A PRIVACY PERSPECTIVE:

THE COLLECTION AND USE OF HEALTH DATA IN PAKISTAN

A STUDY BY DIGITAL RIGHTS FOUNDATION

DRF
DigitalRightsFoundation

About

Digital Rights Foundation (DRF) is a Digital Rights Foundation (DRF) is a feminist, not-for-profit organisation based in Pakistan working on digital freedoms since 2013. DRF envisions a place where all people, especially women and gender minorities, can exercise their right of expression without being threatened.

DRF believes that a free internet with access to information and impeccable privacy policies can create safe online spaces for not only women but the world at large.

Contact information:

info@digitalrightsfoundation.pk
www.digitalrightsfoundation.pk

Acknowledgements

This report would not have been possible without the hard work of our research team comprising of ShehrBano Hassan, Zainab Durrani and Zaman Karamat; and the revision and editing by the Head of Research and Policy, Shmyla Khan, the design work by Ahsan Zahid and Talha Umar and the support of Privacy International.

We are also grateful to all the individuals who agreed to participate in our research and provided the valuable data that make up the findings and analysis of this report.

Table Of Content

Executive Summary

This research was motivated by the desire to understand the ways in which privacy is understood and practiced in hospitals, particularly in the context of the COVID-19 pandemic. Though privacy is already somewhat embedded within medical practices and training, the COVID-19 pandemic brought about an unprecedented escalation of reliance on digital technologies, leading to new questions about the ways in which privacy is perceived and practiced in various fields across Pakistan. Coupled with the weak legislative and institutional infrastructure of countries like Pakistan, it becomes particularly imperative to investigate whether appropriate checks and balances exist to ensure and protect the privacy of individuals. At the time of publishing this report, Pakistan does not have a specific data protection law, nor does it have any legislation allowing individuals the right to request data about themselves. The main governing legislation around crimes in the digital sphere is PECA (Prevention of Electronic Crimes Act 2016), which has come under severe criticism for its harsh penalties for speech acts and its potential for abuse and misuse. In fact, concepts such as data privacy and protection are often basic and superficially understood in Pakistan. This is further corroborated by the fact that health data privacy is a relatively under-studied subject in Pakistan, leading to a lack of implementation and understanding of its principles in practice. Considering this, the aim of this study is to unpack the ways in which privacy is understood and practiced in the health sector of Pakistan. Moreover, we seek to identify the gaps in information and practice between the state, the healthcare commission, healthcare administration in hospitals and individuals practicing medicine in hospitals.

a. Main Objectives

- Investigate the the collection and use of health data in Pakistan
- Understand how, in the context of COVID-19, privacy practices and perceptions have evolved
- Explore the unique challenges posed to data privacy implementation in Pakistan with regards to health data
- Map and analyse the experiences of doctors and hospital staff
- Contribute to literature on privacy experiences and practices during COVID-19

b. Key Outcomes

- There is an alarming gap in knowledge, information and understanding around privacy practices in the healthcare sector in Pakistan.

- The emphasis on and importance given to privacy is mostly up to the individual medical practioner's discretion, with little to no translation of medical training to institutional practice in hospitals.

- Though there is sometimes relevant training provided to medical practitioners, data collection, access and storage practices suggest that the lack of checks and balances allow unauthorized sharing of personal information without redress.

- There is a lack of transparency around data sharing between medical institutions and third parties and stakeholders, including government departments.

- Doctors and healthcare professionals value privacy, both as employees and for their patients, however, they are unable to implement this beyond individual choices due to lack of institutional support.

- The most vulnerable individuals in such cases are primarily patients and female doctors who are often subject to various privacy harms involving their personal data and information.

Introduction

The COVID-19 pandemic saw significant developments in areas such as the technology industry and healthcare sector. In fact, the world witnessed technology being used for healthcare purposes more than ever during the COVID-19 health crisis.[1] Telehealth, virtual consultations, health applications on electronic devices, contact tracing, and digital health databases were employed to detect and contain the virus all around the world.[2] While this collaboration brought many beneficial changes and upgrades to healthcare, this was not consistent across the world with many states overlooking privacy entirely. Others failed to fully adopt virtual systems or secure them properly, be it through policies or protective mechanisms. According to the UNCTAD, 16% of the world does not have any "data protection and privacy legislation" effectively risking the security of millions of peoples' health data,[3] a concerning statistic in a hyper digitised world.

Technological advancements in the medical sector have made healthcare more affordable,[4] accessible, and efficient.[5] However, digital security is a major concern for many considering the number of data breaches that continue to occur around the world — over two hundred million health records in the last decade have been leaked in the United States alone.[6] It is clear then that even highly developed states are not immune to such violations. Many developing countries such as Bangladesh, Sri Lanka and India lack proper privacy and data protection laws[7] and lag when it comes to protecting their citizens' health data. The lack of such legislations have had consequences: Jio, an Indian telecommunications company, suffered from a massive security breach exposing "millions of symptom checker app logs".[8] Pakistan also falls into this category and has lax regulations around data protection,[9] which are often not enforced or followed.

---

[1] https://businesslawtoday.org/2020/03/covid-19-data-privacy-health-vs-privacy/
[2] https://jamanetwork.com/journals/jama/article-abstract/2765252
[3] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[4] https://mhealth.amegroups.com/article/view/16494/16602
[5] https://www.jmir.org/2020/7/e17508/
[6] https://www.hipaajournal.com/healthcare-data-breach-statistics/
[7] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[8] https://privacyinternational.org/examples/3831/india-jio-security-breach-exposes-millions-symptom-checker-app-logs
[9] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

During the pandemic, an increase in health data collection for virus containment prompted questions around privacy. Countries adopted methods such as contact tracing, which has been extensively criticised for being an invasive tool and vulnerable to abuse.[10] Location tracking[11] and other, more aggressive methods, such as the use of drones, were also employed in the other states such as China, Norway, Bahrain and Kuwait.[12] Corporations such as Baidu found their way into the healthcare space too. Baidu assisted the Chinese government in providing teleconsultations, but also collected massive amounts of personal medical data citizens were providing on a large scale in the process; due to a lack of legal safeguards, the data Baidu collected is at risk of being exploited for financial gains.[13] Unauthorised access to data and accidental leaks are also common and on the rise, as reported by the Health Insurance Portability and Accountability Act (HIPAA) Journal.[14]

Despite Pakistan having institutions such as the Punjab Health Commission which are designed to protect health data,[15] there continue to be vulnerabilities in the system. Electronic Healthcare Records (EHR) and Health Management Information Systems (HMIS) are clearly at risk with this context in mind. Considering the importance of privacy in medical practice and education, the privacy practices and state provisions to protect health data in Pakistan requires investigation.

In light of these findings, this study aims to investigate the existence of gaps in privacy and data security with regards to Pakistan's healthcare system's framework. Additionally, we investigate whether existing policies are sufficient in protecting citizens' from privacy violations, particularly given the unique nature of challenges during the pandemic.

[10] https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-
[11] danger-for-privacy/
[12] https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa
[13] https://businesslawtoday.org/2020/03/covid-19-data-privacy-health-vs-privacy/
[14] https://businesslawtoday.org/2020/03/covid-19-data-privacy-health-vs-privacy/
[15] https://www.hipaajournal.com/healthcare-data-breach-statistics/
https://phc.org.pk/privacypolicy.aspx

Methodology

Qualitative data was gathered for this research, involving in depth interviews with a limited number of hospital staff, including doctors, medical students and administrators in the healthcare sector. Both public and private hospitals were considered in the study. It was initially proposed that a combination of mixed methodologies be used for data gathering. However, due to the ongoing COVID-19 pandemic, data gathering from doctors was particularly hindered due to the added burden to the healthcare sector in Pakistan. As such, it was decided that in depth interviews with a limited number of doctors will provide us with a closer understanding of what privacy perceptions and practices look like during COVID in the healthcare sector in Pakistan.

We conducted a total of 10 interviews for around 1.5 hours for each participant. The interviews were semi structured, which allowed doctors to express their personal concerns, elaborate on experiences and address particular questions as well. This data was essential to identify the gaps between government policy, hospital measures and individual experiences of those involved on the frontline. Finally, data from the interviews was compiled and analysed. The insights from these findings are provided in this report and supported by a literature review.

Limitations

It must be noted that this study does not claim to capture the experiences of all hospital staff, medical students or healthcare administrators. Indeed, there are experiences that are not represented within this study purely due to the nature of the methodology, particularly with regards to doctors outside of the Punjab province, due to accessibility issues. Moreover, doctors from private hospitals were also disproportionately represented due to the process of dissemination due to the ongoing COVID-19 pandemic. Therefore, to make generalizable inferences based on this data set would be an error. Furthermore, data-gathering was hindered due to various issues such as limited availability of participants and internet connectivity problems. Most notably, due to time constraints, it was not possible to interview patients who had received treatments in hospitals, which would highlight a key missing element from this study. With a greater data set and increased respondents, the findings may be substantiated and strengthened further in the future.

Literature review

a. The state of health data privacy

Amidst the Covid-19 pandemic, the global health space experienced a surge in development and digitisation, and saw an influx of health data — over two-hundred-and-sixty-two million people contracted the coronavirus.[16] Data collection in the form of contact tracing, modelling and documentation were some common tactics used to tackle the pandemic, however, such methods raised concerns across the globe.[17] Korea, one of the first affected countries, encountered many instances of data breaches, and called for a privacy review prompted by the Korean National Human Rights Commission.[18]

> "The locations of infected individuals attracted extensive news coverage at times. For some cases, the general public engaged in profiling and unveiled or inferred embarrassing personal details. Re-identification allegedly took place on a few occasions. Some of these individuals were affected by unwanted privacy invasion and even became subject to public disdain. Concerns were raised regarding the uneven scope and granularity of disclosures by municipal and local governments".[19]

Statistics published by the Health Insurance Portability and Accountability Act (HIPAA) Journal, gesture that the state of health data privacy is fragile; between 2009 and 2020 268,189,693 healthcare records were exposed, lost or stolen — approximately 81.72% of the United States' total population.[20] On most occasions these breaches were attributed to "hacking", which went undetected.[21] While laws around patient data confidentiality exist, they are often violated; 2020 saw the most "unauthorised disclosure incidents" in the past ten years in the United States and while these violations are fined and punishable, the number of data breaches and their severity only seem to be rising.[22]

---

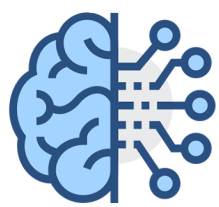
[16] https://covid19.who.int
[17] https://jamanetwork.com/journals/jama/article-abstract/2765252
[18] ibid
[19] ibid
[20] https://www.hipaajournal.com/healthcare-data-breach-statistics/
[21] ibid
[22] ibid

b. Development and history of "digital health"

Digital health data management systems have existed since the 1960s, however they were popularised and became more widely used in the 1980s, when desktop computers became more common.[23] Ismail et al (2020), attribute the development of digital health data management systems over the years to the need for more affordable healthcare solutions,[24] better and more efficient health care, data accessibility, organisation, and even to prevent fraud.[25] In recent decades it has become a core component of the healthcare sector.

> "According to a National Physician survey in 2014, 75% of Canadian physicians have begun using electronic medical records instead of the traditional paper method. With the use of electronic medical records, it is suggested this will increase productivity and keep a better track of each patient and their records."[26]

These data rich systems, compromise of Electronic Health Records (EHR) which have been used for "governance and research";[27] however, since this framework is ever evolving with the needs of the healthcare sector, many concerns arise including those focused on digital privacy.[28] Institutions around the world have developed measures to address these concerns and prevent data breaches; Pakistan, Punjab specifically, for example, has the Punjab Health Commission which monitors and maintains records, investigates system failures and malpractice, and implements policies meant to secure privacy.[29]



E-health or digital health, despite sounding similar, are defined differently than EHRs and digital health management systems, though they share some goals. According to the World Health Organization "digital health" includes the use of "health-related information, resources and services provided electronically", "large volumes of data from different sources that can provide valuable insights into population health" and "artificial intelligence (AI) to perform tasks that would normally require human capacities".[30] Furthermore the United States Food

[23] https://www.vertitechit.com/history-healthcare-technology/
[24] https://mhealth.amegroups.com/article/view/16494/16602
[25] https://www.jmir.org/2020/7/e17508/
[26] https://www.ideatheorem.com/insights/the-emergence-of-digital-health-care-current-and-future-trends/
[27] https://www.jmir.org/2020/7/e17508/
[28] ibid
[29] https://phc.org.pk/privacypolicy.aspx
[30] https://www.euro.who.int/en/health-topics/Health-systems/digital-health/news/news/2019/2/what-you-need-to-know-about-digital-health-systems

and Drug Administration (FDA) adds that digital health refers to a broader set of healthcare categories which include tele-health, mobile health, and the use of mobile or wearable health devices.[31] Digital health has seen exponential growth during the pandemic and its multitude of lockdowns, especially in Pakistan where an increasing number of e-clinics are being established.[32] A United Nations Development Program (UNDP) report stated that tele-medicine is playing a "pivotal role" in aiding patients and concerned citizens, in population dense states like Pakistan.[33]

c. Digital Health and data ownership

In 2019 there were 505 health data breaches, exposing 41.2 million people in 86 different countries.[34] In 2020, 40 million people's health data was exposed in the United States alone.[35] These figures are difficult to obtain for Pakistan since there is no obligation on institutions to report data breaches in the absence of a data protection law. Trends show that data breaches are becoming more common, however in certain states data protection laws still do not exist. Edwin Morley-Fletcher, a researcher for Lynkeus, argues that patients do not have control over who uses "their personal information and for what purposes" and attributes the lack of these rights to the growing number of privacy breaches and identity theft instances.[36]

In recent years the amount of data collected from patients has increased greatly, both in quantity and detail.[37] The Institute of Medicine (US) Committee on Regional Health Data Networks highlighted that the increasing digitisation of health data has made way for the documentation of people's "lifestyles, family history and health status" — information considered to be incredibly personal.[38] Furthermore, they mention what was "once considered the business of patients and possibly their physicians has now become the business of such groups as: (1) officers of government entitlement programs checking on eligibility, and on patient and provider fraud and abuse; (2) agencies granting security clearance; (3) attorneys bringing criminal or civil charges; and (4) social service workers protecting possibly abused children…".[39]

---

[31] https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health
[32] https://www.pk.undp.org/content/pakistan/en/home/blog/2020/how-telemedicine-is-helping-in-the-fight-against-covid-19--and-w.html
[33] ibid
[34] https://www.mdpi.com/2227-9032/8/2/133
[35] https://www.theverge.com/2021/12/8/22822202/health-data-leaks-hacks
[36] https://cordis.europa.eu/article/id/418078-a-new-paradigm-for-healthcare-data-privacy
[37] https://www.ncbi.nlm.nih.gov/books/NBK236546/
[38] ibid
[39] ibid

Digitally stored health data is vulnerable to cyberattacks, and is often sold to pharmaceutical companies or other corporations by hackers. Certain regions, such as Europe are beginning to adopt new privacy protection laws and regulations, such as the General Data Protection Regulation (GDPR) which "requires data processors and controllers to provide users with their own data, clearly disclose data collection, set high-privacy defaults and more".[40] The GDPR was designed to give citizens of the European Union rights over their data, but some concerns still remain, such as those regarding consent and explicit consent.[41]

While the European Union may have instituted regulations, 16% of the world does not have any privacy protection laws and another 10% has drafted legislations but have not put them into effect, according to the United Nations Conference on Trade and Development.[42]

d. DNA and data: a new frontier of privacy risks

Technological progress has penetrated every sector of the healthcare industry and has led to the commercialisation of DNA testing and ancestry tracing; companies such as "23andMe" and "MyHeritage" sell kits "to determine consumers' genetic ancestry" -- 23andMe also offers services such as medical tests.[43] The private ownership of such companies raises concerns around data privacy, since these tests produce a substantial amount of sensitive information about individuals. Data protection obligations for companies, as well as data sharing are issues that must be addressed.

The commercialization of DNA testing also raises concerns around where the data collected or produced is going. Jennifer King, a privacy specialist at the Stanford Institute for Human-Centered Artificial Intelligence questioned "why these different companies and investors have a financial interest in your genetic data".[44] These concerns are valid considering MyHeritage reported that it was hit by a major data breach -- 92 million accounts were exposed to hackers.[45] Another genetics company also suffered from such attacks and lost 1 million people's DNA data.[46]

---

[40] https://www.govtech.com/security/researchers-data-privacy-in-healthcare-needs-boost.html
[41] https://www.pega.com/insights/articles/gdpr-and-healthcare-understanding-health-data-and-consent
[42] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[43] https://www.theguardian.com/technology/2021/feb/09/23andme-dna-privacy-richard-branson-genetics
[44] ibid
[45] https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics
[46] https://www.theguardian.com/technology/2021/feb/09/23andme-dna-privacy-richard-branson-genetics

Hackers are not the only groups interested in DNA data. 23andMe has been sharing health data with big pharmaceutical corporations such as GlaxoSmithKline to develop new drugs.[47]

> "And there are plenty of players interested in DNA: researchers want genetic data for scientific studies, insurance companies want genetic data to help them calculate the cost of health and life insurance, and police want genetic data to help them track down criminals…"[48]

DNA testing is still considered a relatively new phenomenon, and while companies like 23andMe claim to secure their data[49]--data breaches continue to be reported and third party sharing is common.

e. COVID-19 and state actions

A major dilemma emerged during the pandemic: tools, such as contact tracing and self-reporting, used to stop the spread of the virus, safeguarding the health of many, were also responsible for a number of privacy infringements.[50] Individuals were flagged and anonymity was forgotten, as mentioned earlier in the case of South Korea. Claypoole, in his article for the American Bar Association, explores the different methods in which governments and corporations collected health data in an attempt to reduce infection rates, and also how that data was used.[51]

Claypoole cited multiple examples, the first of which was China, where government surveillance went beyond contact tracing and used additional methods to monitor citizen activity.[52] The Chinese government used drones to detect body temperature and flag those who may have been infected; they used electronic devices to observe isolated individuals; and they also used facial recognition to "identify commuters not wearing masks".[53] The government also collaborated with "Baidu", a search engine company, to provide telemedicine solutions.[54] At first glance, these tools seem effective and advanced, however, At first glance, these tools seem effective and advanced, however, they breached the privacy of citizens; once instance being

---

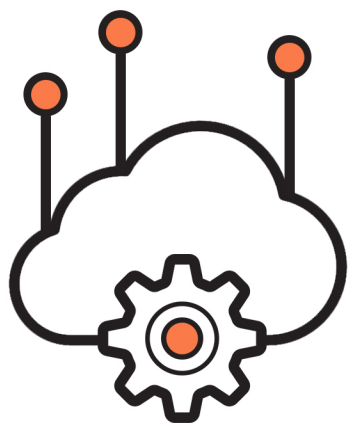
[47] ibid
[48] https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics
[49] https://www.theguardian.com/technology/2021/feb/09/23andme-dna-privacy-richard-branson-genetics
[50] https://businesslawtoday.org/2020/03/covid-19-data-privacy-health-vs-privacy/
[51] ibid
[52] ibid
[53] ibid
[54] ibid

the drones and door monitors which track people's movements.[55] Additionally, China does not have adequate laws to protect the information collected by corporations like Baidu, or limit what they can do with it.[56]

Amnesty International, in their analysis of contact tracing applications, spotlit Bahrain and Kuwait for severely breaching the privacy of their citizens.[57] Claudio Guarnieri, the head of Amnesty International's security lab, explained that these states used a centralized model for data collection and were "essentially broadcasting the locations of users to a government database in real time".[58]

The Human Rights Watch has openly criticised these methods, especially those which involve location tracking using mobile data, suggesting they could be for nefarious purposes and lead to human rights violation.[59] Furthermore, they highlight that mobile data does not merely comprise of a user's location, but also demographic information such as their "identity, location, behavior, associations, and activities" – information companies could exploit.[60]

Concerns around what happens to health data collected by governments are increasing. Individual health data is being used outside the healthcare sector, changing the context in which this data can be processed and utilized.[61]



[55] ibid
[56] ibid
[57] https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/
[58] ibid
[59] https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa
[60] ibid
[61] https://businesslawtoday.org/2020/03/covid-19-data-privacy-health-vs-privacy/

f. Pakistan's legal landscape and healthcare

Pakistan has often been criticized for its lack of privacy laws; legislation around data protection has been a work in progress since 2018, when the government first drafted a bill titled "Personal Data Protection Bill".[62] While the first version of the bill included health data, it had many short-comings as highlighted by Privacy International and Digital Rights Foundation, such as the "failure to include data processing activities of public bodies and government within the ambit of the law".[63] Both in 2020 and 2021, the government amended the draft bill making additions around data processing, though it remains unpassed. It should also be noted at this point that the National Institute of Health, Ministry of Health or NCOC do not have accessible privacy policies that are readily available on their website. This could either mean that privacy policies in the core departments and institutions focused on health data do not exist, or that these policies are not easily accessible for the average citizen.

A lack of data protection laws, as well as others around consent and medical ethics has prompted researchers to criticize the framework in which healthcare workers are trained and operate. Hyder and Nadeem, in their article, argue that a "lack of effective policy and legislation concerning ethical practice of medicine is reported to have negative effects on the profession".[64] They also suggest that this creates situations where individuals are forced to deal with "ethico-legal issues alone, or in consultation with colleagues, in an informal manner".[65]

Medical ethics and confidentiality are key components of medical training and education. These teachings are meant to ensure patient privacy and safety, however, Shamim and Shamim note that oftentimes crucial segments such as biomedical ethics are left out of certain curricula.[66]

However, like many other topics including disaster, information, education and communication, medical ethics is also not formally taught in most of the medical colleges of the country.[67] Considering Pakistan is a country which enshrines privacy

---

[62] https://moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill%20without%20track%20changes.pdf
[63] https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan#dataprotection
[64] https://www.jstor.org/stable/23498844?read-now=1&refreqid=ex celsior%3A4fd020077925815e58aee35ab29baad8&seq=4#page_scan_tab_contents
[65] ibid
[66] https://jpma.org.pk/PdfDownload/2282
[67] ibid

as a right in its Constitution, in Article 14(1),[68] it is ironic it lacks key policies around ethics, privacy and data protection. This not only puts patient data in a vulnerable position but also hinders Pakistan's citizens' ability to exercise their right to privacy.

Findings

[68] https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan#dataprotection

a. Participant demographics

Of the 10 participants interviewed, three self identified as male while seven identified as female. 8 individuals were from the public sector, employed at government-run hospitals, while 1 was from a private hospital and another from a private practice. Geographically, the participants were concentrated in the urban regions, specifically main cities such as Lahore, Karachi and Peshawar, while one doctor was from a smaller city in Khyber Pakhtunkhwa. With regards to their specific positions within institutions, the participants varied in terms of seniority, ranging from post grad residents to house officers, medical officers and trainee interns. One participant specialised in psychiatry while another was a tele-physician.

b. The state of privacy: Data collection, access and storage

The initial point of investigation was exploring the basic privacy protocols in place in various institutions and the privacy practices hospitals enforced and personnel engaged in on a regular basis. This was split into two categories: firstly, the types of data being collected, stored and accessed regularly in the hospital, i.e. the nature of the data being handled regularly by the hospital. Secondly, the specific rules and protocols issued by the hospital to protect and secure it, i.e. the practices expected of hospital staff and mechanisms to protect patient and doctor data. What initial analysis suggests is a pattern of disconnection between the extent of the data being handled, and the mechanisms in place to protect such data. We begin with an exploration of the data collection, access and storage practices as told directly by our participants.

All participants were asked multiple questions about the nature of data collection, storage, access and sharing in their respective institutions. The first of these questions asked what types of data was collected from both patients and employees upon their arrival in the hospital. The extent of the data was referenced by multiple respondents:

"We collect their name, father/husband's name, age, ethnicity, area, next of kin, emergency contact, blood group, any other illnesses, biodata, CNIC…" [P9]

"Patients who come to the hospital, we have a proper file for them where we collect their name, address and telephone number, especially during Covid-19. We would keep a record of patients during covid-19 because if their tests came back positive we could trace the source." [P4]

A particularly alarming finding was, as several respondents noted, that the collection of data was not done by a member of the medical staff, but rather a receptionist in the hospital who would generate a "slip" and "receipt" of the individual's details to refer them further. In some cases, medical records and history was noted by a doctor or health professional but in other cases, details of the patient were entirely handled by a non-medical professional. When asked whether receptionists and members of the administrative body had been given training on the handling of sensitive personal information, a majority of respondents stated that some limited training was given but it was rarely practiced in an effective and conscientious manner. This will be explored in a later section.

"There will be a non-medical person, and he will be collecting all these things. That [collecting medical history and data] is a doctor's responsibility." P5

As referenced above, P4 claimed that as a result of COVID-19, the extent of data collection had expanded as well as other practices including storage of data as well as sharing practices. However, one respondent elaborated on the less technically advanced nature of their public government hospital, which had rebooting systems in place which automatically removed all patient data from the electronic systems after three months. They were not sure about whether there was a backup of this data anywhere or where this data "went" once it was deleted from their digital records. In line with this, further questions probed the nature of data storage, i.e. whether it was done virtually or physically or both. In keeping with traditional patterns of data storage in Pakistan, most respondents claimed that hospitals kept data both into digital formats and physical copies. As expected, respondents from private hospitals engaged predominantly with digital files due to the higher quality of technological interventions in their institutions, while government hospitals relied on maintaining physical copies. These hybrid systems can become hard to keep track of and monitor especially if institutions do not have dedicated resources to ensure privacy.

"The reception collects this for us and it's stored in a large database. In terms of the outpatient department everything else is done physically and we also have physical copies of everything; physical copies of their biodata, diagnosis, what medications they are on." [P1]

"Data is collected [even for a checkup] because whenever you need to make a slip, an MR number is generated and you need to keep a record of everything." [P5]

"The [medical] numbers of patients are recorded on computers because they make a slip which has each patient's number. Other than that everything is on paper." [P8]

As P8 stated, and several respondents corroborated in their responses, a medical number is generated upon the arrival of a patient into the hospital, through a collection and processing of their data at the reception. This medical number, often a combination of the individual National Identification number (CNIC), is then used to reference them while providing medical care. Collection and use of the CNIC at the point of entry in the hospital, regardless of the nature of the treatment, creates additional privacy concerns of linking individual patient records with larger databases. Given the sensitive nature of this data, we asked participants about access practices involving patient data. In particular, we asked who in the hospital had access to this data and why.

"Anyone with an HMIS ID can access it. All doctors can access it, people who work in the computer or IT department can access it." [P1]

"So people who have access to the data during admission would be the attendant, the patient, the doctor and the staff, basically anyone in the ward." [P7]

These responses are representative of what a majority of doctors insisted: access to data was not a privacy priority for hospitals. In most cases, hospitals did not have a regulatory framework to ensure that a limited number of individuals had access to specific patient data. One participant elaborated on how a doctor from another hospital entirely was able to access patient data without any checks and balance or accountability:

"I was on duty and another hospital's doctor came, he told us he was a doctor, and he took pictures of charts [patient health charts] and was collecting data. We told the administration, but by then he had left. We didn't know why he was taking pictures; we found out later he wasn't from our hospital. We didn't know if he was even a doctor." P4

This suggests that the problem of access is indeed an alarming one in many hospitals in Pakistan and requires immediate attention, as vulnerable data is at risk everyday of violations. This will be elaborated on further in a section on the privacy risks and harms faced by patients and doctors on a regular basis. Delving further into the use of this medical number, we asked participants whether any data was shared by the hospital as a whole and if so, what types of data this was and for what reasons. The responses were extensive, spanning several third party sharing practices. It should be noted that some respondents also insisted that they did not have specific knowledge of these practices and could not confirm whether this was exactly the case. Among the organisations that information was shared with were drug company representatives, corporations and educational institutes.

"Medical representatives, from different drug companies. They send their representatives to hospitals, so they want to keep some point of contact. They usually already have our contact numbers and email IDs." [P8]

"Corporations and schools have access to patients, not exactly written patient data perhap but they will be able to physically come and see patients. Nobody is really going to ask the patient "are you okay with this?" [P1]

"The sehat-insaaf card, they have the data. They have a lot of data like admission time, diagnosis, apart from just demographic data." [P5]

The Sehat Insaf Card, part of the Sehat Sahulat Program allows the identification of those citizens eligible for free healthcare services as part of the social welfare efforts in Pakistan. A brief overview of the Sehat Sahulat Programs shows that there is no specific privacy policy listed, nor any accessible code of conduct on their website. It is only in a "Charter of Services" (dated February 2021) that the "right to privacy of information regarding data of beneficiaries" is listed.[69] This is the only mention of privacy in the document. The absence of any concrete emphasis on privacy within the Sehat Sahulat Program only corroborates the worrying nature of data sharing in the healthcare sector. As data moves between these unregulated spaces, it remains constantly at risk of leaks, violations, misuse and other abuses. This isn't the only potential data sharing partnership that hospitals are engaged in. Most notably, one respondent stated that their respective hospital has a database that is linked with the Punjab Healthcare Commission nation-wide database:

[69] https://pmhealthprogram.gov.pk/downloads/charter.pdf

"The Punjab Health Commission implemented this computerised system, which links all hospitals in Lahore. The government has access to all this health data. The Punjab Health Commission is even digitising prescription records and will be accessible by other hospitals. This is not operational yet, but it will be soon." P3

The knowledge that the Punjab Healthcare Commission, a regulatory body designed to improve the quality, safety and efficiency of the healthcare service industry, may be integrating a wider database of information across the province begs further questions about the state of health data privacy in the coming years. In particular, does the integration of a provincial database for health data mean data for patients will be accessible cross-institutionally? How is privacy ensured in a large database such as this? Does the PHC propose a rigid privacy policy for such a database? These questions remain yet to be answered, but what we discover from these findings is an absence of privacy as a priority in practices across hospitals. Whether it is through the extensive data collection practices, lack of sophistication in data storage or the possibility of unregulated sharing practices when it comes to patient and doctor data, it is clear that medical information in Pakistan is neither safe nor entirely private.

c. Institutional mechanisms to protect data

In addition, we investigated the specific checks and balances that exist in hospitals to uphold privacy and regulate the storage of data. To do this, we asked participants whether their hospitals had any privacy policies or codes of conduct in place. To this, some participants suggested that privacy policies did exist, but were either not enforced or were not accessible. This was either because of language barriers, lack of understanding and implementation issues. Many privacy policies only served as lip service to legal requirements, and were not reflected in privacy practices.

"I have never read it, but we have it. I'm pretty sure it's pretty basic. It's in English." [P1]

"Yeah, they did have patient confidentiality, I remember they told us about something but there was nothing else or formal as such because Pakistan doesn't have any patient confidentiality laws." [P2]

"Guidelines are not followed properly. You have to do it yourself, based on your experience." [P7]

In other cases, participants stated that privacy policies either did not exist or were not enforced primarily because privacy was not considered important and awareness around privacy matters does not exist in healthcare circles. This, however, was in contrast to the participants' views on privacy and the importance they assigned to it. This will be discussed further in detail in a later section.

"Even if we do have policies like this, they are on paper, we don't see them being practised." [P4]

"Employee privacy does not seem to be practised either; doctors were not given any privacy agreement on employment." [P3]

Participants were further asked whether their hospitals had boards of ethics and committees to oversee privacy violations and data breaches. We found that much like the absence of privacy policies and proper implementation, there was a gap in effective mechanisms of accountability with regards to data breaches and privacy violations in hospitals.

"We have a board of directors, who will not be bothered about anything except for when the hospital is not making enough profit. They are meant to be highlighting other things as well." [P1]

"They have never taken any action. I have never seen any work or any action taken. Nor have they stopped anyone from breaching privacy. People come in and take pictures, so data could be leaked." [P10]

Though a majority of participants stated that their hospitals, in keeping with legal requirements, had one or more ethics committees, many emphasized that these bodies were superficial in their effectiveness. Participants recalled how the lack of efficient mechanisms made it difficult to report and address cases, and when cases were brought to the attention of specific committees, little to no action was taken. This is a particularly worrying finding; corroborating findings from the previous section and confirming a weak structure of implementing and regulating privacy practices in hospitals.

d. Government guidance, education and training

To further explore whether there was a similar gap between healthcare institutions, educational institutions and government directives, we asked participants whether they were given any training on medical ethics, specifically whether any guidance or training had been given by government departments. Participants almost unanimously agreed that no major guidelines or training had been issued by the government to their respective hospitals or to them as individual employees in the health sector.

"Not from the government specifically but, like our health department, it's incharge is basically a government employee, so it came from him." [P8]

"There are no written codes of ethics or guidelines given to doctors by the hospital. Supervisors are supposed to teach residents these things. However, this does not happen either." [P3]

As P3 noted, the gap left by government directives and training was not filled by hospitals either. To confirm this, we asked participants specifically about whether they had been given any education around medical ethics, including privacy matters, in their schooling.

"Nobody invests time in teaching me or people at my level. At the student level, they teach you and after that, it's taken for granted that you'll know. There is also a laxity towards confidentiality." [P1]

"Theoretically, we were taught about it, but in practice not so much." [P4]

"You are just thrown into the deep end. We were told a family is coming with a patient, so who are you supposed to talk to since the patient is in an altered level of consciousness? You cannot speak directly to the patient and we have ten people there with them. How do you handle that situation? It's a situation where you learn with time." P9

As stated by the participants, a major gap exists between what is being taught to doctors and students in their medical colleges and universities and any reinforcement during their practicing years. All respondents reported having some training in school, albeit to varying degrees. Some had complete medical ethics training while others had some modules incorporated into their education. It also varied from specialisations; for example, those specialising in psychiatry or psychology

were given more in-depth training while others had limited education on medical ethics, privacy and confidentiality. This gap also suggests that perceptions around privacy matters are deeply influenced by the lack of consistent training and emphasis on medical ethics throughout doctors' careers. This was further corroborated by doctors' personal perceptions and views on privacy.

e. Awareness and perception of privacy

In order to understand the ways in which privacy practices aligned with perceptions of privacy among doctors and medical professionals, we asked doctors about their own ideas of privacy and what importance it held for them. Participants unanimously agreed that privacy was an important factor in their practices and relationships with patients, but also as citizens themselves.

"I need the trust of my patients and I can only earn the trust of my patients if they think I will enforce confidentiality" [P9]

"This is a major concern. If a relative or I got sick, I would never want my privacy to be compromised." [P10]

Though many respondents felt confident in their hospitals' ability to safeguard their privacy and protect data, some claimed that there was a clear lack of awareness around privacy issues in hospitals, among both patients and doctors. This lack of awareness has an adverse effect on the development of institutional mechanisms to protect data, as already demonstrated.

"I think people don't focus on it enough. People feel insecure about talking about their problems because they feel their privacy will be breached. These are very major concerns and they are not addressed properly." [P5]

According to participants, awareness also varies according to seniority and rank as well as gender. As such, senior doctors seem more relaxed and complacent about privacy issues, while younger doctors are more sensitive to privacy issues and data protection.

"Junior doctors are more aware of privacy concerns and confidentiality. 4 out of 10 doctors will actually give patient privacy proper attention. Junior doctors may be more careful about privacy because laws are getting stricter, lawsuits are becoming more common, and it is a proper part of the medical curriculum." [P3]

Similarly, though this wasn't expressed explicitly by participants, female participants seemed more aware of issues around privacy in general, potentially due to the gendered experience of harms. This will be further analysed in the next section on privacy harms and risks.

f. Privacy risks and harms

Finally, participants were asked multiple questions regarding their personal experiences of privacy breaches, and what they feared with regards to data violations in their respectives field of work. Of particular concern was the level of gendered harms faced by female doctors and practitioners in particular Specifically, P3 discussed how her data was leaked multiple times, including her personal details such as phone numbers, relatives' contact information and address. She elaborated on how attendants were able to bribe administrators and technical staff in the hospital into supplying this information to them, leading to the doctor being stalked and harassed by patients and their relatives. Other female participants also corroborated this account of privacy violations faced by female doctors:

"Yes, definitely. In my hospital, I have never given my number to anyone but I still get a lot of calls from insurance companies. Then I wondered who shared my data, and thought that it could have been breached." [P10]

"Yes, these things [doctors' phone numbers being leaked] happen. Not regularly, but it can happen." [P5]

"It is very common for phone numbers [to be shared]. This is very common, especially with junior doctors, like our level. Our numbers are often circulated, which is why people have to keep their work phone number and their personal phone number different." [P8]

In addition to having her information shared, P3 also stated that she often felt unsafe working in the healthcare sector, having been sexually harassed by male doctors on multiple occasions. She also suggested that hospitals lacked awareness around privacy and violations in general, leading to victim-blaming within disciplinary committees. Though responses from female participants largely alluded to an issue of gendered harms and violations, other claims of privacy breaches suggested that doctors of lower rank were at greater risk of having their personal information shared externally.

"The hospital staff, who just work there and are not healthcare professionals; they circulate numbers because they say they'll get help, so they keep the important numbers and exchange them with one another" [P8]

"When a patient is admitted and is assigned a specific doctor's bed and if that doctor is not there at that time, then a colleague will usually give out their number without asking." [P4]

Participants were additionally asked about whether they had witnessed any privacy violations around patients and non-medical employees in their hospitals. Most participants stated that patient privacy was the responsibility of individual doctors and under their watch, no patient privacy had ever been violated. However, two participants specifically mentioned worrying types of violations among patients:

"Yes, I have seen such things [patients pictures and bios] being shared on social media. I ask such people to hide their demographic information or show the relevant part. But sometimes these things happen." [P5]

"Yes, one patient's data was leaked. The patient who came in was HIV positive and doctors discussed him and his condition by name." [P10]

Though it was reassuring to hear of the low frequency of privacy violations among patients, the nature of the small number of violations was concerning. In particular, the sharing and spread of information [including but not limited to sharing photos, videos and detailed medical histories of patients] on social media is particularly grim due to the volatile privacy practices and perceptions amongst the general public in Pakistan. P10's statement in particular shows that patients with illnesses that are stigmatised are particularly at risk of having their data violated, and may require additional protective strategies such as ensured anonymity and limited access to their records. Additionally, doctors could only speak to individual leaks and harms–leaks at the institutional level are often not disclosed nor reported.

Conclusion

These findings paint a bleak picture of privacy practices and perceptions within the healthcare sector in Pakistan. This is true for privacy practices in all spheres of the healthcare sector. Whether it is mechanisms, or lack thereof, within healthcare institutions across the country, or data-involving practices, it is clear that the current status quo within the healthcare sector does little to protect either patient or doctors on a daily basis. This is further strengthened by the vast spectrum of privacy harms faced by both groups, from gendered harms involving non-consensual sharing of information to official data sharing practices within hospitals without the explicit consent of patients. This is largely due to a lack of awareness and information about the importance of protecting data privacy, which was clear during our interviews with participants. Findings suggest that those in healthcare are not concerned about privacy in general and those who are, are unable to articulate those concerns in the language of data privacy. This was particularly true for female doctors, who shared daunting incidents of data violations and privacy breaches while they were working. It is imperative, therefore, to encourage wide scale awareness raising in the public domain on issues of privacy and data protection, particularly by calling on the state to take responsibility for the protection of patient data and the protection of doctors' data while they work. As digitalisation expands and new tools to manage data are developed and used, particularly amid COVID-19, it is important to ensure that the privacy of individuals in the healthcare sector is protected.

Recommendations

- Proper training to be given to hospital staff including doctors and nurses as awareness is necessary and formal instruction would be helpful in encouraging a culture of privacy.

- Written and explicit privacy and security policies at the regulatory (both federal and provincial) as well as hospital level. These policies should be expressly communicated, accessible and regularly reinforced.

- The communication gap between the doctors in the wards and the administrators of the medical facility with respect to patient treatment needs to be addressed to create a better healthcare ecosystem.

- Digitization of medical records and patient history is necessary to cut out the higher probability of human error and lack of back up of these important documents and information that comes with manual record keeping. This should only be accessible by doctors, administration and nurses of the particular institution.

- Lack of proper healthcare infrastructure indirectly contributes to weakened privacy protocols and an inclination towards patients lowering it themselves if the need to raise funds through crowd-funding or Zakat-eligibility arises.

- The preparation for the extreme pressure on hospitals should be done at a government level by allocating greater resources to the healthcare budget, and updating vital medical machinery such as ventilators.

- Doctors and hospital staff need to take care to record medical data and use it in such a manner as to ensure the least probability of a patient's identifiable data being made public or exposed in any way. This includes limiting access to patient data to only those related to the specific case, as well as ensuring anonymity where necessary.

- Consent and transparency need to be implemented as the base pillars of patient care and be effective from the minute induction into the system is done. Patients should be able to decide how much data to share and with whom it can be shared. Informed consent of patients should be taken with regards to their personal information with exceptions for cases where medical treatment is needed in extraordinary circumstances.

- There should be stricter laws on privacy, confidentiality and harassment to counteract the growing breaches in these areas. Obligations should be placed on hos pitals and medical institutions to immediately disclose any instance of breaches and take remedial measures to rectify harms.

- Introduction of a comprehensive and human rights compliant legislation to protect data privacy in Pakistan.

- Privacy of female patients' is especially important to cater to, more so given the lack of SOPs and their implementation in and around operation theatres where at times the patient's body has to be exposed in very intimate ways to allow for the procedure to be conducted. Any privacy policy or protocol should take into account the unique and gendered ways in which personal data can impact individuals.

References

1. “A New Paradigm for Healthcare Data Privacy.” CORDIS. European Commission, August 27, 2021. https://cordis.europa.eu/article/id/418078-a-new-paradigm-for-healthcare-data-privacy/en.

2. “Bahrain, Kuwait and Norway Contact Tracing Apps a Danger for Privacy.” Amnesty International. Amnesty International, August 12, 2021. https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/.

3. “Data Protection and Privacy Legislation Worldwide.” UNCTAD. UNCTAD, December 14, 2021. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

4. “Fears over DNA Privacy as 23andMe Goes Public in Deal with Richard Branson.” The Guardian. Guardian News and Media, February 9, 2021. https://www.theguardian.com/technology/2021/feb/09/23andme-dna-privacy-richard-branson-genetics.

5. “Healthcare Data Breach Statistics.” HIPAA Journal. HIPAA Journal, January 22, 2021. https://www.hipaajournal.com/healthcare-data-breach-statistics/.

6. “How Telemedicine Is Helping in the Fight against COVID-19 (and Why It Should Be Here to Stay).” UNDP. UNDP, January 21, 2021. https://www.pk.undp.org/content/pakistan/en/home/blog/2020/how-telemedicine-is-helping-in-the-fight-against-covid-19--and-w.html.

7. “Mobile Location Data and Covid-19: Q&A.” Human Rights Watch. Human Rights Watch, October 28, 2020. https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa.

8. “Personal Data Protection Bill 2018.” Islamabad, Pakistan: Ministry of Information Technology and Telecommunication , 2018.

9. “Personal Data Protection Bill 2018.” Ministry of Information Technology and Telecommunications. MOITT, 2018. https://moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill%20without%20track%20changes.pdf.

10. “Punjab Healthcare Commission: Privacy Policy.” Punjab Healthcare Commission. Punjab Healthcare Commission, n.d. https://phc.org.pk/privacypolicy.aspx.

11. “State of Privacy: Pakistan.” Privacy International. Privacy International, January 26, 2019. https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan.

12. “The Emergence of Digital Health Care: Current and Future Trends .” Idea Theorem, November 1, 2021. https://www.ideatheorem.com/insights/the-emergence-of-digital-health-care-current-and-future-trends/.

13. “The History of Healthcare Technology and the Evolution of EHR.” VertitechIT, March 11, 2018. https://www.vertitechit.com/history-healthcare-technology/.

14. “What You Need to Know about Digital Health Systems.” World Health Organization. World Health Organization, February 5, 2019. https://www.euro.who.int/en/health-topics/Health-systems/digital-health/news/news/2019/2/what-you-need-to-know-about-digital-health-systems.

15. “Who Coronavirus (COVID-19) Dashboard.” World Health Organization. World Health Organization, n.d. https://covid19.who.int/.

16. Center for Devices and Radiological Health. “What Is Digital Health?” U.S. Food and Drug Administration. FDA. Accessed September 22, 2020. https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health.

17. Chen, Angela. “Why a DNA Data Breach Is Much Worse than a Credit Card Leak.” The Verge. The Verge, June 6, 2018. https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics.

18. Claypoole, Theodore. “Covid-19 and Data Privacy: Health vs. Privacy.” Business Law Today from ABA. Business Law Today, March 26, 2020. https://businesslawtoday.org/2020/03/covid-19-data-privacy-health-vs-privacy/.

19. Hyder, Adnan A., and Sarah Nadeem. “Health Ethics in Pakistan: A Literature Review of Its Present State.” Journal of Health, Population and Nutrition 19, no. 1 (2001): 6–11. http://www.jstor.org/stable/23498844.

20. Information Resources Management Association (IRMA) . Research Anthology on Cross-Industry Challenges of Industry 4.0. Google Books. Hershey, Pennsylvania (701 E. Chocolate Avenue, Hershey, Pennsylvania, 17033, USA): IGI Global, 2021. https://books.google.co.uk/books?id=lMgpEAAAQBAJ&pg=PA1960&lpg=PA1960&dq=physical+data+storage+pakistan&source=bl&ots=3eQF17TW17&sig=ACfU3U2gKvQNPTx0CCnQrDD4lCGG10-jDA&hl=en&sa=X&ved=2ahUKEwjbqsbQ2fz0AhWKilwKHXrODuQQ6AF6BAgNEAM#v=onepage&q=physical%20data%20storage%20pakistan&f=false.

21. Institute of Medicine (US), and Committee on Regional Health Data Networks. "Confidentiality and Privacy of Personal Data." Essay. In Health Data in the Information Age: Use, Disclosure, and Privacy., edited by Molla S Donaldson. Washington (DC): National Academies Press (US), 1994.

22. Ismail, Leila, Huned Materwala, Achim P Karduck, and Abdu Adem. "Requirements of Health Data Management Systems for Biomedical Care and Research: Scoping Review." Journal of Medical Internet Research 22, no. 7 (2020). https://doi.org/10.2196/17508.

23. Meskó, Bertalan, Zsófia Drobni, Éva Bényei, Bence Gergely, and Zsuzsanna Győrffy. "Digital Health Is a Cultural Transformation of Traditional Healthcare." mHealth 3 (September 14, 2017). https://doi.org/10.21037/mhealth.2017.08.07.

24. Ministry of National Health Services Regulations & Coordination Government of Pakistan. "Sehat Sahulat Program: Draft 28th February 2021 'CHARTER OF SERVICES.'" Sehat Sahulat Program, February 28, 2021. https://pmhealthprogram.gov.pk/downloads/charter.pdf.

25. Rohatgi, Jitesh. "GDPR and Healthcare: Understanding Health Data and Consent." Pega, December 17, 2018. https://www.pega.com/insights/articles/gdpr-and-healthcare-understanding-health-data-and-consent.

26. Ross, McKenna. "Researchers: Data Privacy in Health Care Needs Boost." GovTech. GovTech, April 21, 2021. https://www.govtech.com/security/researchers-data-privacy-in-healthcare-needs-boost.html.

27. Sangchul Park, JSD. "Privacy Controversies around Information Technology–Based COVID-19 Tracing in South Korea." JAMA. JAMA Network, June 2, 2020. https://jamanetwork.com/journals/jama/fullarticle/2765252.

28. Seh, Adil Hussain, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. “Healthcare Data Breaches: Insights and Implications.” Healthcare 8, no. 2 (2020): 133. https://-doi.org/10.3390/healthcare8020133.

29. Shamim, Muhammad Shahid, and Muhammad Shahzad Shamim. “Medical Ethics: A Slow but Sustained Revolution in Pakistan’s Healthcare.” Journal Of Pakistan Medical Association (JPMA). JPMA, September 1, 2010. https://www.-jpma.org.pk/PdfDownload/2282.

30. Shamim, Muhammad Shahid, and Muhammad Shahzad Shamim. “Medical Ethics: A Slow but Sustained Revolution in Pakistan’s Healthcare.” Journal Of Pakistan Medical Association 60 (September 2010): 706–7. https://doi.org/ https://jpma.org.pk/PdfDownload/2282.

31. Wetsman, Nicole. “Over 40 Million People Had Health Information Leaked This Year.” The Verge. The Verge, December 8, 2021. https://www.theverge.com /2021/12/8/22822202/health-data-leaks-hacks.

32. Whittaker, Zack. “India: Jio Security Breach Exposes Millions of Symptom Checker App Logs.” Privacy International. Privacy International, May 2, 2020. https://privacyinternational.org/examples/3831/india-jio-security-breach-exposes-millions-symptom-checker-app-logs.

DigitalRightsFoundation