DRF

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

DATA PRIVACY IN PAKISTAN'S HEALTHCARE SECTOR

Acknowledgements:

This report could not have been possible without the hard work and time rendered by our research team comprising of primary researcher Zainab Durrani and research associate Zoya Hashim; the revision and editing done by the Director of Research and Policy, Shmyla Khan and Senior Research Associate, Noor Waheed, the design work by Ahsan Zahid and Talha Umar and the support of Privacy International.

We are also immensely grateful to the participants who consented to partake in this research and provided us with their valuable time and input, leading to the data that makes up the findings and analysis of this report.

February 2023

Table of Contents

Executive Summary

This research was envisioned as an inquiry into the status quo of patient privacy in Pakistan's healthcare sector. The main aim of this research is to interrogate the extent of privacy extended to patients' health data in Pakistan from the lens of safeguarding people's dignity– understanding how this data is recorded, processed and stored. The collection of data was achieved through three modes: interviews, online surveys and focus groups. Given the lack of privacy-centric regulations and legislature in the country, this was an important investigation for the Digital Rights Foundation, to build on its existing work on the intersection of health and privacy.

a) Main Objectives

- Map, document and analyze current healthcare data privacy practices in Pakistan.
- Understand and record healthcare professionals' personal practices regarding patient data and practices maintained by medical institutions across Pakistan.
- Investigate patients' experience with healthcare service providers and their medical data privacy processes, policies and protocols.
- Understand the policies and protocols in place for ensuring patient and healthcare professional data privacy in Pakistan.
- Map and analyze the use of technology in healthcare provision.
- Explore avenues of change through feedback from patients and healthcare professionals that can positively impact the current data collection and privacy situation.

a) Key Findings

- There is a significant lack of importance given to patients' data privacy within the healthcare sector in Pakistan, as evidenced by structured conversations with medical practitioners and patients alike.
- Telehealth is a useful avenue for health services provision, especially in remote areas, however, the lack of telemedicine regulations exacerbate existing unaccounted data breaches.
- Overall, both private and public medical facilities lack policies pertaining to patients' health data.
- Limited training on medical ethics is provided to medical practitioners during their education. Very few received on-the-job training or guidelines regarding treatment of patient data.
- Majority of the medical practitioner respondents felt that their data was safe, but not private.

Introduction

As technology progresses and global health risks continue to arise, such as the recent COVID-19 pandemic, the rise of healthcare data digitization is evident across the world. The exponential increase in the number of patients visiting healthcare institutions during the pandemic[1] and beyond has underscored for governments and medical facilities the need for digitized and accessible data. Over the years, it has been evident that the digitization of medical health records poses benefits for patients and healthcare practitioners alike. The move towards electronic health records lies in the ability to achieve increased practice efficiencies and cost savings by reducing transcription costs and errors through better access to patient data[2]. Additionally, electronic health records have reportedly resulted in improved care coordination, diagnostics, patient care and patient participation in some contexts due to better availability and centralization of data. According to a national survey of doctors in the United States, 88% report that their electronic health records produce clinical benefits for the practice and 75% of providers report that their electronic health records allow them to deliver better patient care[3].

The shift from manual bookkeeping to digitalization is more precarious in low-income countries that struggle with poor, outdated infrastructure[4]. In Pakistan, most public hospitals lack the necessary funding and investment to upgrade their systems[5]. However, there is a noticeable increase in the efforts of both public and private hospitals to digitally collect, record and store data. With these paramount shifts comes the increasingly important question of data privacy. Recent incidents of data leaks, including the regular breaches of the National Database and Registration Authority (NADRA) database[6] as well as leaks of personal data during the COVID-19 pandemic[7], indicate the urgency and importance of strong data privacy policies and practices in the country. Secondly, correlations between patient perception of data privacy and more effective patient-provider relationships have been noted as some patients rejected examinations or provided changed personal information due to confidentiality concerns for their data[8]. Further, healthcare data in the conservative legislative and cultural climate of Pakistan runs highly sensitive. Gender minorities such as transgender patients, patients with HIV and women, among many others, are at the risk of facing backlash, social ostracism and bodily harm from society on the basis of their medical information.

Unfortunately, the security of patient and healthcare personnel data in public and private hospitals in Pakistan is largely unexplored. While we know that there are no data protection laws in place, despite several draft laws since 2005, the existing privacy structures, policies and processes of hospitals, clinics and labs remain unchecked. This report aims to build on the findings of the previous study on 'The Collection and Use of Health Data in Pakistan' and gauge changes in the public and private sectors' medical data processes since the seismic changes brought on by COVID-19. Further, the study investigates patients' experience with healthcare service providers and the medical data privacy processes, policies and protocols they encountered. Lastly, the report incorporates possible avenues of change in the form of recommendations, drafted through feedback from patients and healthcare professionals, that can positively impact the current data collection and state of privacy in Pakistan[9].

Methodology

The research study employed qualitative research methods to understand and map healthcare data privacy processes in Pakistan. The study collected data and examined the responses of participants who either belong to the medical community in Pakistan or those who have received treatment and/or other services from the first category of participants. Participants belonging to the medical community included healthcare professionals, nurses, doctors, clinical administration and clerical staff. Both public and private healthcare service providers were used to gather primary data for the study. In-depth interviews, qualitative surveys with open and close-ended questions, focus groups and noted instances of privacy violations were used to glean the optimum picture of the state of the industry.

The data collected using in-depth interviews, qualitative surveys, focus groups and news reports was essential in filling the gaps in knowledge regarding patient data privacy in the healthcare industry in Pakistan. Validating data collected in the previous report, these tools and sample sets enabled us to delve deeper into data healthcare privacy and practices regarding the data of both patients and healthcare service providers.

Additionally, all the data collected in the course of creating this report was kept confidential under the guidelines of DRF's internal 'Research Privacy Policy' which details that all personally identifiable information contained in the data collected for the report be kept separate from the final data set to ensure the anonymity of the participants.

Interviews

A total of 17 in-depth interviews were conducted, 14 of which were with medical practitioners over the virtual video-call platform, Zoom. Each interview lasted approximately 45 minutes on average with 7 women and 7 men between June and September 2022. The interviews were semi-structured and designed to allow healthcare practitioners to share detailed accounts of their perspectives and experiences within the medical profession.

These 17 participants also included 2 public officials, Dr. Rana Safdar and Dr. Faisal Sultan. Dr. Safdar is the lead epidemiologist for the Government of Pakistan at the time of publication. Dr. Sultan was the former special assistant to the Prime Minister on National Health Services from August 2020 to April 2022 and previously served as the Chief Executive Officer for the Shaukat Khanum Memorial Cancer Hospital and Research Center from 2003 to 2020. Lastly, one key informant included a staff member at a male Health Center who provided insights into the privacy of sensitive data.

Survey

Two sets of surveys were developed and circulated among healthcare networks and filled voluntarily. The first, Survey A, collected information from patients on their experience with healthcare data privacy and had 64 responses consisting of 30 self-identified women, 13 self-identified men and 21 patients who preferred not to identify their gender. The survey respondents were from different cities across Pakistan, but concentrated in Punjab with 61.3% of the responses coming in from this region. The second survey, Survey B, collected information and experiences from healthcare professionals on practices they, and their place of employment, have regarding data privacy. The survey collected 85 responses, of which 44 women, 34 men, 2 non-binary and 5 respondents who did not identify their gender, participated from different cities across Pakistan, mostly concentrated in the province of Punjab.

Table 1: Breakdown of Cities in the Study for Survey A

Area/City	Number of Participants
Lakki Marwat, Khyber Pakhtunkhwa	1
Karachi, Sindh	6
Lahore, Punjab	16
Rawalpindi, Punjab	4
Mardan, Khyber Pakhtunkhwa	2
Layyah, Punjab	2
Punjab	3
Khyber Pakhtunkhwa	1
Islamabad	5
Azad Kashmir	1
Multan, Punjab	1
Sheikhupura, Punjab	1
Hub, Balochistan	1
N/A	20

Table 2: Breakdown of Cities in the Study for Survey B

Area/City	Number of Participants
Islamabad	5
Karachi, Sindh	10
Kasur, Punjab	1
Kharian, Punjab	1
Kohat, Khyber Pakhtunkhwa	1
Lahore, Punjab	40
Multan, Punjab	1
Mansehra, Khyber Pakhtunkhwa	1
Mianwali, Punjab	1
Nowshera, Khyber Pakhtunkhwa	2
Peshawar, Khyber Pakhtunkhwa	2
Quetta, Balochistan	1
Rahim Yar Khan, Punjab	1
Rawalpindi, Punjab	3
Renala Khurd dist. Okara, Punjab	1

Focus Groups

4 focus groups were conducted via Zoom in September and October 2022 with different stakeholders, including medical personnel such as doctors, nurses, lady health workers, hospital management, administration staff and other staff members working at medical labs. Each focus group had an average of 3 participants. The focus groups discussed the current state of data collection and privacy processes and policies. Further, the healthcare professionals also shared their recommendations on the necessary changes to improve patient privacy. The focus group discussions had 11 participants in total, consisting specifically of 7 women and 4 men. These participants were spread across 3 provinces, Punjab, Khyber Pakhtunkhwa and Balochistan.

Participants in the focus group were asked a series of semi-structured questions that explored the medical professionals' attitudes towards data privacy. They were asked to rate the importance of data privacy on a scale of 1-10, their experience of the actual state of privacy, and what changes they believe are necessary to improve patient privacy. Furthermore, participants were asked if there were any recorded instances of breach of doctor-patient confidentiality in their knowledge or experience, the consequences of such a breach and lastly, if they were a patient at their own medical facility, how comfortable would they feel sharing their personal information.

Privacy Breaches

To take a more comprehensive look at individual instances of misuse of patient data, this research analyzed a public YouTube video[10] posted by a content creator, Wajih Uddin, who has a following of 55,000 on the platform. In this video, Wajih conducted an hour-long interview with a doctor on his experience with gender and sexual minorities. The doctor in question stated that he has been working with patients, who he revealed to be sexual minorities. He further stated that he considers identifying as a gender and sexual minority a sin. In the course of the interview, the doctor refrains from revealing the identity of his patients, not out of respect for their privacy, but to allow more patients to come and share their so-called 'disease' and personal problems with him. This video was included in the research as a case study after it was reported by transgender activists to the Digital Rights Foundation's Cyber Harassment Helpline and was deemed representative of the unique problems and vulnerabilities faced by gender minorities in healthcare.

The attitudes expressed by this doctor shows that when it comes to access to healthcare services by marginalized communities, medical ethics and patient privacy is often sacrificed at the altar of individual and societal perceptions of who "deserves" privacy and who doesn't.

There have also been instances of structural breaches of privacy, in 2016 it was reported that an employee had stolen patient data[11]. The chief security officer at the hospital in question said it could not be determined exactly how much data was stolen exactly but that it could be assumed to be a considerable amount as the theft had taken place for over four years before the complaint was filed with the police. "This information can be used against them and the hospital. The patients who were treated at the hospital can be blackmailed," said the hospital representative, citing it to be the driving force behind getting the help of the police.

Another noted example of patient privacy being abused is when Pakistan's COVID-19 'patient-zero' was recklessly reported when the pandemic hit the country in 2020. It was reported that "on February 26 [2020], hours before Pakistan's health authorities confirmed the country's first coronavirus case, the patient's photograph and personal details, including his home address, were leaked on social media[12]." The affected patient shared his experience once recovered and likened himself to a pariah in society's eyes. The impact of being exposed to national attention for his diagnosis was inherently negative[13] and one that caused problems for him as well as his family, presumably due to the social stigmatization surrounding the disease that was rampant at the initial stages of the pandemic. His was not the only instance of a COVID-19 diagnosis being leaked as in the weeks following many other patients also faced the same situation.

In March 2020, Balochistan Voices reported[14] that an Excel sheet containing patient data including their names, phone numbers, addresses, ages and 'other identity-specific information' was leaked. This information was shared widely on Whatsapp groups and was compiled by the Covid-19 Cell at the Directorate General of Health department. It was regularly shared with other departments which is what was cited as the possible reason for the leak:

'An official of the health department [who] requested not to be named, said that it's beyond comprehension why all the cells and committees ask for this private data of the patients in the first place. The data about the number of the patients and their location should be enough for these cells, claimed the official.'

These are just some of the cases of data privacy violations in the health sector that have been reported, highlighting the nonchalant attitude shown by the medical fraternity and medical administration in Pakistan. This underscores the immediate need for revision of existing guidelines and the creation of holistic and stringent measures to curtail the spread of confidential patient data.

Limitations

The study's limitations included limited geographic reach, time, access, and participant availability. As the research team is primarily based in Lahore, Punjab, the networks developed and created are in the Punjab province, thus most of the data collected was Punjab-centric and lacked regional diversity, though was not completely devoid of it. The second limitation was the lack of time to expand the methodology to include more healthcare professionals and patients. Notedly, the healthcare sector is a heavily under-resourced sector in Pakistan and thus, while we were able to hold an average of 45-minute interviews with each healthcare professional, there was a lack of access with the interviewees given the other constraints on their time.

Literature Review

a) Digitization of Healthcare Data/Telehealth

With the use of telehealth rising globally, the COVID-19 pandemic accelerated Pakistan's use of digital systems for healthcare services. Dr. Mir, a public health specialist working for the Population Council Islamabad, stated that the pressure COVID-19 brought on the healthcare sector enabled the introduction of technology in the industry, including "mobile devices, health information technology, telehealth, and telemedicine[15]." It is stated that new avenues of telemedicine were introduced at the beginning of the pandemic when isolation and social distancing were mandated, and physical access to public institutions was risky due to the possibility of infection. Some private sector organizations, namely the Society of Obstetricians and Gynecologists of Pakistan (SOGP), Aman Foundation, the Population Council, and the United Nations Population Fund (UNFPA), collectively mobilized to introduce telemedicine to combat the lack of safe access to healthcare services and battle mass misinformation in a critical global health crisis. This includes "launching a helpline for women and men to consult qualified healthcare providers on a range of reproductive health issues... [and] how women could protect themselves during the pandemic and what pregnant women should do to deliver safely."

Taking into account the cultural context of Pakistan and the corresponding sensitivity of women's medical issues, the services do not state the safeguards in place to protect the confidentiality of their data. Dr. Mir, in the article he authored, also mentions how some private and public hospitals have started providing at-home healthcare through telemedicine. The article includes suggestions to strengthen technology within healthcare, however, does not take into account data privacy, sensitive data, or mechanisms of collecting and storing data when dealing with telemedicine.

Moreover, telemedicine is being specifically used to cater to antenatal care and maternal health concerns for female patients in general and especially those from rural areas that either lack proper access to healthcare institutions or face other social barriers that prevent them from availing such services[16]. Some services often include "blood pressure monitors, blood glucose testing, and home-based fetal monitors. It not only monitors a patient's health and aids in reducing multiple antenatal and postnatal visits but can also be used to gauge whether a patient has breached the high-risk threshold and determine the need for immediate medical care[17]." In 2020, the government, in collaboration with the World Health Organisation (WHO), launched a 'Whatsapp Corona Helpline', another example of the use of telemedicine during COVID-19[18]. The aim of the WhatsApp-based helpline was to disseminate the latest updates and information from the WHO and government authorities to the masses. The users could send a 'Hi' text message to the designated number, and the automated chat box responded with a number of options, including one in which the service would answer medical queries posed to it. A similar service[19] was launched on Facebook's Messenger app in collaboration with the WHO where "[the chatbox] will recommend testing based on questions such as "Do you have a fever above a 100?", "Do you have a cough?", "Have you traveled in the last 14 days?" or "Do you have any pre-existing conditions?"

In 2016, NADRA launched e-cards, which function as personal identification cards, and launched an e-health service to ensure computerized, simpler and more accessible administrative procedures, aiming for "reduced participant misuse of resources" regarding insurance money[20]. According to NADRA , the e-cards facilitate "data verification and approval management provisioning data identification, storage and verification of identities" for treatment facilities, healthcare providers and insurance companies to provide better services. The official NADRA website states vaguely that "[d]octors have access to the database and the cards have data encryption ",[21] but lacks any specification on which doctors have access, which insurance companies are accessing and utilizing the data, and whether e-cards are used in private or public health facilities. Digital data collection and storage with this program has catered to 3.1 million underprivileged families already with no transparency regarding the privacy of patients who avail these services[22]. There have been reported efforts to digitize health data in the private sector, but none so far in the public sector.

In the private sector, digital health has been the subject of many projects in recent times. Most notably, Agha Khan Hospital, COMSATS, Sehat Kahani, doctHERs and Oladoc have integrated e-health in the form of telemedicine and digital information systems that increase access to remote areas, generate more data analytics, and provide more streamlined administrative processes in general [23]. Each private institution mentioned above caters to its own clientele, and as there are no overarching laws governing data privacy, thus each of them operate at their own discretion. Within the public sector, initiatives towards digitization of the health sector include pilot programs like the POMS (PIERS on the Move) health app tested between 2014-2016, to assess the utility and benefits of e-health technology in assisting Lady Health Workers (LHWs) in Pakistan to build knowledge and self-efficacy related to caring for women with pre-eclampsia .[24]

However, it should be noted that donor-driven telemedicine projects come with their own drawbacks. A common critique is that donor-driven projects are usually short-term and targeted towards certain development objectives. Upon the completion of the project, there is often little follow-up or attempts to sustain the work. Oftentimes the lack of funding and oversight means that the newly implemented or tested technology or medical practice is discarded. Presently, there is a paucity of data regarding whether most private or donor-funded projects remain in practice.

b) Existing safeguards to patient health information

Pakistan's healthcare sector is aptly described as “a mix of government infrastructure, parastatal healthcare, the private sector, civil society, and charitable contributions[25].” As noted earlier, apart from the Prevention of Electronic Crimes Act (PECA) 2016, there are no laws for data privacy in Pakistan, let alone health data privacy [26]. However, some ethical codes and charters have been developed in the area of healthcare data privacy. ‘Pakistan: Need for Statutory Safeguards as to Privacy of Health Information’ details Pakistan’s existing legal requirements with regard to patient privacy. The paper looks at 2 sets of guidelines and charters. The first is the ‘Code of Ethics’ published by the Pakistan Medical and Dental Council (PM&DC) in 1970 [27]. It establishes the patient's right to privacy and directs all practitioners to take an oath of confidentiality. Further, it says that "the state has no right to demand information from the doctor about his patient, save when some notification is required by statute such as in the case of communicable diseases." This can be reasonably interpreted as that apart from pandemics like COVID-19 or localized health emergencies like dengue, the PMDC, a statutory regulatory authority, maintains that even the state has no right to patient information.

The second is Healthcare Commissions' regulatory oversight in Punjab, Sindh, and Khyber Pakhtunkhwa. Only the Punjab unit, Punjab Health Commission (PHC), constituted a 'Charter for Rights and Responsibilities', that directly addresses data privacy in the healthcare industry "Personal health information to be kept secure and confidential," and "[b]e treated in privacy and dignity... including but not limited to, taking history, examination or adopting any other course of action[28]." However, further on, the charter gives the healthcare provider liberty by stating that they can "[m]aintain and utilize the data collected from patient... for the purposes of improving the healthcare services/systems[29]." Lastly, the article takes care to mention that these are merely charters and not binding statutory rights that give patients any autonomy over their own personal data.

Kazim, a researcher from the University of Utrecht, critiques these codes, saying that "[t]he language used in the codes is ambiguous that can have different interpretations and there is no legal support from the civil law of the country[30]." These codes are more akin to a self-regulatory mechanism as they are independent of the government and are supposed to be managed by the practitioners themselves. Further, a research study exploring the violations of the codes and charters notes that: "Although the PMDC and PNC have made ethics education compulsory, the majority of medical and nursing institutes in the country do not teach compulsory courses in ethics or conduct formal examinations on ethics[31]." These omissions are even more alarming now that telehealth persists even after the pandemic, and "there is an increasing trend of using telehealth technologies in Pakistan in all tertiary care hospitals, because of its efficient and cost-effective means for delivering and accessing quality healthcare services and outcomes[32]."

c) Patient perception of healthcare privacy

A study conducted in the Netherlands found that although there are varying perspectives on data privacy, most patients do value the privacy of their data[33]. The study found that generally:

> *[P]atients want to have full access to their medical data and have control over who has access to it. One-third of patients in primary care want to be informed if their medical information is shared among health care professionals… Patients indicate to be more willing to share anonymised and insensitive data (e.g., limited information about their current health problem) than full current and past medical/health information including potentially sensitive problems (e.g., mental health).*[34]

Other patients not particular about the use of their data were of the opinion that everyone, including pharmaceutical and insurance companies, already had their data. They further said that they wouldn't want the quality of their healthcare to be impacted through unnecessary restrictions on their data. While these patients valued the privacy of their data, they were more concerned about their medical treatment than the potential misuse of their data.

In a study conducted in Canada to gauge patients' perception of privacy with regards to their 'Electronic Medical Records,' they found that "[m]ore than half of the interviewed patients reported that the exposure of personal information was more likely when using EMR rather than paper because of the existence of hackers, and because of the security concerns surrounding the concept of having a password to access information[35]." Canadian citizens, despite having a Privacy Act[36] in place, expressed concerns over data privacy. The patients that were not concerned with privacy reported they felt that way "because access to EMR is limited to medical personnel, protective mechanisms exist to protect the integrity and security of the EMR." Privacy concerns over patient data are prevalent and, as noted above, can be effectively counteracted with data privacy laws that ensure the patients' confidentiality of data, coupled with institutional trust.

Patient perceptions and preferences regarding their data's confidentiality within healthcare institutions in Pakistan are largely unexplored. According to Ghazanfar Saleem, a researcher on 'Patient perception regarding privacy and confidentiality: A study from the emergency department of a tertiary care hospital in Karachi, Pakistan', the majority of the patients surveyed in the study conducted at the Indus Hospital ED felt that their privacy and confidentiality was maintained, with a net positive impact on the patient-doctor relationship[37]. However, there was a percentage of people who said otherwise, with 15% of respondents indicating that they didn't provide correct personal information and 10% rejecting examination. Limitations of the study included sample bias and the fact that the nursing staff administered the survey.

While this study did not gauge patient preferences, Bushra Shirazi in 'Patient's expectations of privacy and confidentiality in Pakistan: A mixed-methods study' found that patients did not only value and expect their data to be protected but also were most comfortable sharing personal information with only the concerned medical practitioner[38]. The study by Shirazi highlights the dynamic relationship between the patient and the healthcare provider[39]. Her study found that the perception of doctors in the country is very different from Western conceptions of medical professionals and thus impacts the way they view healthcare providers,"the position of physicians as"healer" or as many patients reverently state "after God there is only you (the doctor)" indicates the pedestal on which patients place physicians, and also conveys an inherent power dynamic in the doctor patient relationship." When asked for their definition of confidentiality, one participant notably responded that it is "trusting the doctor and his team to not broadcast [information] to just about anyone." The participants' response demonstrates a lack of understanding of broader frameworks of protection and rights afforded to patients, and rests on their 'trust' in the healthcare providers.

d) Healthcare professional's treatment of data

In a study conducted with medical students from the provinces of Balochistan, Sindh, Khyber Pakhtunkhwa and Punjab, the "[r]esponses for various questions regarding the ethical issues associated with Telemedicine were recorded and it was observed that the majority of respondents (n = 347, 87.1%) either agreed or strongly agreed that there should be development of separate ethical laws regarding telemedicine[40]." Often, the importance of patient data confidentiality is realized and even acknowledged but seldom followed. A study, carried out in Islamabad, Pakistan, collected responses from healthcare professionals on informed consent regarding data collection[41]. One respondent commented that informed consent is not a necessity as the patient arrives at the hospital as a client and with the intention to "consult a doctor," while another stated that old patients' families should be notified and there are some circumstances where "it is not even possible to take consent." Other problems healthcare professionals stated that prevented them from taking informed consent included language barrier, time constraints, knowledge gap due to low literacy rate, and lastly, class-related dynamics where patients from elite classes are given protocols including informed consent while those from lower socio-economic classes are perceived to not "want any protocol regarding procedure to be followed[42]."

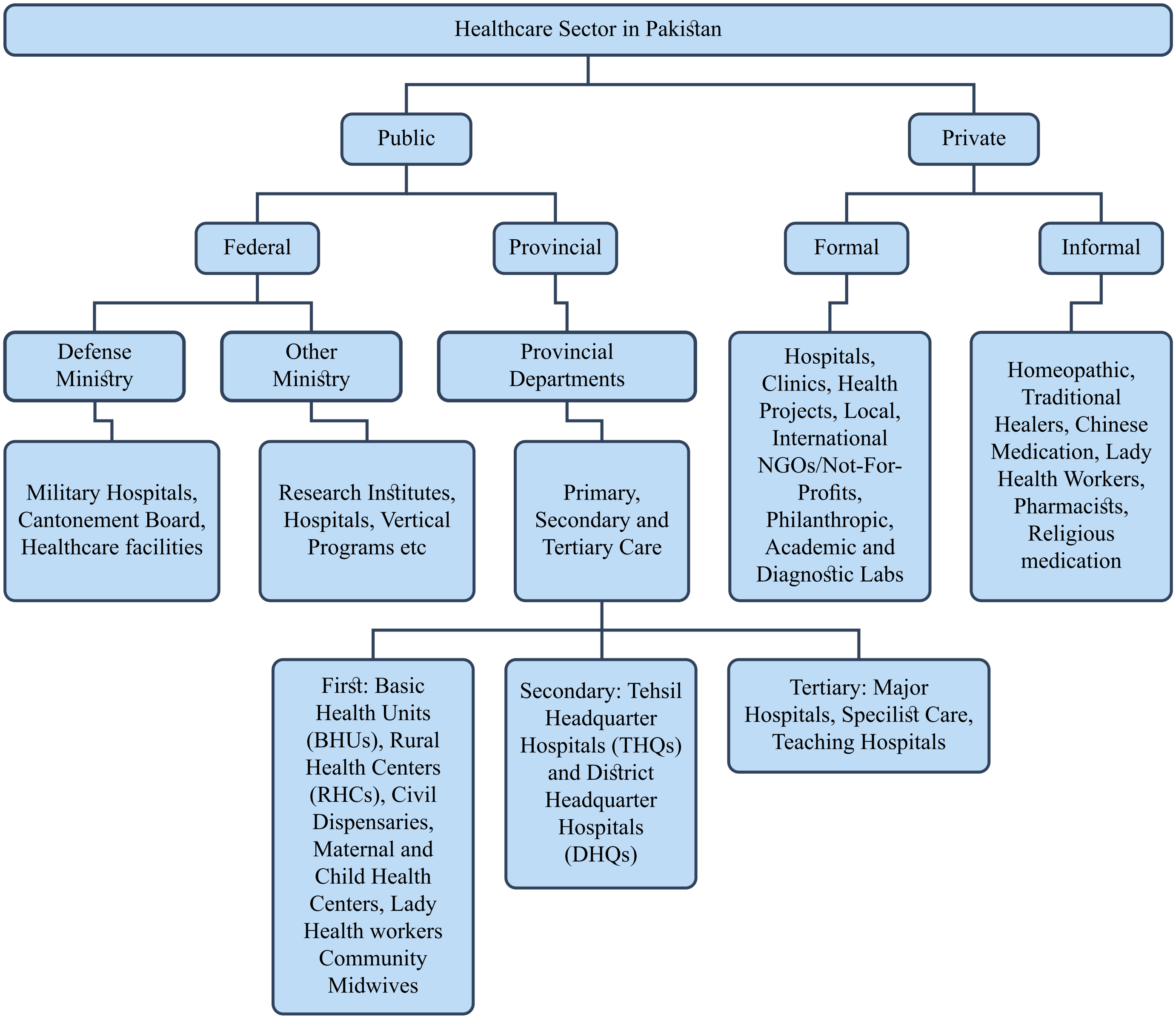
On a larger scale, the treatment of mass data by healthcare service providers and institutions such as the state can be observed during the COVID-19 pandemic. Following the WHO recommendation of employing contact tracing to limit and contain the spread of COVID-19[43], the United States, for instance, used government softwares that drew on big data analytics to identify user ID, location, vehicle, mobile phone trace, face data, transportation routes, and proximity data after an individual tested positive for the virus. By "tracing the patients activities and the roles of people around them" and requiring the patient to list 'close contacts'. Those contacts were then "tracked down, interviewed and tested" and further, put in isolation if they, too, tested positive. Some states in the US even employed cyber surveillance, utilizing smartphone data to track activity. It should be noted that Pakistan also tracked geo-spacial data from mobile phone towers early in the pandemic to alert people regarding possible exposure to the COVID-19 virus .[44]

Alternatively, in a study conducted with participants in the healthcare sectors from seven cities, namely Islamabad, Hyderabad, Lahore, Sheikhupura, Peshawar, Quetta and Mustand, the authors found "limited scope of HMIS, dubious data quality, political motives behind demand of data and an element of corruption in data reporting[45]." The study stated that the data from the Health Information Management Systems is used for a multitude of purposes, some are provided by the government and others have their own versions, often referred to by different names such as health management system, electronic medical record, etc. The study states that data collected is often in "non-use, misuse and disuse," meaning that either the data is not used or used for purposes other than treatment, ranging from justifying the need for extra resources, new procedures, and keeping track of the number of patients per disease. The authors further explain that strong initiatives need to be taken politically and administratively, including suitable legislation and capacity building within the healthcare sector, for health management information systems to function with some degree of transparency.

Moreover, even with legal frameworks in place, the advent of technology has left many professionals uncertain about the ethics of dealing with an online environment. In a study conducted in Australia, the researchers found that with increasing communication over social media platforms, ethical dilemmas arose in which some doctors were unsure about how to respond to approaches by patients through digital forums, "[d]octors were concerned about legal issues when communicating with patients online and reported that privacy and legal concerns were driving their reluctance to participate more fully in social media[46]." For example, when doctors were asked how they would respond to a friend request from a patient on Facebook, most said they would decline the request, while some said they would accept it. Many healthcare professionals are taking steps to adapt to these changes in the absence of any proper ethical guidelines. With regards to the healthcare professionals' own data privacy, "Most participants (110/181, 60.8%) reported they would not be comfortable interacting with a patient who had accessed personal information about them online prior to the consultation and 17.1% (31/181) of participants had experienced someone else posting information online about them, which they would not want patients to see "[47]and some participants said they had encountered patients who had access to information about them that was not made professionally available.

Further, when it comes to using digital platforms, "[d]octors are uncertain of patient expectations, and of their ethical and legal obligations when using online communication[48] ." Before the proliferation of technology in all sectors, doctors used face-to-face consultations as their primary mode of communication and service provision. The rapid introduction of social platforms that allow for virtual communication has left doctors to use "their own intuition, as new online ethical dilemmas arise" in online consultations.

Structure of Healthcare Industry in Pakistan



Healthcare Sector in Pakistan

Public

Private

Federal

Provincial

Formal

Informal

Defense Ministry

Other Ministry

Provincial Departments

Hospitals, Clinics, Health Projects, Local, International NGOs/Not-For-Profits, Philanthropic, Academic and Diagnostic Labs

Homeopathic, Traditional Healers, Chinese Medication, Lady Health Workers, Pharmacists, Religious medication

Military Hospitals, Cantonement Board, Healthcare facilities

Research Institutes, Hospitals, Vertical Programs etc

Primary, Secondary and Tertiary Care

First: Basic Health Units (BHUs), Rural Health Centers (RHCs), Civil Dispensaries, Maternal and Child Health Centers, Lady Health workers Community Midwives

Secondary: Tehsil Headquarter Hospitals (THQs) and District Headquarter Hospitals (DHQs)

Tertiary: Major Hospitals, Specilist Care, Teaching Hospitals

The structure of healthcare in Pakistan is broadly divided into two categories: public and private. The public sector is further divided into federal and provincial territories. The federally administered sector consists of institutions under the Defence Ministry (including military hospitals, Cantonment Board and other healthcare facilities) and civilian ministries (including research institutes, hospitals and vertical programmes). The federal structure overlooks Islamabad, Azad Jammu and Kashmir (AJK), Gilgit-Baltistan (GB) and the formerly Federally Administered Tribal Areas (FATA).

The provincial structure governs the respective provincial health departments, including primary (encompassing basic health units {BHU}, rural health centers, civil dispensaries, maternal and child health centers, lady health workers and community midwives), secondary (Tehsil Headquarter Hospitals {THQ} and District Headquarter Hospitals {DHQ}) and tertiary (major hospitals, specialist care and teaching hospitals). The provincial structure includes medical institutions in all four provinces, Punjab, Sindh, Balochistan and Khyber Pakhtunkhwa.

The private sector consists of formal and informal healthcare. Formal healthcare institutions include hospitals, clinics, healthcare projects, local and international NGOs, and philanthropic, academic and diagnostic labs. Informal healthcare institutions consist of homeopathy, traditional healers, Chinese medication, pharmacists and religious healers.

The information on this structure of Pakistan's healthcare system has been sourced through the details available on the WHO's country-wise directory on health service delivery[49] and the website[50] of the Punjab Government's Specialized Healthcare and Medical Education Department which outlines the tertiary care system in the country.

Findings and Discussion

The data collected for the study was organized, analyzed and coded by the research team at DRF into 9 main themes. The corresponding sub-themes are: (1) perception of privacy by doctors, (2) perception of privacy by patients, (3) actual state of privacy, (4) recommendations, (5) types of data collected, (6) treatment of sensitive data, (7) sharing of data, (8) treatment of data (storage and collection and access), and (9) breach of data. Further, the data was analyzed and segregated by gender to understand the gendered nature of patient data practices and their impact.

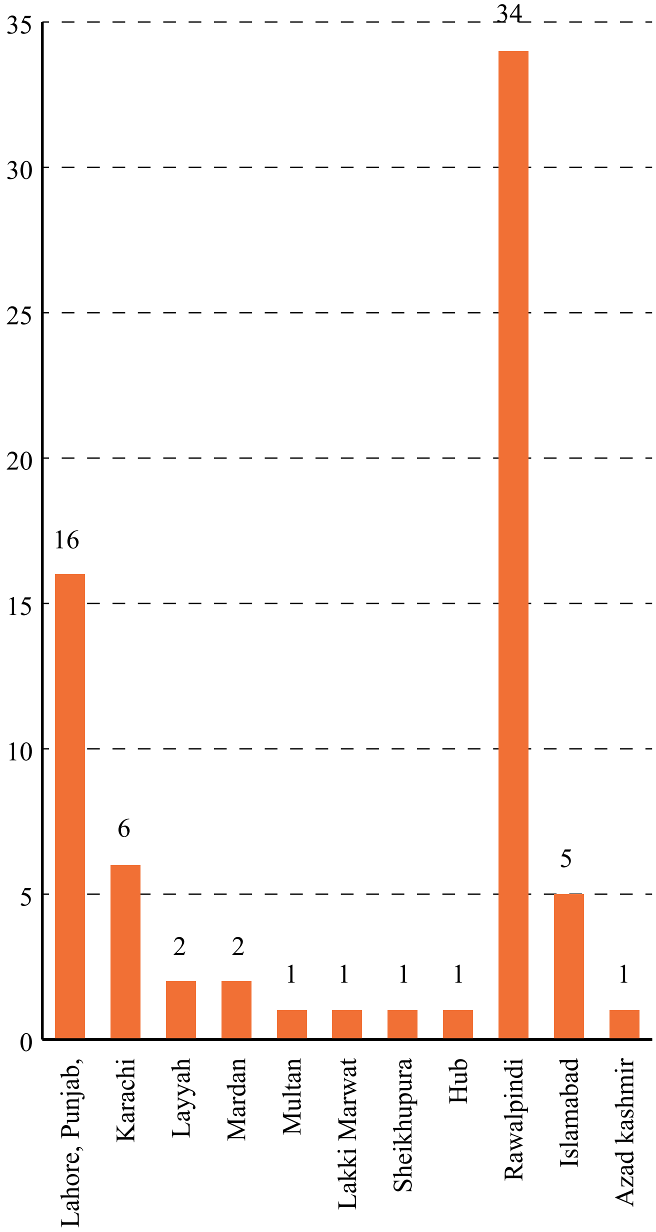
Findings from Survey A (Patient Responses):

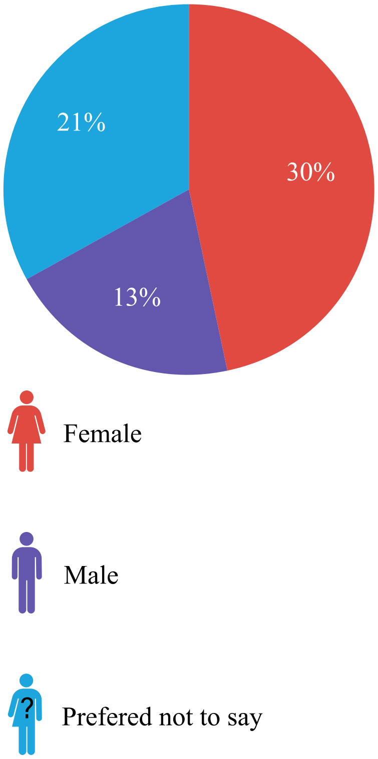
Findings from the survey responses are as follows:

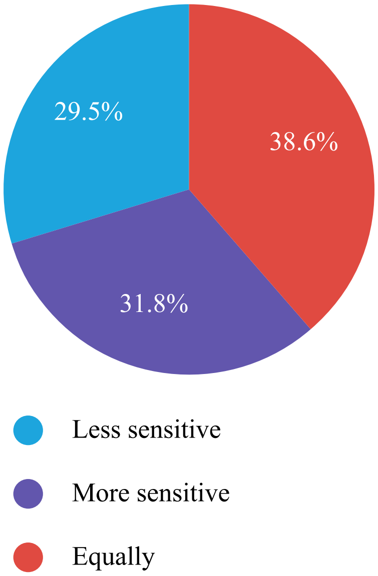
Survey A (which collected data from patients) had 64 respondents, 16 of whom were based in Lahore, Punjab, 6 in Karachi, Sindh, and the rest belonged to various cities such as Layyah, Mardan, Multan, Lakki Marwat, Sheikhupura, Rawalpindi, Islamabad, and Azad Kashmir. The ages of the respondents ranged between 19 and 59 years. 30 respondents self-identified as female, 13 as male, and 21 preferred not to say. The most popular location of availing medical treatment amongst the respondents was private hospitals, at 84.1%, followed by public hospitals at 68.2%, private clinics at 47.7% and then in descending order, Basic Health Units (BHU), Lady Health Workers (LHWs) and local clinics.

64 REPONDENTS

19 - 59 YEARS







Perception of Privacy

When asked how sensitive they considered personal health data to be compared to overall health data, 38.6% said they considered it equally important, 31.8% considered it more sensitive and 29.5% considered it less sensitive.

When asked to explain, responses ranged from patients who guarded their privacy to others who believed that data collection was necessary for service delivery. The following is a sample of responses:

a. ‘Because it’s personal data which can be used for exploitative purposes’

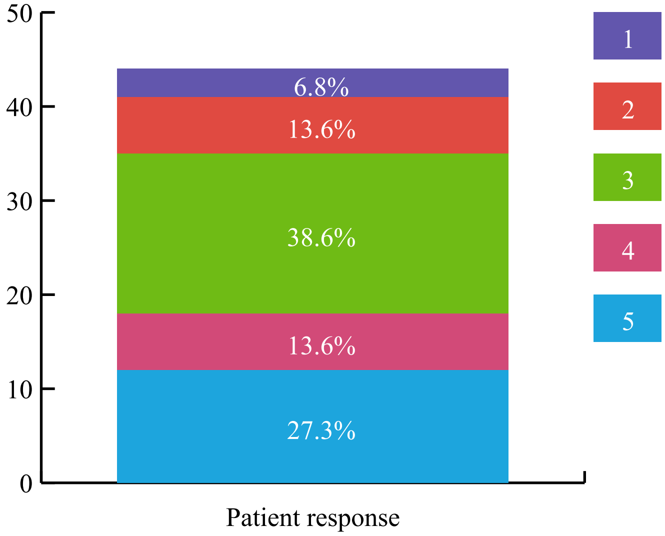
b. ‘No one wants to share their personal matters with others and I do not want that my health issues are discussed without my permission’

c. ‘It’s equally sensitive as it can help in building a data map of my life’

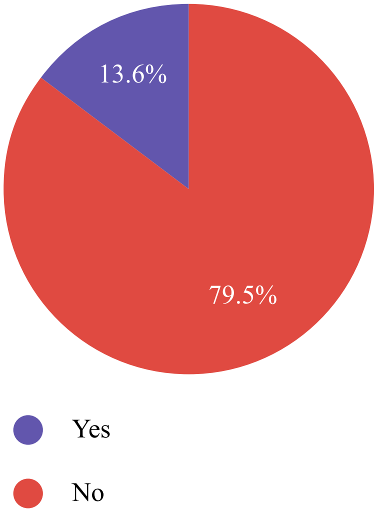
d. ‘I believe I’m comfortable sharing my health issues or health concerns with others’

e. ‘I don't think Pakistani healthcare institutions have found buyers willing to spend large amounts of money for our data YET’

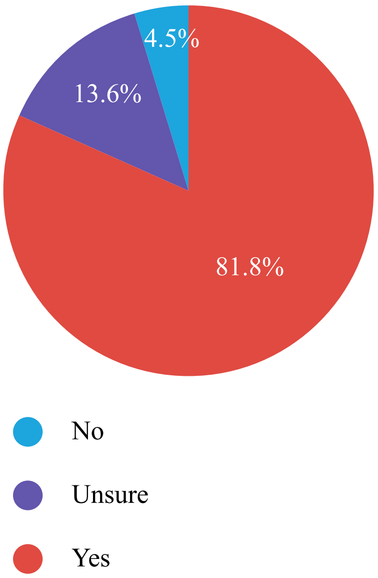
In terms of a scale-based vote of confidence regarding the safety of data in medical facilities, 27.3% of patient respondents chose the score of 5 which indicated high confidence, 13.6% chose 4 and the majority, constituting 38.6%, chose 3 as their response. This was followed by 13.6% who selected 2 and 6.8% who chose 1.



The researchers inquired if participants were more concerned about their medical data since the COVID-19 pandemic, to which 44 responses were recorded out of which 79.5% said no, they were similarly or not as concerned, 13.6% said yes, one respondent claimed they had not given much thought to this aspect however they retained a certain degree of paranoia about the pandemic and had been avoiding hospitals altogether. Lastly, we had one respondent each share that they felt their data was safe and not safe, respectively, regardless of the pandemic. The findings illustrated that for the sample group, the pandemic did not significantly impact their perceptions or concerns about privacy.



One of the main aims of this study was to determine the degree of importance respondents attached to laws and legal mechanisms for data privacy. When asked if respondents would want data protection laws for the Pakistani healthcare system (data protection laws were defined as requirements for the safety of patient data, patients confidentiality, restricted access of data to essential medical professionals, and duty not to share with a third party) an overwhelming percentage of respondents (81.8%) said yes, while 13.6% stated they were unsure and 4.5% said no. These figures indicate that patients within the Pakistani cultural and political structure value personal privacy, despite simplistic declarations otherwise–however, there is room for further research in this area.



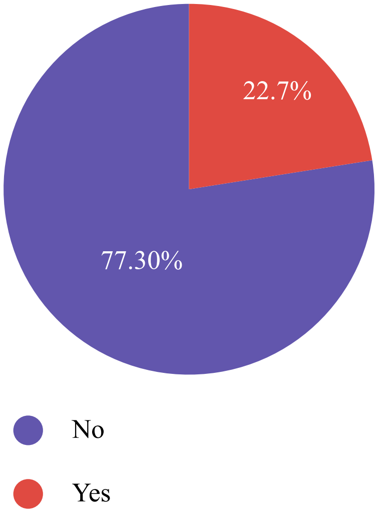
Actual State of Privacy

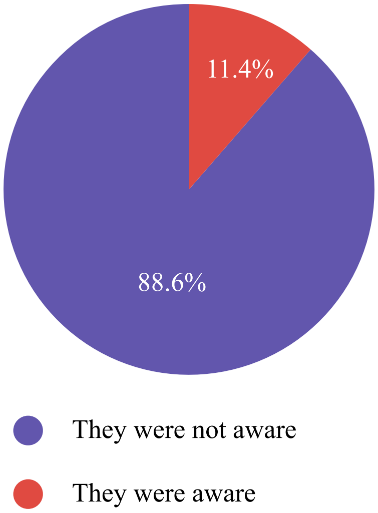
This section tallies the responses to Survey A which aimed to determine the de facto state of patient privacy in Pakistan in contrast to the perceptions and attitudes explored earlier.

When asked if there have been any instances where patients felt their medical and personal data has been leaked or used inappropriately, 77.3% said no, whereas 22.7% said yes. The instances shared by respondents could not be verified as they relied on self-reporting but one respondent shared that they had been receiving calls on their phone number 'about medication and treatments' related to past patient history. Another relayed that they had reason to believe their personal data was leaked; they shared:

> *"As soon as I took a follow-up appointment I received calls to make online payment whereas I had taken an in-person appointment [... .] Luckily I cross-checked by making a call to the department and they had no knowledge about the call."*

The researchers also inquired if the respondents knew of any existing methods of redressal or lodging a complaint in case their medical data is misused through healthcare practices. The majority (88.6%) responded that they were not aware of any mechanisms, while 11.4% said yes that they were aware of the next steps to take in such a situation.





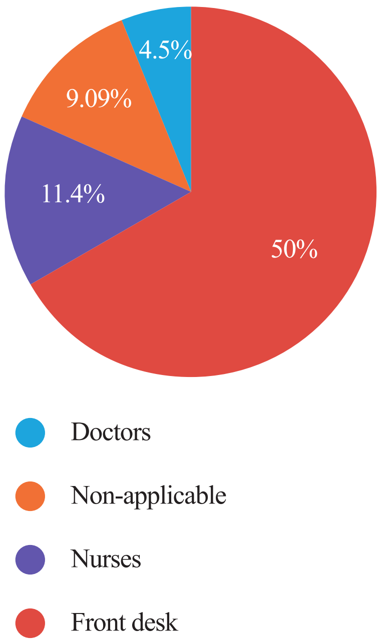
As a final query, the respondents were asked an open-ended question, “Is there anything you would like to share with us in the context of patient data safety and privacy that has not been covered by the questions above?”, to overcome the possible rigidity of a Google form as opposed to the freer format of an interview. Responses ranged from “No” to “I think [sic] personal health data is just basic info. So I don't mind sharing it” to “I wanted to complain to SIH authorities but [sic] didn’t know to whom I should exactly complain. There should be guidelines displayed [in hospitals] if data is leaked and what patients can do about it.”

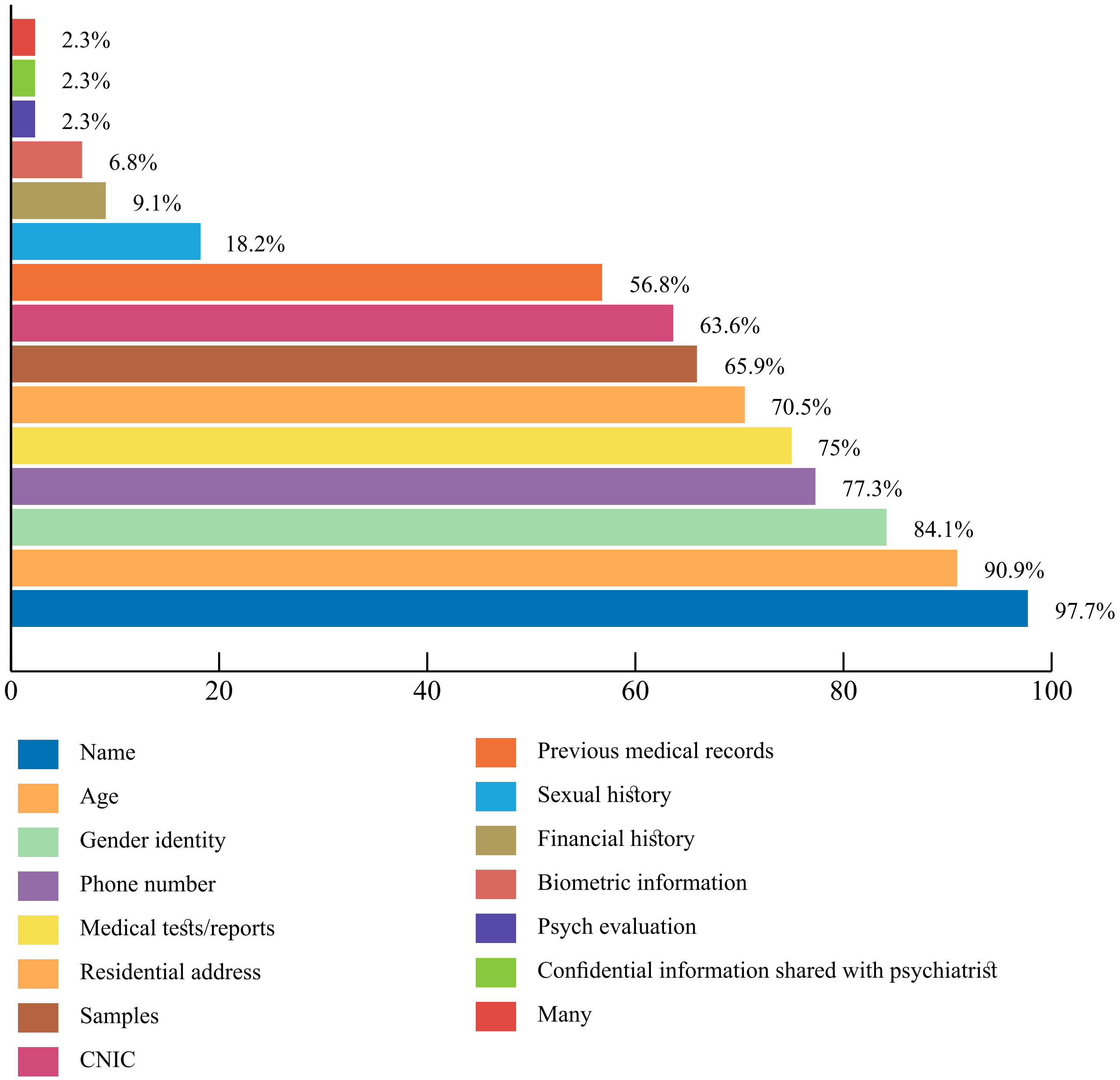
One respondent also shared concerns regarding transparency and the access patients have to their data. They relayed their experience of blood banks:

> *“In blood banks when any donor gives blood they screen it before using it and I talked to an in-charge of a blood bank. He said half of the blood they receive from donors was not used due to infections and diseases but the donors were not informed about their medical problem. They just waste the blood. I have two concerns in this regard:*
>
> *1) The donor should be informed about his/her disease like hepatitis, or any other issue*
>
> *2) Make sure that the infected blood must be wasted and not used for any patient.”*

Data Collection & Consent

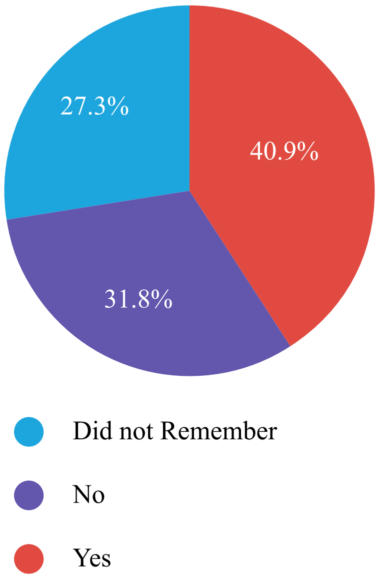
When asked when their data was recorded at the medical facility they visited, 50% identified the front desk, 11.4% said it was recorded by nurses, 13.6% shared data was collected at all points, while 4.5% said it was taken by doctors and 9.09% chose ‘non-applicable’ as a response. Respondents shared the categories of data collected from them as depicted in this infographic:

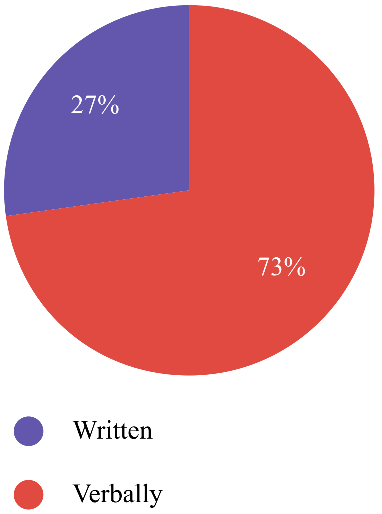


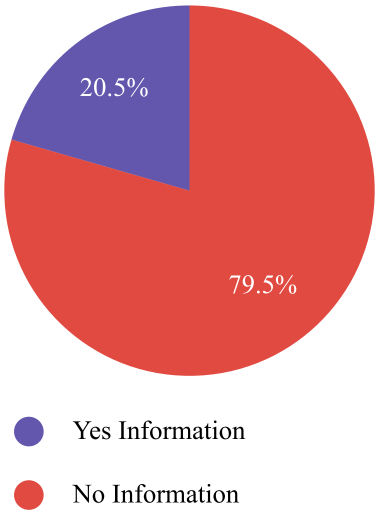


When asked about the ethical requirement of consent for data collection, 40.9% of the respondents said yes, 31.8% said no, and 27.3% said they were unsure if consent was obtained or did not remember. When asked if the consent was taken verbally or in writing, a solid 73% said verbally, whereas 27% said written consent was obtained by the medical facility they visited.

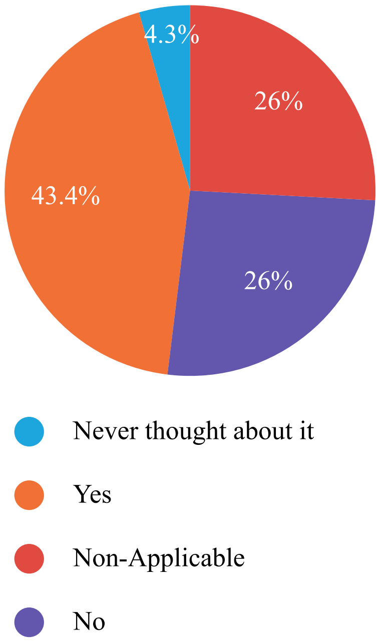
79.5% of the survey respondents said no information was given on how the data being collected from them would be stored or used by the hospital or clinic, whereas 20.5% answered that information was provided.

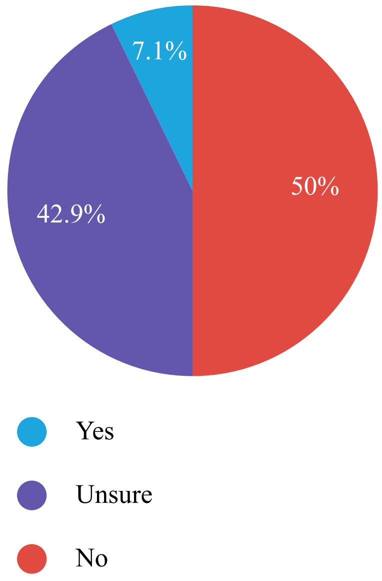


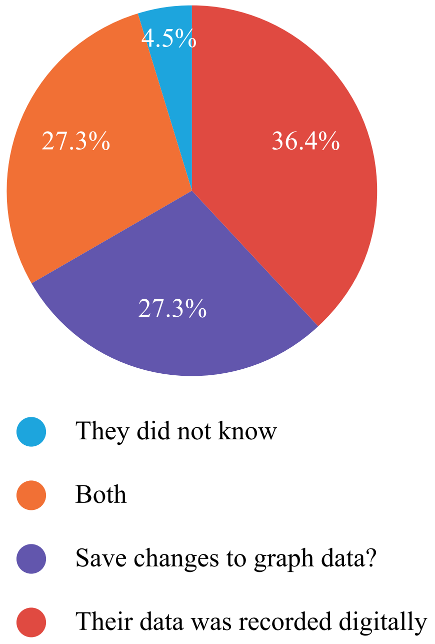




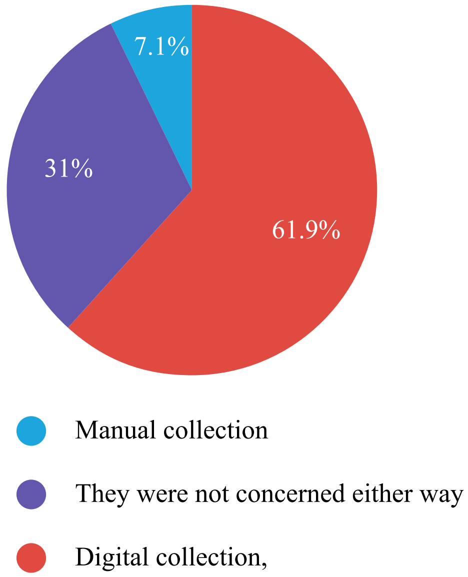
One of the principles of informed and meaningful consent is that it must be voluntary. To understand the voluntary nature of consent within the healthcare system, respondents were asked if they felt comfortable inquiring about why their data was being recorded and how it would be used and stored by the institution or person collecting it. Out of 23 respondents, 26% said no or not at all, 43.4% said yes, and 26% chose 'non-applicable' to answer the question 4.3% said they had 'never thought about it'. On the question of whether denying consent was an option, 50% said no, 42.9% said they were unsure, and 7.1% responded with a yes.

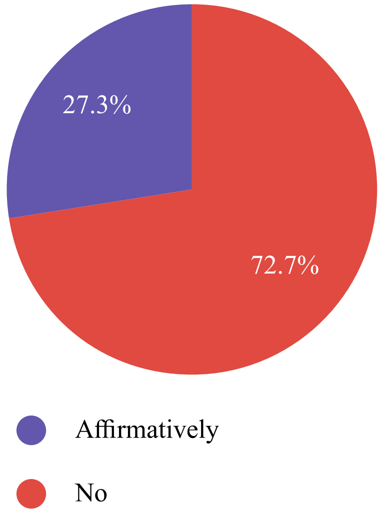






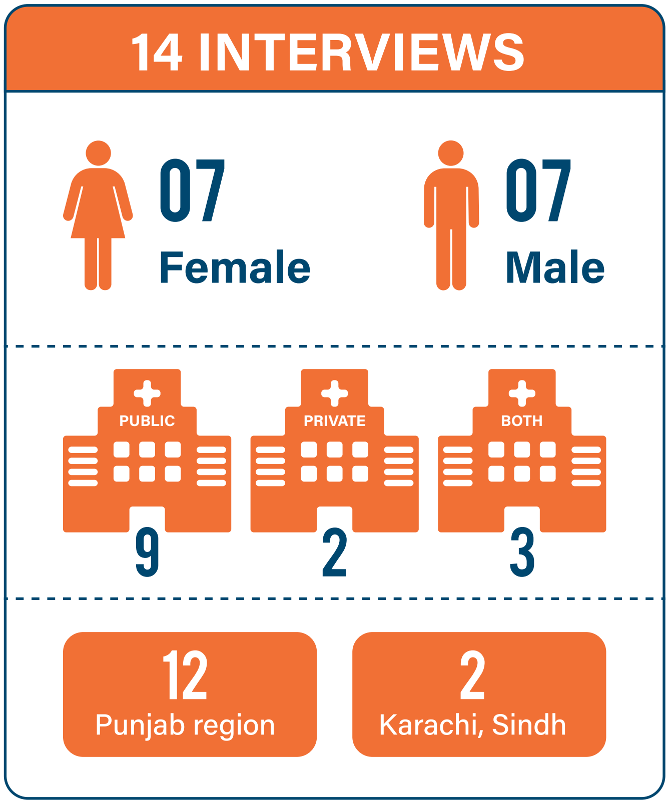
Regarding the form in which data was collected and kept, 36.4% of patient respondents reported that their data was recorded digitally, while 27.3% said it was manually collected, 27.3% said both, and 4.5% stated that they did not know which method was employed. In terms of preferences, they expressed a 61.9% interest in digital collection, 31% said they were not concerned either way and 7.1% preferred manual collection of their personal data. When asked if they had noticed any difference in how data is collected and used by healthcare practices since the pandemic, 72.7% said no, whereas 27.3% replied affirmatively. On highlighting those differences, 2 of the 13 respondents to this query stated that more data was being collected now, while 1 participant felt the method of collecting data was "more digitally forward".





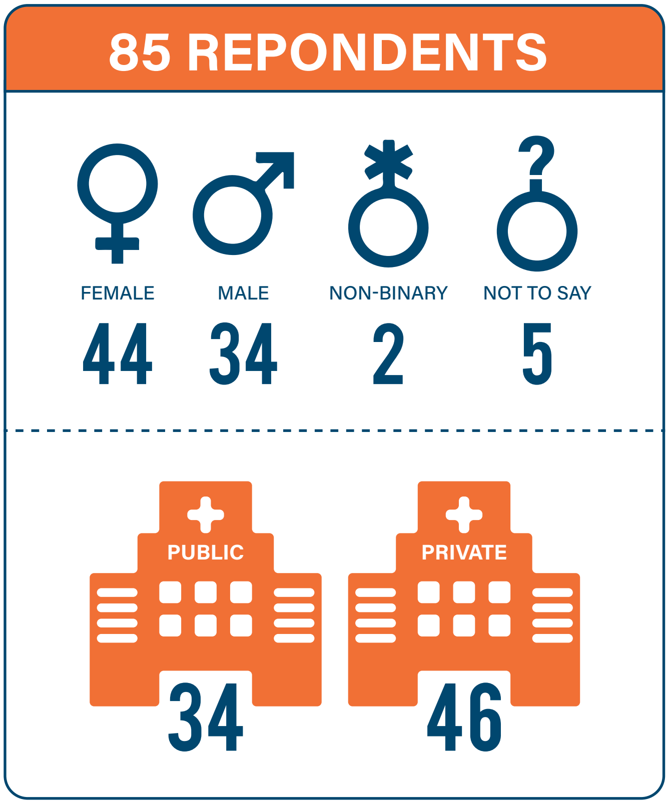
Interviews with Medical Practitioners: Demographic Data

Of the 14 interviews conducted with medical practitioners, 7 participants self-identified as female and 7 as male. 9 of the participants were working in a public sector healthcare institution, while 2 worked exclusively in the private sector, and 3 in both. All interviewees worked at their respective institutions as doctors, except for two who were a lady health worker and nurse respectively. Their years of experience also varied greatly, with the most amount of experience being 26+ years and the least 7 months. Most participants (12) were concentrated in the Punjab region, with only 2 from Karachi, Sindh.

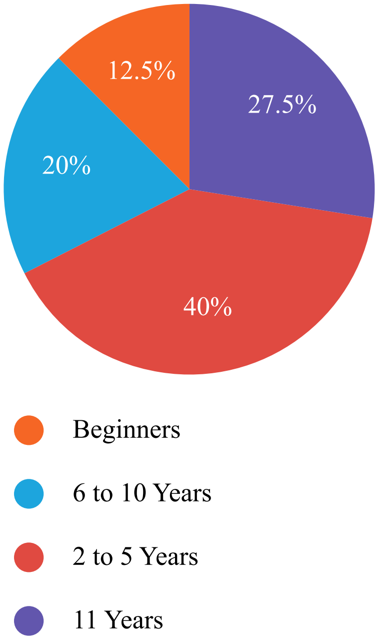


Findings from Medical Practitioner’s Responses:

85 medical personnel responded to Survey B, out of which 36 participants were based in Lahore (Punjab), 10 in Karachi (Sindh), and the rest belonged to various cities such as Kasur, Kharian, Mansehra, Multan, Mianwali, Quetta, Rawalpindi, Okara, Rahim Yar Khan, Islamabad, and Peshawar. 44 (51.7%) respondents self-identified as female, 34 (40%) as male, 2 (2.3%) as non-binary, and 5 respondents chose not to answer the question. 46 (57.5%) respondents worked in the private sector, while 34 (42.5%) worked in the public sector, and occupied a range of positions including doctors, consultants, physicians, dentists, professors, registrars and pharmacists.



52.5% of the respondents worked at a hospital, while others worked in clinics, burn centers, laboratories and tertiary care setups. 27.5% of the respondents had 11 years or more work experience as a medical professional, while 40% had 2 to 5 years, 20% had 6 to 10 years, and 12.5% were beginners having up to a year of experience.

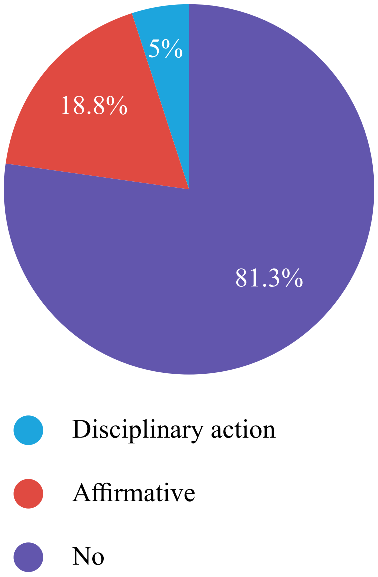


Perception of State of Privacy

Medical personnel's understanding of data privacy was gauged through a series of questions that explored their perceptions of employee and patient data procedures, practices and policies. Interviewees and respondents were asked how secure they felt about their own data as employees and whether they believed that patient data requires a higher level of care as compared to other personal data. Most respondents felt that their data was safe, but not private. One respondent shared her feelings on this:

> *"[My data] is safe, but it’s not private. In CMH [Combined Military Hospitals] they were discreet about personal information, I wasn’t comfortable with sharing that information, but I had to. It was just a paper-based, no computerized system. I don’t know where my information is."*

On leaks and data breaches, respondents for Survey B were asked whether there had been, to their knowledge, any incident of patients' data being leaked or used inappropriately. 81.3% reported no, and 18.8% answered in the affirmative. Out of those who answered yes, only 5% of respondents said that disciplinary action had been taken by their medical institution in cases of patient data misuse.



Similarly, a few respondents who said that their data was not safe mentioned the ease at which data can be retrieved through hospital or clinic administration. One respondent shared how easily staff could share personal data: "someone would have to go to CO [Chief Officer] office to get my information, however, if they wanted to have a discussion about me, my name and basic info they could do so by just talking to a clerk. It then depends exclusively on the clerk whether or not my information will be out there." Further, the participant said that medical information could also be taken from clerks because "doctors do sometimes give information to clerks. Such breaches are not unheard of."

Most healthcare professionals, 65.7% of Survey B respondents and 67.4% of interview respondents who participated in the study believed that patient health data requires a special level of attention. They pointed out the need for consent and approval from the patient before data is shared with anyone. One respondent believed that "[n]o one should have access to confidential health information without the explicit consent of the patient" as patient data is confidential and private.

Medical professionals' opinions on the importance of patient data privacy were largely predicated on three main themes: 1) confidentiality, 2) capital-driven patient data exploitation, and 3) patient-practitioner trust. Health data, they shared, should firstly be kept confidential as it is more sensitive and can have repercussions on the safety of patients. One respondent said that certain "health issues can be physical, psychological or a taboo for certain culture" and that we are "trusted with the most intimate details of their [patient] lives." Another shared their frustration as they noted that "[n]owadays we see doctors posting about patient conditions on social media without their consent." Secondly, they pointed out that the nature of the data "can impact health insurance" and be misused by corporations. Lastly, the need to develop a doctor-patient relationship was a key reason why confidentiality was held in high importance among doctors. One respondent shared that "[i]n order to establish confidence among healthcare providers and patients, this step [trust] is absolutely necessary." However, despite being cognizant of these aspects, one respondent pointed out other tensions with the use of patient data, stating that "obviously we will have to share the patient's symptoms and history with colleagues and females to discuss and learn new things. This is how we learn. It's a demand of our field."

Another interesting angle that emerged in the study was class. One healthcare professional shared that keeping patient data was difficult as some patients were not aware of the importance of patient privacy:

"The patients that come who are very well educated, you can tell by the way they talk, the way they walk, that you can definitely not breach their privacy at all. Now, I work in the periphery, and they don't even know what patient privacy is. They just want to be treated even if the place is overly crowded."

"The patients that come who are very well educated, you can tell by the way they talk, the way they walk, that you can definitely not breach their privacy at all. Now, I work in the periphery, and they don't even know what patient privacy is. They just want to be treated even if the place is overly crowded."

This was a common attitude among practitioners, who lay the burden on the lack of patient awareness and education, not taking into account the structural socio-economic factors that lead to this disparity in awareness. Some participants in the focus group discussion also stated that patient privacy was hard to uphold because patients did not value their own privacy, even though their lack of value may stem more from the urgency of receiving treatment. Prominent suggestions included the need for more awareness and education on privacy, without a structural understanding of privacy and how it is experienced along class lines.

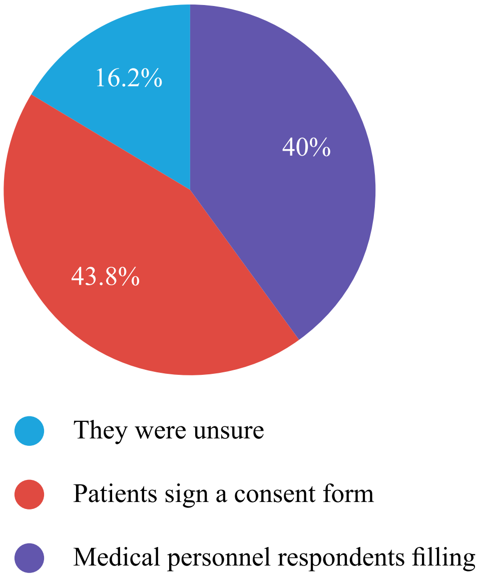
Actual State of Privacy: Data Collection and Sharing

To explore healthcare practices around employee and patient data that would help map the actual state of data privacy within the healthcare sector in Pakistan, we asked medical personnel a series of questions centered on data collection, data sharing and data storage. Questions about their practices were posed to both medical personnel interview participants and survey respondents.

a) Data Collection

The first set of questions focused on data collection and inquired about the type of data collected, methods of collection, who collected it and whether these processes were governed by any rules or guidelines. 82.5% of the respondents on Survey B stated that they collected patient data as part of their job.

The concept of consent is a cornerstone in the administration of healthcare to patients as well as in the collection of data from them. When asked, only 40% of the medical personnel respondents filling in Survey B said that patients sign a consent form while 43.8% said they do not, and 16.2% said they were unsure.



Participants were also asked about the kind of data collected and answers included a wide variety, ranging from name, gender identity, age, Computerized National Identity Card (CNIC) number, residential address, phone number, medical tests and reports, samples (such as blood, DNA, etc.), previous medical records, biometric information, sexual history, and financial information. Even data related to "'spontaneous vaginal deliveries', pregnant women, deliveries, newborn; vaccination records, data related to children's vaccination including nutrition, height, weight, development; data related to adults who may have certain endemic diseases such as tuberculosis, i.e. records on suspicious of TB, case referrals" was recorded. One participant described the process of patient data collection as an “investigation”: “we take forensic history, premorbid history, drug history, development history, childhood history, family history and do baseline investigation.” The responses differed according to the specialization of the medical professional and the institution they worked in, however, the general trend of information collected from patients is detailed below and reveals that a large amount of private information is collected.

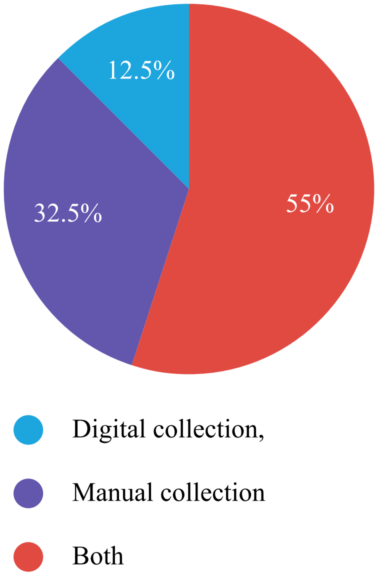
One medical professional told us that they "only take important and limited data, for example, do they [patients] have STDs [sexually transmitted diseases], their marital status, history," and when asked about access restrictions for this data, we were told that generally "anyone who [works at the hospital and] can put in [the patients] CNIC" can access the patient information. Even though they collect data such as marital status and STDs which can generally be classified as sensitive information in Pakistan’s cultural climate, no restrictions or protocols were put in place for data accessibility at the institution. Other data collected included "the name of [the] father, age, phone number and address.” One participant said they started collecting phone numbers after being directed by WHO and the government. It is worth noting that phone numbers and SIM cards are connected to NADRA’s biometric centralized database .[51]

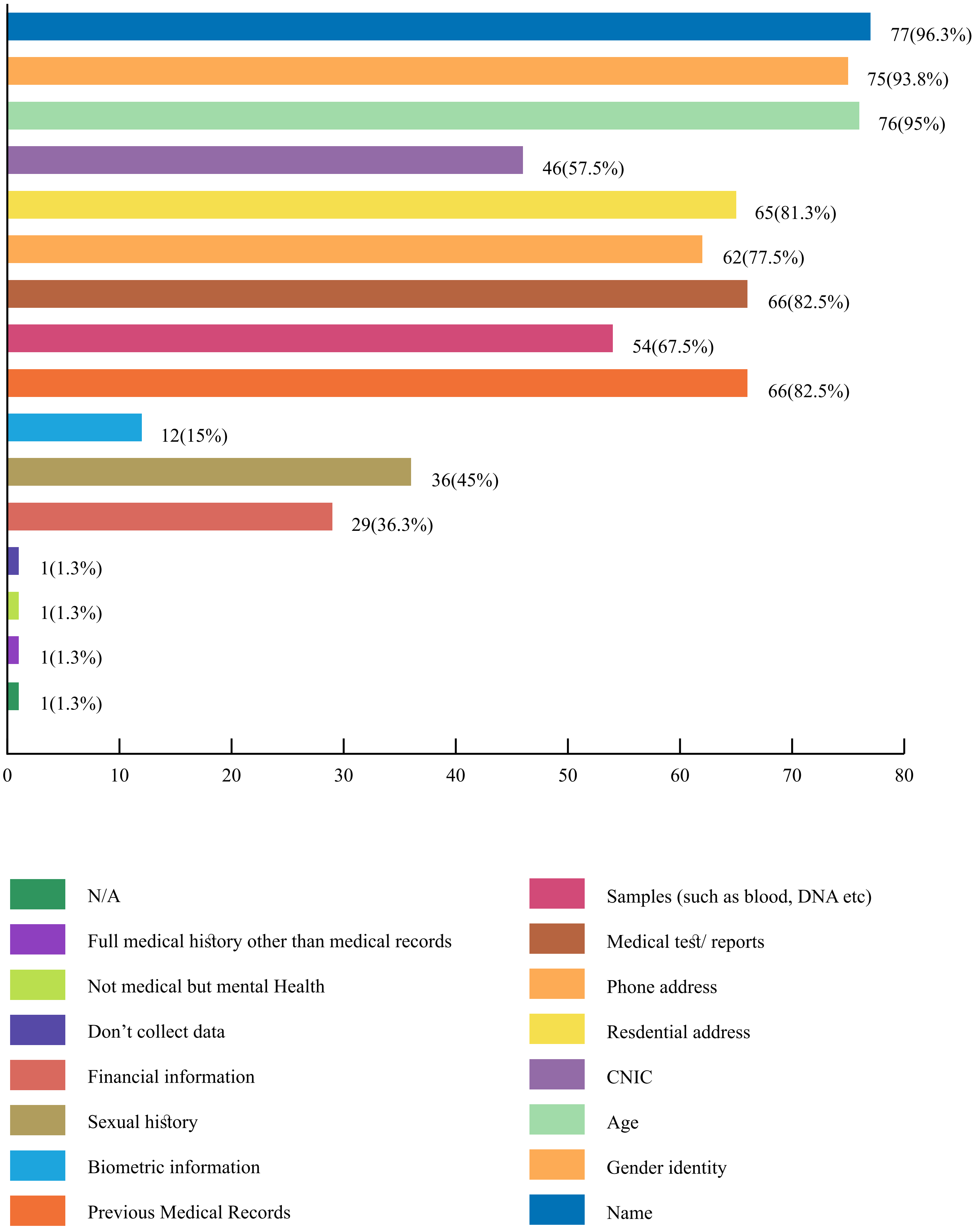
Patient data collection for female patients is considerably different. Categories of data collection include "antenatal check-up of pregnant women, deliveries, postnatal, vaccination, child nutrition (oral therapeutic program, weight, height, record maintaining). We use the DHIS [District Health Information System] app to record this data, and the EMR app for data uploading for the Ministry of Health." When asked if there was any confidentiality training regarding gendered data, the participant said they were "verbally told in training given by doctors and then sent to hospital." The individuals responsible were not made to sign any non-disclosure agreements nor were there any confidentiality clauses in their contracts that would establish any sense of responsibility and accountability. Further, this participant also shared that, in their experience, "sensitive data is treated the same as rest of data."

55% of the respondents on Survey B said that data is collected both manually and digitally. 32.5% said it was collected manually, i.e. was noted down by hand on paper and kept in physical files. Only 12.5% said that data was exclusively recorded digitally, on a computer or electronic device. Contrasted with the majority preference of patients in Survey A (61.9%) to have their information collected digitally, these practices speak to the gap between patients’ expectations and the status quo. According to the participants, data is usually collected by a medical technician or support staff and they are provided with "government given tabs and like computers in the facility so they just enter the CNIC number or the patient [name] and their address [...] so they go into our system so every single time they come again we have their record." There was no indication regarding security and data sharing protocols on these “government-given” devices. On the rules and regulations governing patient data collection, one participant said that "the rules are told to us verbally in government hospitals meaning they tell us which important questions to ask regarding history but there is no accountability or check and balance, meaning it depends on the doctor on duty at the time, it is their decision to ask a question or not. No strict rules."

One of the participants of the focus group discussions shared how rules are often subject to the idiosyncrasies of bureaucratic inefficiencies and lack of oversight:

> *“PHC [Punjab Health Commission] wanted to visit us and we were told by upper management to implement the guidelines that required us to listen to the patient in a closed-door room in order to protect their privacy. We were told to start implementing it for a week because the PHC was supposed to come for a visit.”*




77(96.3%)
75(93.8%)
76(95%)
46(57.5%)
65(81.3%)
62(77.5%)
66(82.5%)
54(67.5%)
66(82.5%)
12(15%)
36(45%)
29(36.3%)
1(1.3%)
1(1.3%)
1(1.3%)
1(1.3%)
0
10
20
30
40
50
60
70
80
N/A
Full medical history other than medical records
Not medical but mental Health
Don’t collect data
Financial information
Sexual history
Biometric information
Previous Medical Records
Samples (such as blood, DNA etc)
Medical test/ reports
Phone address
Resdential address
CNIC
Age
Gender identity
Name

b) Data Storage

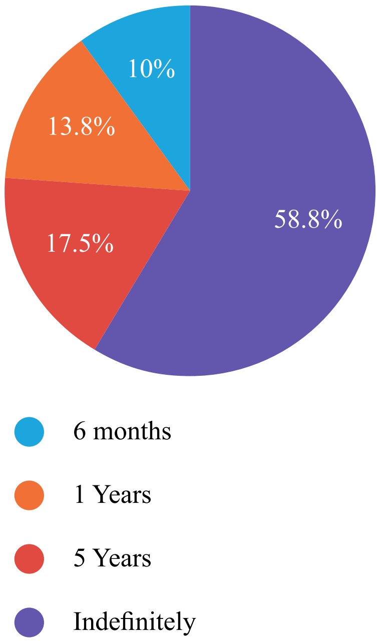
To understand the structures in place regarding data storage, the next set of questions focused on how long data is stored and retained, whether the storage is manual or digital, and lastly, where it is stored.

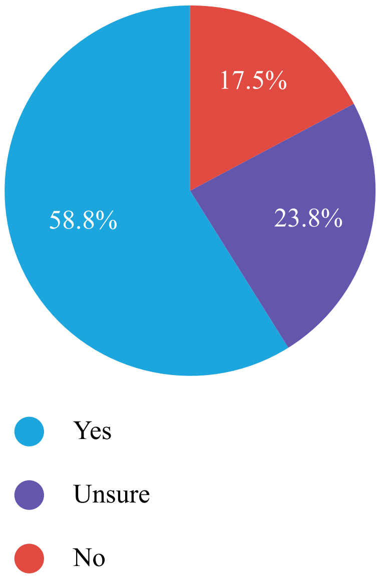
When asked how long the data is stored, one participant said that data at their place of work was stored “ever since the health facility was made, ever since then because we have it stored in the back with really old copies and registered still present, nothing is allowed to be thrown away. Approximately [sic.] 50 years." Others gave answers that varied from 10 years to 3 months. 58.8% of the respondents on Survey B reported that data was stored indefinitely. 17.5% shared that it was stored for up to 5 years, 13.8% said 1 year and 10% said less than 6 months. Responses varied regarding the form of data storage, with some data digitized and some manually stored. Digitally recorded data is kept in health management integration systems that allow healthcare institutions to centralize it with the aim of smoothing out administrative procedures. One participant shared that “outpatient is 90% computerized, while inpatient is manual in terms of doctors’ notes.” Due to a lack of research in the area, there are no statistics to verify the claim, but the general gist gleaned from the participants is that basic information collected on arrival is digitized and medical diagnosis from the doctor is manually recorded in most hospitals that have upgraded their systems. Others with more outdated systems collect and store data wholly manually. Exploring how long patient data is retained by a medical institution after the patient's demise, 50% of the respondents on Survey B stated they did not know what was done with that data. 23.7% provided some insight by sharing that it was stored indefinitely, while a small percentage gave varied answers stating that the data was stored for between 3 years to 5 years, and in some cases, less than 6 months.

Manual data is handled by hand in record rooms "we have a Record Room, and it is categorized by year so you can get data from 10 years ago as well." Some institutions keep data in these record rooms in perpetuity, while others either share or discard them. One participant explained: "[data is] stored for about 1 to 2 years, after that the registers are given to the government and put into cupboards and are not taken care of." However, manually-held data can be subject to wear and tear as one participant points out, “[y]our data will be stored in a small room in an old register that barely anyone can access, it will be damaged. [In the institutions where I have worked, the volume of data] is very big and there’s no filing system, they aren’t organized so you can’t access it.”

58.6% of the respondents on Survey B did not have an overarching medical ethics board at their hospital or medical institution. The 41.3% that did have one were largely unsure whether it dealt with patient data, with only 20% answering yes. Even if institutions did not have a medical ethics board, some institutions operated with their own policies, a respondent stated. 57.5% reported that their medical institution did have a medical ethics policy in place. When asked if their hospital/medical practice had a doctor-patient confidentiality/patient data confidentiality policy, 58.8% said yes, 23.8% said they were not sure and 17.5% said no.

These statistics indicate the actual state of privacy, directly in contrast with the responses regarding their personal perception of how privacy is maintained in their workplace, demonstrate the tepid level of importance associated with the protection of personal data in Pakistan’s healthcare system.





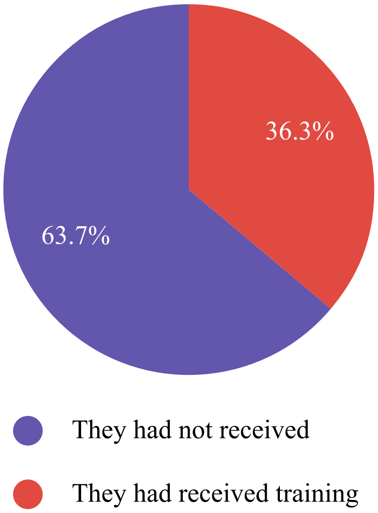
c) Data Sharing

The last set of questions explored what processes, policies and regulations healthcare institutions follow, how data is accessed within the healthcare institution and how it is shared externally. The questions posed explored whether the workplace had any doctor-patient confidentiality guidelines, who had access to the data, who was responsible for safeguarding it, and if they knew of any breach or misuse of patient data at their workplace. Some questions specifically inquired whether data is shared with any third parties such as government or insurance companies, and whether the government requires the healthcare provider to share any specific categories of patient data, especially regarding the Sehat Card and other government/welfare schemes.

Most participants said that guidelines had only been communicated to them verbally. Further, one participant explained that sensitive situations such as those related to gender were common and practices around them were strict:

> *"We're not supposed to tell the woman who come for ultrasounds the child's gender because if it's a female they usually go for [gender-selective] abortions so what we do is that we usually tell the mother but we are not allowed to tell the family. We also provide contraception, [and] so most of the time the women tell us not to tell their family if they're taking any contraceptives so we also provide confidentiality over there as well. So these are some cases where the guidelines are more strict otherwise it's not much."*

Contraception and abortion are largely controversial areas of female sexual and reproductive health that can have serious consequences if not dealt with sensitively. Notably, on workplace training for patient data handling, only 36.3% of the respondents in Survey B said they had received training, while the majority 63.7% said they had not. Without strict, formal policies and guidelines, women are put in an extremely vulnerable position, liable to serious consequences if their health data were to be shared irresponsibly.



On sharing data outside the institution itself, one participant said, "[w]e collect individual data for ourselves and the government. We have malaria, dengue, etc. [as] the main things, and their data is regularly collected on a monthly basis and we send it to the health department so they can see how many people are affected. It's very methodical and systematic." Despite these processes, lapses exist as data has been shared openly according to some responses that told us: "[s]ome of the Covid patients' data was leaked to a local social media channel and patients photos and their biodata was released on the social platform." Apart from data leaks, "data is shared openly in groups when asking for consultation. Even doctors are not safe from this. ECGs and medical records of colleagues have been shared openly on whatsapp by some senior colleagues". Another respondent reported that "data of my patient was posted on an open Whatsapp group by a higher member of faculty." Some data sharing even led to serious consequences as in one case "someone from the press threatened to sue the doctors involved in patient care." Exploring data misuse, one participant presented a different view: "no [it is not misused]. We get very high-profile patients at CMH and we protect their privacy." As noted earlier, "high profile" patients are often coded as elite, well-connected or politically important patients whose privacy is 'bound' to be protected. Hinging levels of privacy on the status of the patient can be discriminatory and does not address privacy issues within medical institutions at a systemic level.

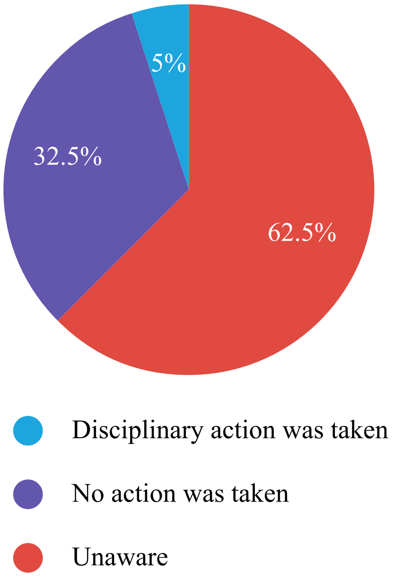
Regarding third-party access to data, one participant listed that: "Yes, our data is given to the CO then the head office and it is shared [with] WHO, UNESCO and other organizations that work on maternal mortality. Data is also shared with insurance companies and the Sehat card." Others stated that "monthly reports taken down manually go to the government, PHFMC [Punjab Health Facilities Management Company] is given data."

The most common third parties that were accessing the medical records of patients were the government and insurance companies. Since Pakistan does not have any data protection law, and public/private institutions do not have any proper policies on the protection of patient data, healthcare personnel are thus often at liberty to decide whether to share necessary data such as disease types and the number of patients, or all of it.

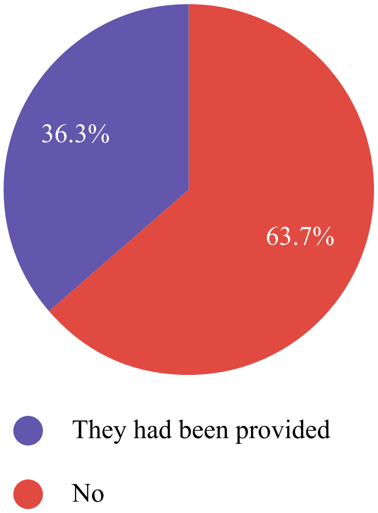
The government also requires that certain data about "communicable diseases like COVID, tuberculosis and dengue" are reported. One participant shared that the "Punjab Healthcare Commission asks for the data bi-annually [and it is] shared with State Life [government-owned insurance company] because of Sehat Card." This was validated by other participants who confirmed that the government "requires the patient's details for the processing of Sehat card, like biodata, diagnosis and its expected management." However, upon further pressing on the categories that are required, the list became longer to include CNIC, biodata, diagnosis, gender, address, COVID tests' and in case of death, "the cause of death, time and treatment given." The list of people who had access to patient data varied as well, ranging from administration to heads of departments to doctors, nurses, and technicians.

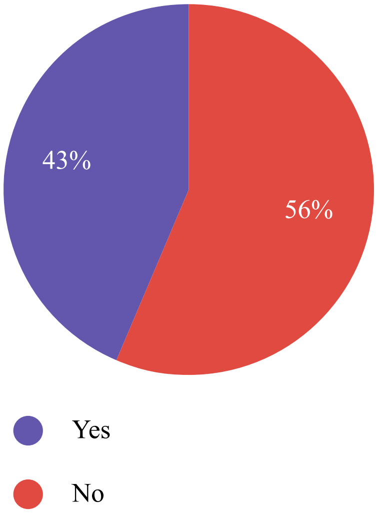
Framework and Accountability

The Framework and Accountability section, as designed by the researchers, contained 4 lines of inquiry in the interview and through Survey B. The first of these queries focused on whether any disciplinary action had been taken against any misuse of patient data, in case a breach had occurred. A majority of the survey respondents, i.e 62.5%, answered that they were unaware that any such action had been taken, 32.5% said no action was taken and 5% replied affirmatively that disciplinary action was taken.



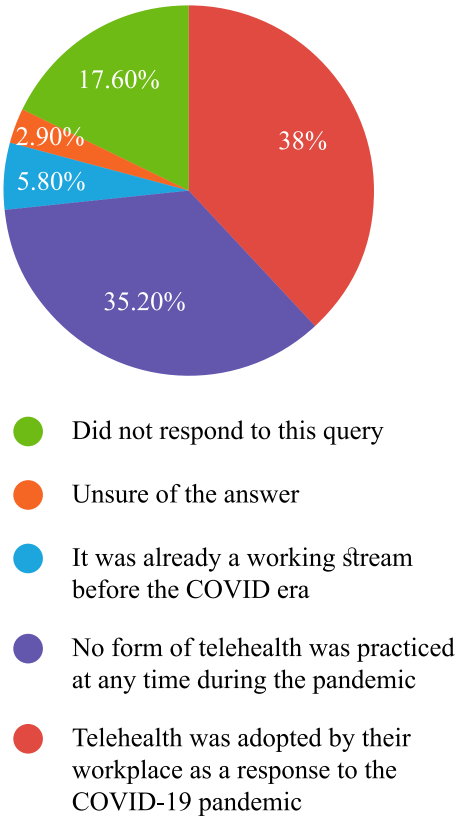
When asked if their workplace provided any guidelines on handling patient data, 63.7% said no and 36.3% said they had been provided with such training. Out of the interview respondents that did engage with the question regarding guidelines, 56% said no, while 43% said yes they had received training or been given guidelines.



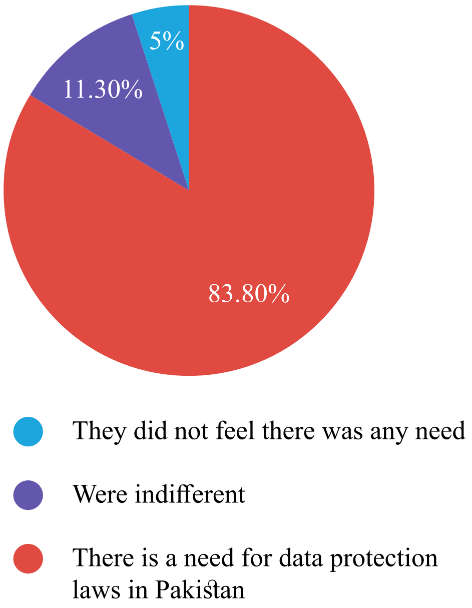


Regarding third-party data sharing by their respective medical facilities, and whether it is governed by any framework, most respondents did not address the query as they felt it did not apply to them, and a few said no. One interviewee shared that the “Bait ul Maal (government body for poverty alleviation) office is located in[side] the hospital, to give aid to those deserving, they receive data which is attested by [the] local councilor/imam and then confirmed by the doctor.” In earlier questions, respondents had identified that data was shared with regard to contagious diseases such as COVID-19 and dengue. In Punjab, the Punjab IT Board (PITB)'s 'Disease Surveillance System' collects data from across “all levels of healthcare facilities i.e. primary (2,828 RHCs and BHUs), secondary and tertiary (147 hospitals)[52].' Information sharing with the respective provincial health departments is built into one of their core functions: “Data collection and compilation of vital health statistics… [p]lanning and Development of healthcare delivery for improving[53].”

For the last question under this theme, the researchers asked the interviewees if telehealth was practiced at their medical facility. 38.2 % reported that telehealth was adopted by their workplace as a response to the COVID-19 pandemic, 35.2% said no form of telehealth was practiced at any time during the pandemic or otherwise, 5.8% said it was already a working stream before the COVID era, while 2.9% were unsure of the answer. 17.6% of the interviewees did not respond to this query.



Additionally, when inquired, 83.8% of the respondents said that they felt there was a need for data protection laws in Pakistan, 11.3% were indifferent, and a small percentage of 5% said they did not feel there was any need. These percentages are indicative of the lack of an existing framework that is protective of the rights of Pakistani citizens, specifically patients, as data subjects.



Sensitive Data Collection and Consent

Sensitive personal data is categorized as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation' as per Article 9 [54] of the General Data Protection Regulation of the European Union (GDPR). A similar definition appears in the draft Personal Data Protection Bill put forth by the Ministry of Information Technology and Telecommunication (MoITT)[55]. In the GDPR, "the vital interest" of the data subject and protection of privacy is given paramount importance, and the processing of such sensitive information is mostly prohibited. The exception to this includes a very explicit criteria by which this data can be collected. Namely, instances "where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms[56]."

Some interview and survey questions focused on the data of gender and sexual minorities and regarding patients of stigmatized diseases to glean answers about the protection or guidelines surrounding sensitive data categories. When asked if there were any protocols regarding the collection of transgender patients' data at their respective workplaces, 58.8% said no, 35% said they were unsure, and only 6.3% said yes.

One respondent, while commenting on the dearth of progressive and holistic data collection in the industry said that practices are "very regressive with "sex" questions being termed "gender" and the gender question only having male/female categories as possible responses." Reliance on biological and binary categories has the effect of either excluding transgender individuals from these datasets altogether or leading to misgendering during treatment. Other studies show that these practices, among others, act as deterrents to access for the transgender community: 74% of transgender persons in Punjab avoid going to public hospitals [57], and 92% of transgender people have experienced discrimination in Khyber Pakhtunkhwa medical facilities .[58]

Additionally, when it came to socially stigmatized diseases, 66.3% of the respondents said that they process, admit and treat patients with HIV at their workplaces, while the rest said they did not. 22.5% of those that did treat HIV patients, said that there is mandatory data sharing regarding HIV patients with the government or companies, especially with regard to diagnosis or HIV status.

According to a key informant who is associated with a community male health center in Punjab, one of the main challenges in working with HIV cases in Pakistan is that information about these cases has to be shared with the local health department which can undermine the privacy of the patients that they are trying to help. The relationship the male health center has built with the government includes the understanding that the personally identifiable information of these patients is sensitive and must not be shared with any third parties. This relationship, however, came about after years of advocacy work and gradually when the United Nations Development Program (UNDP) began working in Pakistan on HIV prevention[59]. In response to this advocacy, the government signed treaties to lessen discriminatory behavior in healthcare facilities, which has improved the quality of care received by HIV patients.

As for the data the government collected for the Integrated Biological and Behavioral Surveillance (IBBS) service, the key informant shared that the Ministry of Health was only counting sex workers as a key populace and that the community workers focused on the cause of providing and advocating for HIV patients asked the Ministry to include several relevant terms. The 2017 report[60]states that the populations whose data was mapped included people who inject drugs (PWID), men who have sex with men (MSM), transgender population and female sex workers (FSW). He added that "we had to be careful that the data wasn't stigmatized and the database is not used for discrimination".

When collecting and integrating data, he stated that the health center does not categorize the information through CNIC numbers but through individual IDs generated by their own system, to further ensure confidentiality. Sharing his experience of working with the national and local governments, he said that in the last year, the center has signed a contract with the Punjab government and they have been keeping the government apprised of positive diagnoses and the number of cases they have been receiving: "The Pakistani law is behind and the problems need to be worked out, the government needs to draft laws and develop integrated systems to help them and make sure they are not targeted based on their gender and sexuality." Sensitization of staff treating patients with HIV is also an important element to lending good healthcare support, he contends:

> *"When they [patients] take our help we make sure that these problems don't happen. But for example, if a transgender man or bisexual man walks in a center and he is HIV positive, if he comes to our staff he has a tag [identifier entailing stigma] on him but the problem is that the group of staff needs to be sensitized by the government to make sure that they don't mistreat the patient, so [we have seen] their behavior is weird when it comes to this population. There are many layers of problems and we address them to an extent [that] we hear in clinics that we are promoting homosexuality in Pakistan. Secondly, a lot of moral policing happens, they think that it [HIV] is only transmitted through sexual intercourse. Even so, medical personnel should not judge their life choices. You don't see a breach in [our] clinics. We don't tolerate it. We [need] good capacity building if we see a staff member behaving a certain way we know who to complain to or to protest to. They have no right to leak their [patients'] data or breach their confidentiality or give them a lecture on a religious basis."*

Regarding their own approach to sharing data, he stated that the center does not allow actual patient data to be viewed or accessed by anyone, as according to the health center's manual, breach of confidentiality is a serious offense. "You can look at our system, but we can't compromise on [personal] data," he states.

Public Health Sector

In the course of collecting data for this report, the researchers were able to speak with two noted public health officials of the country Dr. Rana Safdar and Dr. Faisal Sultan, on the state of privacy in their area of work. Dr. Safdar, who is an epidemiologist by profession, attributes many of the public policy considerations in place now, to the COVID-19 pandemic, deeming it a 'great learning curve' for the public health response sector. He shared that at the National Institute of Health (NIH), all the manual data they receive is digitized, to a great extent.

> *"In terms of NIH if you look, the laboratory setup that provides support to all kinds of infectious disease outbreaks across Pakistan, all the samples that are processed after an outbreak, the investigations and their individual data is maintained in the national laboratory system. Apart from that, within polio eradication, the priorities are that you have to reach every child and apply surveillance to all suspected cases of paralysis and body weakness under the acute paralysis system. All the data received from this is also identified with the personal information. There is a limited amount of data that is in our system but the kind of system that perhaps should be there, which is there in Europe and developed countries, is limited over here [and] we need to move towards there."*

Addressing a query regarding the privacy of patients' data, he stated:

> *"No raw data is shared with personal identifiers, this is standard practice, and all our top institutions, including NIH and all the priority programs, anyone who needs personal information we remove the personal identifiers and provide data in an analyzed form. And if there is an operational requirement of any program, in which we have to give raw data, we just remove personal identifiers."*

When asked whether the enactment of a data protection law would be a welcome step, he responded:

> *"…my submission is that we are good in law-making but we fail in implementation, so right in the process of devising such laws, I would very strongly recommend that the key stakeholders and their inputs are taken into account so that the laws we make serve their purpose and simultaneously are also implementable."*

Dr. Sultan, who is currently serving as CEO at one of the largest private hospital networks in Pakistan, emphasized the importance of data safety while also stating that exceptions have to be made when the risk of not sharing information could have a substantial impact on the larger population. From a public sector perspective, he shares that: "Privacy is high [priority] but not absolute where public good is paramount", adding that the information about a patient's health status can be shared to create public awareness without revealing identifiers such as their name or CNIC details.

Explaining access to public health data, he said, for instance, during the COVID-19 pandemic, the data (including vaccination and testing data) was maintained at a central repository secured by a special software developed with the help of NADRA. The database, he shared, was kept technologically and physically safe and was not shared with anyone who did not have a legitimate right to know:

> *"The path is, you go to a laboratory collection, give your name, address, etc., and they add it into the database from there the test is pushed to a system. All the steps are individually vulnerable. We need to strengthen this, there's a lot [more] to do. The healthcare division is a highly provisional topic, which is another problem, a disease is not going to look at borders, so coordination is important, and data sharing is an issue."*

Addressing a question on the overall standards of healthcare data safety in the country, Dr. Faisal said that given the diversity of systems, it ranges from good to weak. According to him, the weakness is not linked to technology but behavioral failings, sharing that many of our healthcare workers lack the expertise to treat private data. This attitudinal change needs to be corrected with training, which sensitizes medical professionals and staff that data privacy means changing daily habits like not casually discussing patient data or cases in the elevator or cafeteria conversations. Furthermore, it means integrating privacy into every practice, no matter how small–for instance, even when disposing of printouts containing patient information, secure practices need to be adopted, such as using sealed bins that are pulped under supervision.

Conclusion

The overall data collected through this study indicates a varied understanding of patient data privacy, even when coming from the patients themselves. The lack of guidelines around healthcare data privacy coupled with the overall deficiency in general awareness of privacy in Pakistan has impacted general perception and enforcement of privacy rights, despite being Constitutionally guaranteed.

Our findings suggest that while the perceived privacy afforded to patients ranked at mid to lower-range values, their responses around actual instances of data breaches were low, in that most (77%) had not experienced such an occurrence. However, despite patient perceptions of privacy breaches, most patient respondents expressed lukewarm interest in a data protection framework that could govern the handling of their private information. It has been discussed in the report that given the essential nature of health services required, patients see privacy within the false binary of access to health services, i.e. getting treatment, and privacy. This reception can have an impact on advocacy efforts around patient-centric regulations and practices and thus highlights the importance of awareness raising measures to increase the general understanding around the need for digital and data literacy.

The medical practitioners that were interviewed and/or surveyed indicated that accountability mechanisms were rarely in place and only a paltry 5% of those questioned reported use of disciplinary action in the case of misuse of patient data.

58.6% healthcare respondents reported not having an overarching medical ethics board at their hospital or medical institution, 57.5% reported that their medical institution did have a medical ethics policy in place. When asked if their hospital/medical practice had a doctor-patient confidentiality or patient data confidentiality policy, a mere 58.8% said yes.

The holistic picture that emerges is one of weak infrastructural perimeters drawn loosely around the health sector in the country. The need of the hour is a robust set of guidelines looking over all aspects of informational privacy as pertains to medical patients, in fact, it is long overdue and continues to result in breaches of varying severity. It is not surprising that such instances often go unnoticed or unremarked given the cultural responses and lack of accountability we have gleaned from our respondents.

Recommendations:

Given the gap between aspirations of privacy and the actual state of privacy in terms of practices, policies and experiences, this report has collated the following recommendations based on the interviews, focus group discussions and surveys conducted. It is important to note that not all recommendations made by participants of the study were included as they were weighed against international human rights standards and principles of data privacy.

Recommendations from Medical Practitioners

- In addition to patient security, the personal security of doctors and medical staff should be ensured through the privacy of medical practitioners' personal data. However, this should be balanced with the need for accountability and redress in cases of malpractice. Policies and protocols should be in place regarding who can access staff data, with mechanisms in place to provide transparency and access for complaints of malpractice and misconduct. Access to data must be only allowed as per standardized rules that are not bent or misused through connections or bribery.

- Patient data privacy and ethical best practices should be taught and included as mandatory subjects in medical school curriculums nationwide. These subjects must be reinforced at the workplace through regular training and sensitivity building for all staff.

- There should be increased protection against digital data breaches at medical facilities, in terms of patients' and employees' data, through improved and more secure software systems, vigilant supervision and accountability mechanisms such as ethics reviews.

- Quality of data privacy experienced by patients should not be dependent on class or socio-economic factors, uniform protections should be afforded to all patients by providing the same standards and guidelines around data safety in both public and private healthcare sectors in Pakistan.

- Specialized rules or laws need to be enacted, similar to standards set by the Health Insurance Portability and Accountability Act (HIPAA) in the US, that binds doctors to uphold doctor-patient confidentiality. These can be in addition to a general data privacy law, the specialized rules can cover the particularities of medical data privacy under the framework provided by the general law.

Recommendations from Patients

- Data should be available on a need-to-know basis, accessible only through the written, informed consent of the patient. In cases where written or active consent is not possible, such as due to a lack of literacy or a medical condition that does not allow for obtaining consent, protocols should be in place to ensure consent is taken at the next possible opportunity and recorded through other means. Protocols for obtaining consent should take into account the power dynamics between doctors and patients, which can be reinforced by class status, gender, (dis)abilities, nationality/citizenship status, nature of disease, etc., and measures should be in place to allow patients to deny or withdraw consent.

- Greater emphasis needs to be placed on patient consent by the management of medical institutions through standardized procedures enforced by guidelines and reinforced through regular training sessions. These guidelines should be publicly available at the physical premises of the medical facility and online. Format and language of consent forms require standardization across the healthcare sector, particularly in smaller-scale, private or informal medical settings.

- Existing rules or guidelines should be amended to ensure patient data should only be accessible to authorized personnel who require it to provide quality medical services, other staff or personnel within the organization not falling under the definition of authorized or necessary personnel should not have access to this data.

- Healthcare institutions should be obligated to keep their data management systems updated and have data security practices in place, so that patient data is stored in a secure and encrypted manner.

- The Code of Conduct document[61] created by the Pakistan Medical and Dental Council (PM&DC) outlines its Standards of Confidentiality and Privacy of Information in section 7, however, these guidelines need to define what personal data would mean in this context (such as names, contact information, medical histories, diagnosis, reports, pictures and other personal data) and also dictate that the personal and sensitive data of patients should not be used as case study material for medical students. Additionally, any access to patient data for teaching or research purposes should have all personally identifiable information removed beforehand.

- Healthcare organizations should codify rules/penalties in the event of privacy breaches, and there needs to be a push for national policy development by the Ministry of Health and respective provincial health departments on the protection of patient health data and privacy. The process for filing a complaint regarding a breach needs to be accessible to all patients.

- Furthermore, medical institutions should be required to self-report any breaches or lapses, incentivising self-regulation and transparency.

- A comprehensive data protection law should be passed, with special protections for medical data, according to international best practices and human rights standards which center the privacy of individuals and patients. Clear definitions of important concepts such as consent, sensitive personal data, third parties and public interest need to be provided in such a law.

- Against purpose limitations need to be identified and enforced. Access to patient data should be restricted to relevant healthcare professionals. Additionally, patient data gathered at an institution should not be passed off to third parties without patient consent and transparency, and should be used by the original institution for medical purposes only.

- Special protocols and training should be in place to sensitize medical practitioners on the collection, use, retention and sharing of sensitive personal information, particularly regarding women and gender minorities. Gender sensitivity training on the safeguarding of such data should be provided to all staff of medical institutions and government departments, not just personnel who deal directly with patients.

- Government departments, particularly health and education, must invest resources in mass public education campaigns regarding privacy rights, particularly concerning sensitive medical information. Collaborations with civil society and media must be fostered to ensure the mass reach of these education campaigns.

DRF Policy Recommendations

- Protocols need to be developed to ensure the patient is kept informed on how the data will be used. In case of a breach of privacy or consent, the patient should not only have the option but the ability to pursue legal action. Additionally:

- A data protection law needs to be passed which encompasses safeguards for medical data under the category of "sensitive personal data" which can only be obtained on the basis of informed, active consent. This can either be encapsulated in the ambit of the draft Personal Data Protection Bill (PDPB) introduced by the MoITT or through a new specialized legal instrument for which the PDPB serves as the parent law.

- Medical practitioner protocols and code of ethics need to be made more robust and changed to make obtaining consent a mandatory requirement.

- Accountability and redressal mechanisms need to be developed through data protection legislation and professional licensing regimes to create pathways for filing complaints in case of breach of consent and data.

- The utmost priority should be given to ensure that data is shared only with the relevant medical authorities as per the law. Government authorities, through their rule-making, explicitly define what data they require to be shared, in what form, for how long and for what purpose. Measures should be taken to ensure that data is stored in an anonymised and aggregated manner as much as possible, with the understanding that even anonymised data can be identified. If government-held data is stored on a central server managed by the government, access to it must be restricted and delinked from other databases as much as possible to ensure data privacy and security.

References

1 IFRC. (2021, May 12). Asia: 5.9 million COVID-19 infections overwhelm hospitals - world. ReliefWeb. Retrieved February 17, 2023, from https://reliefweb.int/report/world/asia-59-million-covid-19-infections-overwhelm-hospitals

2 Improved Diagnostics & Patient Outcomes | HealthIT.gov. (n.d.). Retrieved 17 February 2023, from https://www.healthit.gov-/topic/health-it-and-health-information-exchange-basics/improved-diagnostics-patient-outcomes

3 Improved Diagnostics & Patient Outcomes | HealthIT.gov. (n.d.). Retrieved 17 February 2023, from https://www.healthit.gov-/topic/health-it-and-health-information-exchange-basics/improved-diagnostics-patient-outcomes

4 Kazi, A., Qazi, S., Ahsan, N., Khawaja, S., Sameen, F., Saqib, M., Khan Mughal, M., Wajidali, Z., Ali, S., Ahmed R, Kalimuddin, H., Rauf, Y., Mahmood, F., Zafar, S., Abbasi, T., Khoumbati, K., Abbasi, M., & Stergioulas, L. (2020). Current Challenges of Digital Health Interventions in Pakistan: Mixed Methods Analysis. J Med Internet Res 2020;22(9):e21691. Retrieved 17 February, 2023 from https://www.jmir.org/2020/9/e21691/

5 Fitch Solutions Country Risk & Industry Research. (2022, August 19). Pakistan's Healthcare Budget Is Set To Decrease, Placing Further Pressure On An Already Underperforming Healthcare System. Fitch Solutions. Retrieved February 17, 2023, from https://www.fitchsolutions .com/healthcare/pakistans-healthcare-budget-set-decrease-placing-further-pressure-already-underperforming-healthcare-system-19-08-2022

6 Express Tribune. (2021, November 27). NADRA Data Leak. tribune.com.pk . Retrieved from https://tribune.com.pk/story/2331199/nadra-data-leak

7 Privacy International. (2020, May 1). Pakistan's "patient zero" stigmatized after data leak. privacyinternational.org. Retrieved from https://privacyinternational.org/examples/3839/pakistans-patient-zero-stigmatized-after-data-leak

8 Zanaboni, P., Kristiansen, E., Lintvedt, O., Wynn, R., Johansen, M.A., Sorenson, T., Fagerlund, A.J. (2022). Impact on patient-provider relationship and documentation practices when mental health patients access their electronic health records online: a qualitative study among health professionals in an outpatient setting. BMC Psychiatry. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9331580/#

9 Durrani , Z., Hassan , S. B., &amp; Karamat, Z. (2022, December). A Privacy Perspective: The Collection and Use of Health Data in Pakistan. digitalrightsfoundation.pk. Retrieved from https://digitalrightsfoundation.pk/wp-content/uploads/2022/02/Health-Data-Study.pdf

10 YouTube. (2022). The Agenda Exposed . Wajih Uddin. Retrieved February 17, 2023, from https://www.youtube.com/watch?v=xIbJ7jTWyZw.

11 Patient data stolen from Quaid-i-Azam Hospital . (2016, August 22). Dawn.com. https://www.dawn.com/news/1279147

12 Jahangir, R. (2020, May 1). "I became a pariah." Coronavirus victims' data is leaked on social media in Pakistan. Coda Story. Retrieved February 17, 2023, from https://www.codastory.com/authoritarian-tech/pakistan-tech-coronavirus/.

[13] Jaffery, Y. (2020, May 25). Tales of survivors: How I became Pakistan's first Covid-19 patient. Express Tribune. Retrieved February 17, 2023, from https://tribune.com.pk/story/2183876/1-tales-survival-became-pakistans-first-covid-19-patient/.

[14] Aamir, A. (2020, March 23). Private Data of Coronavirus Patients Leaked in Balochistan. Balochistan Voices. Retrieved February 17, 2023, from https://www.balochistanvoices.com/2020/03/private-data-of-coronavirus-patients-leaked-in-balochistan/.

[15] Mir, A. M. (2021, April 21). Digital health: the future of healthcare in Pakistan. Express Tribune. Retrieved February 17, 2023, from https://tribune.com.pk/story/2295812/digital-health-the-future-of-healthcare-in-pakistan.

[16] Sulaman et al. (2022, February). Beyond COVID-19: Prospect of telemedicine for obstetrics patients in Pakistan. International Journal of Medical Informatics. Retrieved February 17, 2023 from https://www.sciencedirect.com/science/article/pii/S1386505621002793

[17] Bilal et al. (2022, September). Digital health and telemedicine in Pakistan: Improving maternal healthcare. Annals of Medicine and Surgery. Retrieved February 17, 2023 from https://www.sciencedirect.com/science/article/pii/S2049080122011852?via%3Dihub

[18] Jahangir, R. (2020, March 31). Govt launches virus information service on WhatsApp. Dawn.com. Retrieved February 17, 2023, from https://www.dawn.com/news/1545149.

[19] Chudnovsky, S. (2020, April 14). World Health Organization Launches Messenger Experience to Help Deliver Accurate Information on COVID-19. Messengernews.fb. Retrieved 17 February, 2023, from https://messengernews.fb.com/2020/04/14/world-health-organization-launches-messenger-experience-to-help-deliver-accurate-information-on-covid-19/

[20] Admin & Admin. e-Cards (Health). NADRA website. Retrieved 17 February, 2023, https://www.nadra.gov.pk/solutions/secure-document-solutions/e-health-cards/

[21] Admin & Admin. e-Cards (Health). NADRA website. Retrieved 17 February, 2023, https://www.nadra.gov.pk/solutions/secure-document-solutions/e-health-cards/

[22] Digital Policy E-Health Revised with Changing. DigitalPakistan.pk. Retrieved February 17, 2023 from https://digitalpakistan.pk/pdf/d-health.pdf

[23] Digital Policy E-Health Revised with Changing. DigitalPakistan.pk. Retrieved February 17, 2023 from https://digitalpakistan.pk/pdf/d-health.pdf

[24] Kinshella et al. (2021, May 14). "Now You Have Become Doctors": Lady Health Workers' Experiences Implementing an mHealth Application in Rural Pakistan. Frontiers in Global Women's Health. Retrieved February 17, 2023, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8594017/

[25] Zahid et al. Perception and attitude of Pakistani doctors towards the use of telemedicine technology. Cureus.com. Retrieved February 17, 2023, from https://www.cureus.com/articles/122254-perception-and-attitude-of-pakistani-doctors-toward-the-use-of-telemedicine-technology#!/references

[26] Ahmed, A., Ahmed, M. (2018, December). The Telemedicine Landscape in Pakistan-Why are we falling behind?. Journal of the Pakistan Medical Association. Vol.68 Issue 12. Retrieved 17, February 2023, from https://jpma.org.pk/article-details/8973?article_id=8973

[27] Ahmed, A., Ahmed, M. (2018, December). The Telemedicine Landscape in Pakistan-Why are we falling behind?. Journal of the Pakistan Medical Association. Retrieved February 17, 2023, from https://jpma.org.pk/PdfDownload/8973

[28] Daudpota, F. (2016, December 17). Pakistan: Need for Statutory Safeguards as to Privacy of Health Information. SSRN. Retrieved February 17 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2886918

[29] Daudpota, F. (2016, December 17). Pakistan: Need for Statutory Safeguards as to Privacy of Health Information. SSRN. Retrieved February 17 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2886918

[30] Kazim, F. (2007, June). Critical analysis of the Pakistan Medical Dental Council Code and Bioethical Issues. Centre for Applied Ethics Linköpings universitet. Diva Portal. Retrieved 17 February 2023, from https://www.diva-portal.org/smash/get/diva2:23919/FULLTEXT01.pdf

[31] Jafree, S. R., Zakar, R., Fischer, F., & Zakar, M. Z. (2015). Ethical violations in the clinical setting: The hidden curriculum learning experience of Pakistani nurses. BMC Medical Ethics, 16(1). https://doi.org/10.1186/s12910-015-0011-2

[32] Zahid, N., Ali, A., Gul, B., Danish, S. H., Israr, S. N., & Anwar, J. (2022). Perception and attitude of Pakistani doctors toward the use of telemedicine technology. Cureus. https://doi.org/10.7759/cureus.31556

[33] Wetzels, M., Broers, E., Peters, P., Feijs, L., Widdershoven, J., & Habibovic, M. (2018). Patient perspectives on Health Data Privacy and management: "Where is my data and whose is it?" International Journal of Telemedicine and Applications, 2018, 1–6. https://doi.org/10.1155/2018/3838747

[34] Wetzels, M., Broers, E., Peters, P., Feijs, L., Widdershoven, J., & Habibovic, M. (2018). Patient perspectives on Health Data Privacy and management: "Where is my data and whose is it?" International Journal of Telemedicine and Applications, 2018, 1–6. https://doi.org/10.1155/2018/3838747

[35] Willinger, M. L. (2015, June). Patient perception of privacy and the role of Electronic Medical Records. Union | Digital Works. Retrieved February 17, 2023, from https://digitalworks.union.edu/cgi/viewcontent.cgi?article=1404&context=theses

[36] Government of Canada. (2022, October 1). Privacy Act. Justice Laws Website - Site Web de la législation (Justice). https://laws-lois.justice.gc.ca/eng/acts/P-21/index.html

[37] Saleem, S. G., Ali, S., Ghouri, N., Maroof, Q., Jamal, M. I., Aziz, T., Shapiro, D., & Rybarczyk, M. (2022). Patient perception regarding privacy and confidentiality: A study from the Emergency Department of a tertiary care hospital in Karachi, Pakistan. Pakistan Journal of Medical Sciences, 38(ICON-2022). https://doi.org/10.12669/pjms.38.icon-2022.5785

[38] Shirazi, B., & Shekhani, S. (2021). Patient’s expectations of privacy and confidentiality in Pakistan: A mixed-methods study. Journal of the Pakistan Medical Association, 1–6. https://doi.org/10.47391/jpma.888

[39] Shirazi, B., & Shekhani, S. (2021). Patient’s expectations of privacy and confidentiality in Pakistan: A mixed-methods study. Journal of the Pakistan Medical Association, 1–6. https://doi.org/10.47391/jpma.888

[40] Kazmi, S., Yasmin, F., Siddiqui, S. A., Shah, M., Tariq, R., Nauman, H., Saeed, U., Hassan, A., Asghar, M. S., & Hussain, T. (2022). Nationwide assessment of knowledge and perception in reinforcing telemedicine in the age of COVID-19 among medical students from Pakistan. Frontiers in Public Health, 10. https://doi.org/10.3389/fpubh.2022.845415

[41] Riaz, S., Khan, E., & Jaffar, T. (2017). Ethics In Health Care Settings: Practices of Healthcare Professionals and Perceptions of Patients Regarding Informed Consent, Confidentiality and Privacy at Two Tertiary Care Hospitals of Islamabad, Pakistan. Journal Of Ayub Medical College Abbottabad - Pakistan, 29(3), 472–476. https://doi.org/https://jamc.ayubmed.edu.pk/jamc/index.php/jamc/article/view/2805/1068

[42] Riaz, S., Khan, E., & Jaffar, T. (2017). Ethics In Health Care Settings: Practices of Healthcare Professionals and Perceptions of Patients Regarding Informed Consent, Confidentiality and Privacy at Two Tertiary Care Hospitals of Islamabad, Pakistan. Journal Of Ayub Medical College Abbottabad - Pakistan, 29(3), 472–476. https://doi.org/https://jamc.ayubmed.edu.pk/jamc/index.php/jamc/article/view/2805/1068

[43] Aziz, J., Malik, A., & Fatima, N. (2021, September 16). Health v. privacy in the age of cyber surveillance - research society of international law. Research Society of International Law. Retrieved February 17, 2023, from https://rsilpak.org/2020/health-v-privacy-in-the-age-of-cyber-surveillance/

[44] Jahangir, R. (2020, March 24). Govt starts cell phone tracking to alert people at virus risk. DAWN.COM. Retrieved February 17, 2023, from https://www.dawn.com/news/1543301

[45] Qazi, M. S., & Ali, M. (2011). Health Management Information System Utilization in Pakistan: Challenges, pitfalls and the way forward. BioScience Trends, 5(6), 245–254. https://doi.org/10.5582/bst.2011.v5.6.245

[46] Brown, J., Ryan, C., & Harris, A. (2014). How doctors view and use Social Media: A national survey. Journal of Medical Internet Research, 16(12). https://doi.org/10.2196/jmir.3589

[47] Brown, J., Ryan, C., & Harris, A. (2014). How doctors view and use Social Media: A national survey. Journal of Medical Internet Research, 16(12). https://doi.org/10.2196/jmir.3589

[48] Brown, J., Ryan, C., & Harris, A. (2014). How doctors view and use Social Media: A national survey. Journal of Medical Internet Research, 16(12). https://doi.org/10.2196/jmir.3589

[49] EMRO, W. H. O. (2023). Health Service Delivery. World Health Organization. Retrieved February 17, 2023, from https://www.emro.who.int/pak/programmes/service-delivery.html

[50] Tertiary Care | Specialized Healthcare & Medical Education Department . Specialized Healthcare & Medical Education Department . (2018). Retrieved February 17, 2023, from https://health.punjab.gov.pk/TertiaryCare.aspx

[51] Khan, M. I. (2015, March 24). Pakistan takes aim at SIM cards in anti-terror drive. BBC News. Retrieved February 17, 2023, from https://www.bbc.com/news/world-asia-31924186

[52] PITB. (2023). Disease surveillance system. PITB. Retrieved February 17, 2023, from https://pitb.gov.pk/dss

[53] Portal, P. (2023). Health Department | Punjab Portal. Retrieved February 17, 2023, from https://www.punjab.gov.pk/narowal_health

[54] Wolford, B., 2021. What is GDPR, the EU's new data protection law? - GPR.eu. [online] GDPR.eu. Retrieved 7 July 2021 from https://gdpr.eu/what-is-gdpr

[55] MoITT. (2023). Draft Policies | Ministry of Information Technology and Telecommunication (MoITT). MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION. Retrieved February 17, 2023, from https://www.moitt.gov.pk/Detail/NzUyZGE0MWMtMmYzZC00YmIzLTk2ODUtYmVjNTk1Nzg4MTBm

[56] EU. (2019, September 2). Recital 51 - protecting sensitive personal data. General Data Protection Regulation (GDPR). Retrieved February 17, 2023, from https://gdpr-info.eu/recitals/no-51/

[57] Good Thinkers Organization. (2016, July). Recognition of Third-Gender: Realizing the Plight and Rights of Transgender Community in Punjab (Pakistan). https://www.gtopakistan.org/wp-content/uploads/2021/03/Situation-Assessment-Report-Recognition-of-Transgender.pdf

[58] Health and Access to Care and Coverage for Transgender Individuals in Pakistan: A Call for Action. (2017). RHRN Young Omang.

[59] UNDP. (2022). Procurement-notices.undp.org. UNDP | Pakistan Global Fund HIV Prevention and Treatment Programme . Retrieved February 17, 2023, from https://procurement-notices.undp.org/view_file.cfm?doc_id=313444

[60] UNAIDS. (2017, April). Integrated biological and behavioral surveillance in Pakistan: Round 5 - 2016-17. HIV/AIDS Data Hub for the Asia Pacific. Retrieved February 17, 2023, from https://www.aidsdatahub.org/resource/ibbs-pakistan-round-5-2016-2017

[61] PMDC. (2018). PM&DC professional ethics and code of conduct - pmc.gov.pk. PM&DC Professional Ethics and Code of Conduct. Retrieved February 17, 2023, from https://www.pmc.gov.pk/Documents/law/PMDC%20Code%20of%20Ethics%202018.pdf

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

https://digitalrightsfoundation.pk

info@digitalrightsfoundation.pk

www.twitter.com/digitalrightsPK

www.instagram.com/digitalrightsfoundation

www.facebook.com/DigitalRightsFoundation

www.tiktok.com/@digitalrightsfoundation