetham, “Surveillance practices, risks and responses in the post pandemic university,” *Digit Cult Educ*, vol. 14, no. 1, pp. 16–37, Feb. 2022.

[57] G. Newlands, C. Lutz, A. Tamò-Larrieux, E. F. Villaronga, R. Harasgama, and G. Scheitlin, “Innovation under pressure: Implications for data privacy during the Covid-19 pandemic,” *Big Data Soc*, vol. 7, no. 2, p. 205395172097668, Jul. 2020, doi: 10.1177/2053951720976680.

[58] D. Townsend, F. Knoefel, and R. Goubran, “Privacy versus autonomy: A tradeoff model for smart home monitoring technologies,” in *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Aug. 2011, pp. 4749–4752. doi: 10.1109/IEMBS.2011.6091176.

[59] N. Y. Philip, J. J. P. C. Rodrigues, H. Wang, S. J. Fong, and J. Chen, “Internet of Things for In-Home Health Monitoring Systems: Current Advances, Challenges and

Future Directions," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 300–310, Feb. 2021, doi: 10.1109/JSAC.2020.3042421.

[60] Y. Mekdad *et al.*, "A Survey on Security and Privacy Issues of UAVs." Jan. 2021.

[61] P. National Information Technology Board, "https://cd.nitb.gov.pk/projects/pak-negheban-app."

[62] P. National Information Technology Board, "https://nitb.gov.pk/ProjectDetail/Zjc0MWQxOTUtYWIzZC00M2UwLThhY2YtODc5NTY2N2M4MmE0," 2020.

[63] NADRA Pakistan, "https://nims.nadra.gov.pk/nims/."

[64] S. Cui and P. Qi, "The legal construction of personal information protection and privacy under the Chinese Civil Code," *Computer Law & Security Review*, vol. 41, p. 105560, Jul. 2021, doi: 10.1016/j.clsr.2021.105560.

[65] J. K. O'Herrin, N. Fost, and K. A. Kudsk, "Health Insurance Portability Accountability Act (HIPAA) Regulations," *Ann Surg*, vol. 239, no. 6, pp. 772–778, Jun. 2004, doi: 10.1097/01.sla.0000128307.98274.dc.

[66] C. J. Wang and D. J. Huang, "The HIPAA conundrum in the era of mobile health and communications," *JAMA*, vol. 310, no. 11. American Medical Association, pp. 1121–1122, Sep. 18, 2013. doi: 10.1001/jama.2013.219869.

[67] J. Pipersburgh, "The push to increase the use of EHR technology by hospitals and physicians in the United States through the HITECH Act and the Medicare incentive program.," *J Health Care Finance*, vol. 38, no. 2, pp. 54–78, 2011.

[68] N. Yaraghi and R. D. Gopal, "The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights From an Empirical Study," *Milbank Quarterly*, vol. 96, no. 1, pp. 144–166, Mar. 2018, doi: 10.1111/1468-0009.12314.

[69] P. F. Edemekong, P. Annamaraju, and M. J. Haydel, *Health Insurance Portability and Accountability Act*. 2022.

[70] E. Politou, A. Michota, E. Alepis, M. Pocs, and C. Patsakis, "Backups and the right to be forgotten in the GDPR: An uneasy relationship," *Computer Law & Security Review*, vol. 34, no. 6, pp. 1247–1257, Dec. 2018, doi: 10.1016/j.clsr.2018.08.006.

[71] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing, 2017. doi: 10.1007/978-3-319-57959-7.

[72] C. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," *Computer Law and Security Review*, vol. 34, no. 1, pp. 134–153, Feb. 2018, doi: 10.1016/j.clsr.2017.05.015.

[73] B.-J. Koops and R. Leenes, “Privacy regulation cannot be hardcoded. A critical comment on the ‘privacy by design’ provision in data-protection law,” *International Review of Law, Computers & Technology*, vol. 28, no. 2, pp. 159–171, May 2014, doi: 10.1080/13600869.2013.801589.

[74] G. Chassang, “The impact of the EU general data protection regulation on scientific research,” *Ecancermedicalscience*, vol. 11, Jan. 2017, doi: 10.3332/ecancer.2017.709.

[75] W. Presthus and K. F. Sønslien, “An analysis of violations and sanctions following the gdpr,” *International Journal of Information Systems and Project Management*, vol. 9, no. 1, pp. 38–53, 2021, doi: 10.12821/ijispm090102.

[76] J. H. Jeanette Herrle, “The Peril and Potential of the GDPR,” *Centre for International Governance Innovation*, Jul. 2019.

[77] C. Tankard, “What the GDPR means for businesses,” *Network Security*, vol. 2016, no. 6, pp. 5–8, Jun. 2016, doi: 10.1016/S1353-4858(16)30056-3.

[78] VERITAS TECHNOLOGIES, “Organizations Worldwide Fear GDPR Non-Compliance Could Put Them Out of Business,” May 2018.

[79] I. Calzada, “Citizens’ Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL),” *Smart Cities*, vol. 5, no. 3, pp. 1129–1150, Sep. 2022, doi: 10.3390/smartcities5030057.

[80] Z. He, “When data protection norms meet digital health technology: China’s regulatory approaches to health data protection,” *Computer Law & Security Review*, vol. 47, p. 105758, Nov. 2022, doi: 10.1016/j.clsr.2022.105758.

[81] L. M. Austin, “Is Consent the Foundation of Fair Information Practices Canada’s Experience under Pipeda,” *U. Toronto LJ*, vol. 56, p. 181, 2006.

[82] T. Piper, “The Personal Information Protection and Electronic Documents Act-A Lost Opportunity to Democratize Canada’s Technological Society,” *Dalhousie LJ*, vol. 23, p. 253, 2000.

[83] The National Assembly of Pakistan, “The Constitution of the Islamic Republic of Pakistan,” 1973.

[84] National Assembly Secretariat, “Prevention of Electronic Crimes Act (PECA) – 2016,” 2016, Accessed: Jan. 24, 2023. [Online]. Available: http://www.na.gov.pk/uploads/documents/1462252100_756.pdf

[85] X. Ying, K. Pan, X. Wu, and L. Guo, “Comparisons of randomization and K-degree anonymization schemes for privacy preserving social network publishing,” in *Proceedings of the 3rd Workshop on Social Network Mining and Analysis*, Jun. 2009, pp. 1–10. doi: 10.1145/1731011.1731021.

[86] K. Rajendran, M. Jayabalan, and M. E. Rana, “A study on k-anonymity, l-diversity, and t-closeness techniques,” *IJCSNS*, vol. 17, no. 12, p. 172, 2017.

[87] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, “‘t-closeness: Privacy beyond k-anonymity and l-diversity.’ 2007 IEEE 23rd international conference on data engineering.,” *ACM Trans Knowl Discov Data*, vol. 1, no. 1, p. 3, Mar. 2007, doi: 10.1145/1217299.1217302.

[88] P. Mahajan and A. Sachdeva, “A study of encryption algorithms AES, DES and RSA for security,” *Global Journal of Computer Science and Technology*, 2013.

[89] P. C. van Oorschot, *Computer Security and the Internet*. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-83411-1.

[90] X. Yi, R. Paulet, and E. Bertino, “Homomorphic Encryption,” 2014, pp. 27–46. doi: 10.1007/978-3-319-12229-8_2.

[91] I. A. Mohammed, “Intelligent authentication for identity and access management: a review paper,” *International Journal of Managment, IT and Engineering (IJMIE)*, vol. 3, no. 1, pp. 696–705, 2013.

[92] E. Marilly, O. Martinot, S. Betgé-Brezetz, and G. Delègue, “Requirements for service level agreement management,” in *IEEE Workshop on IP Operations and Management*, 2002, pp. 57–62.

[93] W. H. Organization and others, “Contact tracing in the context of COVID-19: interim guidance, 10 May 2020,” 2020.

[94] R. K. R. Kummitha, “Smart technologies for fighting pandemics: The techno-and human-driven approaches in controlling the virus transmission,” *Gov Inf Q*, vol. 37, no. 3, p. 101481, 2020.

[95] S. Tahir, H. Tahir, A. Sajjad, M. Rajarajan, and F. Khan, “Privacy-preserving COVID-19 contact tracing using blockchain,” *Journal of Communications and Networks*, vol. 23, no. 5, pp. 360–373, Sep. 2021, doi: 10.23919/jcn.2021.000031.

[96] J.-D. Cascón-Katchadourian, “Tecnolog\’\ias para luchar contra la pandemia Covid-19: geolocalización, rastreo, big data, SIG, inteligencia artificial y privacidad//Technologies to fight the Covid-19 pandemic: geolocation, tracking, big data, GIS, artificial intelligence, and privacy,” *Profesional de la información*, vol. 29, no. 4, 2020.

[97] J. Li and X. Guo, “COVID-19 contact-tracing apps: A survey on the global deployment and challenges,” *arXiv preprint arXiv:2005.03599*, 2020.

[98] C. Troncoso *et al.*, “Decentralized Privacy-Preserving Proximity Tracing.” [Online]. Available: https://ncs-tf.ch/en/policy-briefs/contact-tracing-strategy-

[99] E. Hernández-Orallo, C. T. Calafate, J.-C. Cano, and P. Manzoni, “Evaluating the effectiveness of COVID-19 Bluetooth-Based smartphone contact tracing applications,” *Applied Sciences*, vol. 10, no. 20, p. 7113, 2020.

[100] L. F. M. Ramos, “Evaluating privacy during the COVID-19 public health emergency: The case of facial recognition technologies,” in *ACM International Conference Proceeding Series*, Sep. 2020, pp. 176–179. doi: 10.1145/3428502.3428526.

[101] A. Akinbi, M. Forshaw, and V. Blinkhorn, “Contact tracing apps for the COVID-19 pandemic: a systematic literature review of challenges and future directions for neo-liberal societies,” *Health Inf Sci Syst*, vol. 9, no. 1, p. 18, Dec. 2021, doi: 10.1007/s13755-021-00147-7.

[102] A. Anglemyer *et al.*, “Digital contact tracing technologies in epidemics: a rapid review,” *Cochrane Database of Systematic Reviews*, vol. 2020, no. 8, Aug. 2020, doi: 10.1002/14651858.CD013699.

[103] J. Li and X. Guo, “Global deployment mappings and challenges of contact-tracing apps for COVID-19,” *Available at SSRN 3609516*, 2020.

[104] D. J. Leith and S. Farrell, “Contact tracing app privacy: What data is shared by europe’s gaen contact tracing apps,” in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*, 2021, pp. 1–10.

[105] C. Monroe, F. Tazi, and S. Das, “Location Data and COVID-19 Contact Tracing: How Data Privacy Regulations and Cell Service Providers Work In Tandem”, doi: 10.14722/usec.2021.23010.

[106] S. Altmann *et al.*, “Acceptability of app-based contact tracing for COVID-19: Cross-country survey study,” *JMIR Mhealth Uhealth*, vol. 8, no. 8, p. e19857, 2020.

[107] M. E. O’Callaghan *et al.*, “A national survey of attitudes to COVID-19 digital contact tracing in the Republic of Ireland,” *Irish Journal of Medical Science (1971-)*, vol. 190, no. 3, pp. 863–887, 2021.

[108] S. Abuhammad, O. F. Khabour, and K. H. Alzoubi, “COVID-19 contact-tracing technology: acceptability and ethical issues of use,” *Patient Prefer Adherence*, vol. 14, p. 1639, 2020.