Security for Health

An Exploration of Cybersecurity, eHealth, and Sustainable Development Goal Three

Candidate 1048810

A thesis presented for the degree of
Masters of Computer Science
Trinity 2021

Word Count: 22,915
(Source: Overleaf Estimate)

Department of Computer Science
University of Oxford
United Kingdom

Abstract

eHealth - the incorporation of information and communications technologies (ICT) into healthcare - is widely regarded as crucial towards achieving universal health care and, by extension, the third Sustainable Development Goal. Yet while healthcare cybersecurity is a common topic of research and concern, its lessons are not always applied to developing eHealth programs. This thesis acts to examine the concept of cybersecurity for healthcare at all levels of development, arguing that security controls can be built into diverse eHealth programs in order to assure the benefits of ICT. Using the 2015 WHO eHealth survey as a guide, we explore eHealth policies, eHealth legislation, mHealth and telehealth programs, and electronic health records in order to gain an understanding of the state of cybersecurity in healthcare around the world and what security controls could help to enhance the confidentiality, integrity, and availability of data and systems.

Contents

Chapter 1

Introduction

Ensure healthy lives and promote well-being for all at all ages.

- United Nations Sustainable Development Goal Three [1]

eHealth - the incorporation of information and communications technologies (ICT) into healthcare - is a discipline in which the impact of cybersecurity is clear. Patient records contain deeply sensitive information attractive to attackers; connected systems need to remain available and running for healthcare professionals to use. Yet when we consider eHealth in an international development context - its applications towards achieving the third Sustainable Development Goal (SDG) - we may dismiss cybersecurity as being somewhat extraneous, or even a waste of resources. When we talk about building connected healthcare systems in low and lower middle income countries, or ensuring that individuals in rural and underserved communities have access to consultation and treatment, where does cybersecurity fit into the picture? Could every dollar spent on security have been better spent elsewhere?

This thesis attempts to examine where security fits into eHealth systems, particularly developing ones, and how we may be able to work security into policies, legal frameworks, and technologies in support of digital healthcare and the third

SDG. It offers a defense of cybersecurity as a supportive technology that can help to assure the benefits of ICT in healthcare, rather than a luxury reserved for wealthy countries. Often, security is not so significantly at odds with other aims as we might initially believe.

In Chapter 2, we will offer background context by discussing the SDGs and their relationships with ICT in general and with cybersecurity in particular. We will argue that while ICT is widely regarded as an enabling technology for many of the SDGs, there is a new focus on security as a means of assuring the benefits of digitization for development. Additionally, both ICT and security require not only technological capacity but also strong governance: one is incomplete without the other. We will also review academic literature discussing security as related to eHealth, arguing that while there is a limited amount of research discussing healthcare cybersecurity in developing countries, there is evidence to support the importance of trust to technology adoption and the necessity of avoiding a "one-size-fits-all" approach to the problem.

In Chapter 3, we will analyze the results of the 2015 eHealth survey conducted by the World Health Organization (WHO), which asked countries about their progress in each of eight eHealth domains. We will consider the determinants of eHealth development and compare the relationship between eHealth and cybersecurity capacity, concluding that while there may exist a "gap" between eHealth and cybersecurity at low incomes, many higher income countries appear to consider both as critical issues.

Chapters 4, 5, 6, and 7 will consider five of the eight eHealth domains in the WHO survey: foundations, legal frameworks, mHealth and telehealth, and electronic health records. These topics were chosen for their clear importance to healthcare accessibility and their strong relationship to cybersecurity. For each topic, we will complete a short literature review, analyze WHO survey data, examine a case study, and prescribe a number of relevant security controls that can have an outsize impact

on protecting data and systems. Here, we will see that there are a number of ways in which countries can quickly build up their eHealth security in step with their eHealth capacity, particularly by beginning with strong policies, strategies, and legal frameworks which can enable further development in this area.

Finally, in Chapter 8 we will conclude our deep dive with a summary of our findings and recommendations for future work, including additional data collection on the state of eHealth security internationally and the creation of an eHealth-cybersecurity framework.

This thesis aims to offer a jumping off point for future research into eHealth security and capacity by establishing the premise that these two goals can operate in support of one another and be achieved alongside each other, rather than in two distinct stages. By balancing the need to increase access to care with the need to keep systems and data secure, and by finding ways in which security controls can work for accessibility and availability, countries can create strong eHealth systems trusted by the patients who use them.

Chapter 2

Background and Motivations

2.1 Introduction

The relationships between development, eHealth, ICT, and cybersecurity have been widely discussed in the literature. We will explore these topics below, beginning with an explanation of the SDGs and an overview of prior work on the ways ICT can facilitate their achievement. This first section is the foundation on which our case is built: without the need for ICT in development, there would be little need for cybersecurity.

We will then build upon our groundwork by considering cybersecurity as a means of ensuring the development benefits of ICT, keeping in mind the need to balance accessibility and growth with security. We will especially focus on Robert Morgus' model of "security for" and recognition that money spent on securing ICT infrastructure is not zero-sum [2]. After a brief exploration of existing models for measuring national cybersecurity capacity, we will discuss the importance of security towards eHealth and the third SDG: "ensure healthy lives and promote well-being for all at all ages" [3]. We will conclude by identifying gaps in the existing literature – the scarcity of eHealth security research that focuses on the requirements and capacities of developing countries and the lack of nuanced frameworks for eHealth security –

and offering this thesis as a jumping-off point for future research in this area.

2.2 SDGs and ICT

The Sustainable Development Goals (SDGs) were introduced in the United Nations (UN) 2030 Agenda for Sustainable Development, which was adopted by all member states in 2015 [1]. The goals target a wide variety of areas related to economic growth and population well-being – health, education, equality, and more – while recognizing the importance of preserving the environment and addressing climate change [1]. While the SDGs build off prior work towards achieving the now-superseded Millennium Development Goals (MDGs) [1], they are both broader in scope and more ambitious than their predecessors: whereas the first target of the first MDG was to "halve... the proportion of people whose income is less than $1 a day" [4], the first target of the first SDG is to "eradicate extreme poverty for all people everywhere" [1]. The full list of SDGs is available in Figure 2.1.

In order to facilitate the accomplishment of these goals, the SDGs also espouse a more modern perspective than the MDGs. The 2030 Agenda explicitly incorporates information and communications technology (ICT) into its vision for sustainable development, claiming that "[the] spread of information and communications technology and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies" [3]. Goals 4, 5, 9, and 17 also mention ICT in their targets [3].

Recent research has delved even deeper into the potential contributions of ICT towards achieving all SDGs [5, 6, 7]. For example, a 2016 report by Columbia University's Earth Institute and the Swedish telecommunications company Ericsson describes the ways ICT can positively impact development efforts related to financial inclusion, education, health, and energy [8]. The report particularly emphasizes the significance of mobile broadband, which it labels "the essential infrastructure

Figure 2.1: The 17 Sustainable Development Goals (SDGs), adopted by United Nations (UN) member states in 2015 as part of the UN 2030 Agenda for Sustainable Development [1]. The SDGs build upon the work of their previous counterpart, the Millenium Development Goals, in order to establish ambitious development objectives that take into account the growing need for sustainability.

platform for the SDGs" due to its potential for quickly connecting large percentages of the world's population to the Internet [8, p. 8]. This accelerated rate of diffusion can enable deploying and upgrading critical development services and technologies, training students and workers to use them, and spreading awareness of their existence to the wider population – all quickly and at low cost [8, p. 15-16].

It is important to note, however, that the haphazard deployment of ICT solutions by private sector companies will not necessarily result in sufficient development gains: strong institutions and governance - represented by SDG 16 - are necessary for fully realizing the benefits of digitization. Kostoksa and Kocarev argue that "many of the challenges of sustainable development (education, health, infrastructure, and environmental sustainability) call for an intense role on the part of the public sector

and those responsible for policy making" [9].

A deep dive into a specific public-sector use case of ICT is available in the World Health Organization's (WHO) 2016 Global Diffusion of eHealth report, which argues in favor of designing national strategies for eHealth (defined as "the cost-effective and secure use of information and communications technologies in support of health and health-related fields" [10, p. 121]) for the facilitation of public well-being [11]. The report contends that "universal health coverage...cannot be achieved without eHealth" and that eHealth technologies such as electronic health records "[enhance] patient diagnosis and treatment by providing accurate and timely patient information," potentially leading to better health outcomes [11, p. 5, 8]. Throughout, the WHO emphasizes the importance of effective governance, legislation, and policy to realizing the systemic benefits of eHealth, rather than relying on one-off, highly targeted efforts. This sentiment was echoed by a passage in the WHO's 2014 report on the use of eHealth in women's and children's health initiatives:

> The survey results show that while there are many initiatives to support delivery of health services for women and children, knowledge of eHealth use and its effectiveness is incomplete...For example, in Uganda, there were so many eHealth initiatives that in January 2012 the Ministry of Health issued a directive that all eHealth projects/initiatives be stopped until they had secured approval with the Ministry, agreed sustainability mechanisms, and could ensure interoperability with DHIS2. This was because although the Ugandan government recognized the potential advantages of ICT, the development of an enabling environment needed to be guided by a clear eHealth policy and strategic framework [12, p. 31].

It is therefore important to remember that ICT does not exist for its own sake or in a vaccuum, but should be considered in the context of its benefits to population well-being and its relationship to governance and strong institutions.

Table 2.1 breaks down the SDGs into general categories and references a number of potential applications of ICT for each one, as determined by a review of the literature. As shown in the table, ICT can have a wide array of applications to development, from mobile banking to remote learning to smart infrastructure

technologies. As a result of these broad benefits, increases in ICT adoption and integration are correlated with increases in GDP [13].

Category	**Relevant Goals**	**ICT Applications**
Quality of Life	1, 2, 3, 4	- financial inclusion (mobile banking) - mobile consultations for farmers - electronic health records - distance health (mHealth) - remote learning platforms
Infrastructure	6, 7	- smart grids - smart water management
Economic Growth	8, 9	- ICT correlates with GDP growth - reduced costs to ecommerce / int. trade
Equality	5, 10	- expanded access to jobs and education - access to basic services for refugees
Sustainability	11, 12, 13, 14, 15	- smart tech for efficient resource use - climate change + land use monitoring - citizen science biodiversity efforts
Governance	16, 17	- digital identity services - increased government transparency - technology transfer + capacity building

Table 2.1: Potential information and communications technology (ICT) applications to the SDGs, as gathered from a literature review [8, 11, 14, 13, 15]. The applications of ICT to the SDGs are widely understood; however, good governance is necessary in order to fully realize their benefits.

2.3 SDGs and Cybersecurity

With the increased adoption and integration of ICT comes the need for security: the WHO eHealth report also states that "protecting the privacy and security of patients' health data must be a high priority for all countries" [11, p. 99]. This theme is relevant not only to the health sector but to all ICT-supported SDGs: says Robert Morgus in *Securing Digital Dividends*, "without cybersecurity, ICT becomes a potential new point of failure that could threaten to undo development progress" [2, p. 5]. Attacks on improperly secured cyber-physical infrastructure

or online government, banking, or health services can lead to outsize effects on a population [16]. This has been evidenced by a number of incidents in recent years, including the 2007 distributed denial of service (DDoS) attack that took down government, banking, and news websites in Estonia [17]; the 2015 attack on Ukrainian *oblenergos* that cut power to 225,000 people for several hours [18]; and the 2017 WannaCry ransomware attack that impacted 80 hospital trusts across the United Kingdom [19]. Additionally, cybercrime can be a large financial drain on developing economies: the Kenya-based cybersecurity company Serianu estimated in 2017 that cybercrime costs African economies roughly 3.5 billion dollars annually [20, p. 11]. Altogether, these threats can undermine the benefits of increased ICT adoption. The World Bank's 2016 World Development Report corroborates this claim, arguing that "[threats] to cybersecurity, and censorship are undermining confidence and trust in the internet and increasing costs to businesses and governments, resulting in economic losses as well as higher security spending" [21, p. 26-29].

However, whereas ICT as related to SDGs is a popular topic of research, cybersecurity as related to SDGs is less so. Morgus identifies a number of reasons for this, including that cybersecurity spending is often seen as "zero-sum" – while money spent on developing ICT is often perceived as supporting development goals, money spent on securing ICT is often perceived as taking money away from development goals [2, p. 5]. Morgus recommends addressing this gap by steering away from "security from" language and instead shifting towards a model of "security for," focusing on the ways the benefits of cybersecurity can make the promises of digitization a reality [2, p. 45]. Microsoft's Hierarchy of Cybersecurity Needs demonstrates that widespread Internet access is only the first step towards addressing global connectivity needs: resilience (defined as "consistent, dependent, and reliable access to the Internet or Internet-based services") and trust in ICT systems are also key components [22, p. 4, 15]. According to the report, "[t]elemedicine, e-banking, e-government and more can only flourish when the cybersecurity of these connected

transactions can be assured to an acceptable level" [22, p. 22].

While trust in the Internet is still quite high worldwide, there do exist some concerning trends. In a 2019 survey, the Centre for International Governance Innovation found that 81% of those who distrust the Internet cite cyber criminals as a concern [23]. This distrust is causing many individuals to change their behavior online. In some cases, this is beneficial: 40% of respondents who distrusted the internet claimed to be paying more attention to their devices' security, and 19% claimed to be using encryption more often [23]. However, it can also be harmful: 13% of respondents who distrusted the internet (and 18% in the Middle East and Africa) claimed to be using the Internet less often [23]. If distrust in ICT forces people offline, it may prevent these individuals from taking advantage of its benefits. However, work to facilitate cybersecurity can therefore also facilitate trust in ICT, amplifying its development advantages: a 2020 study by Creese et. al. found that a country's cybersecurity capacity correlated with positive end-user experiences: decreased piracy rates; increased ICT adoption by individuals, companies, and governments; and citizen perceptions of better freedom and government accountability [24].

Table 2.2 identifies potential cybersecurity applications for each SDG, as gathered from a review of the literature and using the same broad categories seen in Table 2.1. These applications are shown to be primarily supportive, assuring the confidentiality, availability, and integrity of ICT used to achieve the development goals. This reinforces Morgus' "security for" mentality, which focuses on the benefits of achieving security and trust in technology beyond threat prevention.

2.4 Cybersecurity Capacity

To measure cybersecurity capacity in their study of its benefits to ICT adoption, Creese et. al. used the Cybersecurity Capacity Maturity Model for Nations (CMM), created by Oxford University's Global Cyber Security Capacity Centre (GCSCC) [24,

Category	**Relevant Goals**	**Cybersecurity Applications**
Quality of Life	1, 2, 3, 4	- protection of sensitive financial and medical data from theft - assurance of availability for critical financial and medical ICT systems
Infrastructure	6, 7	- assurance of availability and integrity for critical cyberphysical infrastructure
Economic Growth	8, 9	- reduction of cybercrime threat, which costs economies billions annually - assurance of availability and safety of ICT to realize GDP growth benefits
Equality	5, 10	- assurance of availability and safety of ICT to realize equality benefits
Sustainability	11, 12, 13, 14, 15	- assurance of availability and integrity for smart tech for sustainability - integrity protection for climate change and biodiversity monitoring data
Governance	16, 17	- reduction of cybercrime threat, which undermines institutions and trust - protection of digital identity systems

Table 2.2: Potential cybersecurity applications to the SDGs, as gathered from a literature review [22, 20, 25, 2, 16]. Cybersecurity in support of the SDGs is a less popular topic than ICT in the same context; however, cybersecurity can help to assure the benefits of ICT and encourage trust in technologies and programs designed to aid in the achievement of the goals.

p. 5-7]. The CMM assesses a country's cybersecurity capacity along five dimensions: policy and strategy, culture, knowledge and capabilities, legal and regulatory frameworks, and standards and technologies [26]. In each dimension, a country can fall under one of five maturity levels, from start-up (indicating no concrete development) to dynamic (indicating global leadership and an ability to adapt to emerging threats) [26]. However, a number of other models for measuring cybersecurity capacity have been proposed, such as the International Telecommunication Union's (ITU) Global Cybersecurity Index [27] and the e-Governance Academy's National Cybersecurity Index [28]. A sample of these indexes, their methodologies, and the number of countries they cover are available in Table 2.3.

Index Name	**Organization**	**Countries**	**Method**
Cyber Maturity in the Asia-Pacific Region	Australia Strategic Policy Institute International Cyber Policy Centre	25	multi-stakeholder research based on open-source documents
Cybersecurity Capacity Maturity Model for Nations	Oxford Global Cyber Security Capacity Centre	87	multi-stakeholder reviews based on primary sources and interviews
Cyber Readiness Index	Potomac Institute for Policy Studies	125	expert assessment based on primary sources
National Cybersecurity Index	e-Governance Academy	160	expert analysis of existing legislation and official documents
Global Cybersecurity Index	International Telecommunications Union	195	expert weighting of survey responses

Table 2.3: Sample of national cybersecurity indexes [29, 30, 31, 28, 27]. There are a number of different mechanisms for measuring cybersecurity capacity and commitment on a governance scale; however, these models do not necessarily define which aspects of cybersecurity to prioritize at different stages of development or distinguish between the varied security needs of distinct industries and sectors.

It should be noted that while many of these indexes differ in their finer points, where overall weighted scores exist they tend to strongly correlate with one another. This is shown in Table 2.4, which displays the Pearson's correlation coefficients between the 2020 Global Cybersecurity Index (GCI), 2020 National Cybersecurity Index (NCI), and the 2017 Cyber Maturity in the Asia Pacific Region (CMAPR) scores. The symbols ***, **, and * next to the coefficients indicate significance levels of below 0.001, 0.01, and 0.05, respectively.

Morgus points out, however, that "these models leave a gap in the market for information that has been requested from developing governments: an outline of what cybersecurity capacities to prioritize for development and when" [2, p. 38]. While all of the above models assess countries along multiple dimensions, the dimensions

	GCI	NCI	CMAPR
GCI	1.0***	-	-
NCI	0.804***	1.0***	-
CMAPR	0.835***	0.801***	1.0***

Table 2.4: Pearsons's correlation coefficients of the 2020 Global Cybersecurity Index (GCI), 2020 National Cybersecurity Index (NCI), and 2017 Cyber Maturity in the Asia Pacific Region (CMAPR) scores. While each uses slightly different metrics, the final score results are strongly correlated with one another.

tend to fall less along specific technologies or sectors and more along broad categories such as legislation, standards, and culture. Yet not all countries digitize in a linear fashion: a nation might have high levels of Internet use among its population, but no system for keeping electronic health records (or vice versa). Different sectors have different cybersecurity needs at different stages of development progress.

2.5 Cybersecurity and eHealth

This thesis will therefore explore cybersecurity capacity as it relates to the third SDG: "ensure healthy lives and promote well-being for all at all ages" [3]. Given that the medical field deals with sensitive patient data and relies heavily on the availability of systems, it is relevant to consider the ways in which cybersecurity intersects with efforts to introduce eHealth, mHealth, and telemedicine efforts in support of the third SDG, particularly in developing countries. However, there is still a lack of clarity regarding the best balance between security and accessibility in eHealth, and how the security and privacy concerns of medical professionals and patients affect the adoption of eHealth technologies.

A significant body of work has already explored the topic of cyber threats to the healthcare sector [32, 33, 34, 35]. In a 2018 paper, Coventry and Branley argue that the combination of often-vulnerable (often-legacy) systems and valuable medical data make hospitals tempting targets for cyber criminals [36]. As hospitals are often under severe budget constraints, the costs required to update systems

can often fall by the wayside in favor of a more central mission: improved patient care [37, 38]. In many cases, hospitals struggle to manage their own networks: old accounts are not deleted, unnecessary ports are left open, and proper inventories of technologies in use are not taken [38]. This lack of understanding of their own assets means that attacks may be difficult to identify [38]. Additionally, there is an increased use of Internet of Things (IoT) devices in modern hospitals, which often offer critical health services - patient monitoring, medication administration, etc. - but are challenging to patch and frequently lack basic security features [38].

While many healthcare sector attackers are primarily motivated by the theft of medical records, which can often be sold for large amounts of money, there has also been a rise in ransomware attacks that encrypt hospital data and request a payout in exchange for the key [37]. These attacks can have an enormous financial burden on medical institutions: the UK Department of Health and Social Care estimated in 2018 that the WannaCry ransomware attack cost the National Health Service (NHS) £19 million in lost output during the attack and an additional £72 million in after-the-fact IT support [39].

To keep patient information and critical systems safe, Coventry and Branley recommend both basic security practices (regular patches, thorough backups, staff security culture) and national legislation [36]. There has been significant progress on the latter front: the most recent WHO eHealth survey reveals that in 2015, 78% of responding countries had general privacy legislation regarding personally identifiable information, and 54% had specific legislation regarding the privacy of patient data stored in electronic health records [11]. Yet legislation alone is not sufficient to prevent data theft or disruptive attacks, as evidenced by the recent spike in cyberattacks targeting the healthcare sector - even in countries with robust data privacy laws [40]. A holistic approach leveraging enforcement, training, awareness, and an active "cybersecurity culture" is necessary to achieve the goals set out by national health data privacy laws.

However, existing security research tends to focus on developed nations with well-established eHealth and cybersecurity norms; less attention is paid to countries just beginning to digitize their healthcare sector. In papers focusing on eHealth and mHealth in the developing world, the importance of cybersecurity and data privacy is frequently mentioned – but only briefly, and usually without a great deal of specificity regarding recommended technical or policy measures [41, 42, 43, 44]. A 2010 paper on global eHealth simply states that "[eHealth] policy issues in the developed world relating to data security, data quality, licensure, patient confidentiality, and privacy may be major impediments in the developing world" [45, p. 243].

It is true that existing research around cybersecurity in healthcare may not straightforwardly apply to developing countries, and attempting to do so could result in barriers to access that harm more than help. However, that does not mean that we should avoid defining appropriate cybersecurity standards, policies, or technical necessities altogether. In a 2018 paper, Namara et. al. attempt to strike a balance when discussing eHealth privacy challenges in an African context [46]. The authors argue that while legislation around data privacy is necessary to keep sensitive patient information safe, "it is important to not simply copy other frameworks established from other countries and assume that it would work in Africa" [46, p. 74]. They go on to recommend avoiding a "one-size-fits-all" approach to data privacy and instead ensuring that privacy efforts "reflect the nuanced customs, privacy attitudes, perceptions, and local needs to best serve the people [they are] intended to protect" [46, p. 74].

Security and privacy concerns around the growing use of eHealth technologies do exist in developing countries. In a 2018 paper on barriers to eHealth implementations in Zimbabwe, authors Furusa and Coleman interview a number of doctors who express anxiety about the security of patient data stored electronically and argue that "concerns about the privacy and security of e-health systems remain a barrier to

broader use of e-health by medical doctors in public hospitals and may undermine the possible accomplishment of e-health if not addressed properly" [47]. Additionally, a 2019 survey of individuals in Ghana found that while most were not overly concerned about the collection of their health data by hospitals, many were worried about malicious actors gaining unauthorized access to this data [48]. In order for eHealth efforts to succeed, it is clear that buy-in is needed from both patients and medical professionals. However, existing data and surveys do not make it fully clear whether, or to what extent, security concerns harm the deployment or uptake of eHealth technologies. It is also important to note that security must be balanced with other concerns related to eHealth implementation, such as infrastructure, technical training and support, and budget constraints [47]. A perfectly secure eHealth system that is too expensive to build and too complex to maintain provides no benefit to a patient.

Yet attempts to develop a nuanced global framework around cybersecurity for healthcare have been explored only sparingly in the literature. A 2019 paper surveying national cybersecurity indexes states that "cybersecurity standards specifically designed for the healthcare sector are nonexistent, and none are routinely or consistently applied" [49]. This has only recently changed: in 2020, O'Brien et. al. published Essentials of Cybersecurity in Healthcare Organization (ECHO), a framework established by expert consensus and containing six dimensions applicable to healthcare cybersecurity: (cultural, financial, and institutional) context; governance; organizational strategy; risk management; awareness, education, and training; and technical capabilities [50]. The authors contend that developing nations may be able to "leapfrog" the issues affecting developed countries by building security into their eHealth and mHealth systems by default [50, p. 9]. However, while the framework offers important cybersecurity considerations for healthcare systems, it does not attempt to define a scale – there is no mechanism for assessing a country's eHealth-cybersecurity capacity at a given time.

2.6 Conclusion

Above, we have made a case for the importance of cybersecurity to the SDGs generally and to the third SDG ("ensure healthy lives and promote well-being for all at all ages" [1]) in particular. We have also identified a number of gaps in the literature: while there is an extensive exploration into the importance of cybersecurity to the health sector, this is not usually applied to the developing world and to newly-digitizing healthcare systems. Additionally, existing models of cybersecurity capacity do not offer a clear picture of priority for eHealth development: how does a country with limited resources balance the population health benefits of ICT integration with the need to ensure data privacy, cybersecurity, and trust? The following sections of this thesis will attempt to explore this question in the hope of offering a starting point for future research on the topic of cybersecurity and the SDGs, as well as make a case for cybersecurity as an enabling rather than prohibitive force for ICT in development.

Chapter 3

Data Analysis

3.1 Data Sources

Data included in this analysis came from a variety of sources, which are discussed below.

The primary source for data on the status of a country's eHealth was the World Health Organization's (WHO) Atlas of eHealth Country Profiles [51]. This document represents a compilation of the results of the WHO's third global survey on eHealth, which was conducted between April and August 2015. The survey asked a variety of categorical (primarily yes/no) questions about healthcare digitization efforts in the following eight areas:

- *eHealth Foundations* - "fundamental building blocks" of eHealth such as national policies and capacity building efforts
- *Legal Frameworks* - existence of legislation around eHealth, particularly with regards to patient privacy and data rights
- *Telehealth* - existence of various telehealth programs at various maturity levels, such as telepsychiatry and remote patient monitoring
- *Electronic Health Records (EHRs)* - existence and use of a national EHR system and supporting technologies

- *eLearning* - education for health workers, both during initial schooling and as on-the-job training
- *mHealth* - existence of various mHealth programs at various maturity leveles, such as call centres, appointment reminders, and disease surveillance
- *Social Media* - use of social media by healthcare organizations, communities, and individuals for disseminating and receiving health-related messages
- *Big Data* - existence of policies and strategies around the use of big data in health care

Note that the survey did not include responses from all WHO member countries: the response rate was 125 out of 195, or about 64%. It is therefore relevant to consider whether the responding countries form an appropriately representative sample of WHO member countries. Figure 3.1 displays bar charts displaying the counts of both survey respondents and WHO member countries as a whole by region (as according to the WHO) and income level (as according to the World Bank) [52, 53].

Note that there does appear to exist a slight bias in response rates: in particular, the WHO includes more Western Pacific member countries than Eastern Mediterranean member countries, but more Eastern Mediterranean countries than Western Pacific countries completed the survey. Additionally, there is a mild skew in response rates towards European and Eastern Mediterranean countries as opposed to countries in Africa or the Americas. This may mean that some valuable data about the state of eHealth in certain country groups is missing. However, most of the responding countries do appear to be grouped roughly in proportion with expectations, indicating that the survey results still have value as a representative sample.

The second major dataset used, in this case to represent a country's cybersecurity capacity, was the International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) [54]. This particular index was chosen for its clear numeric scoring system, wide country coverage, and consistent output across several

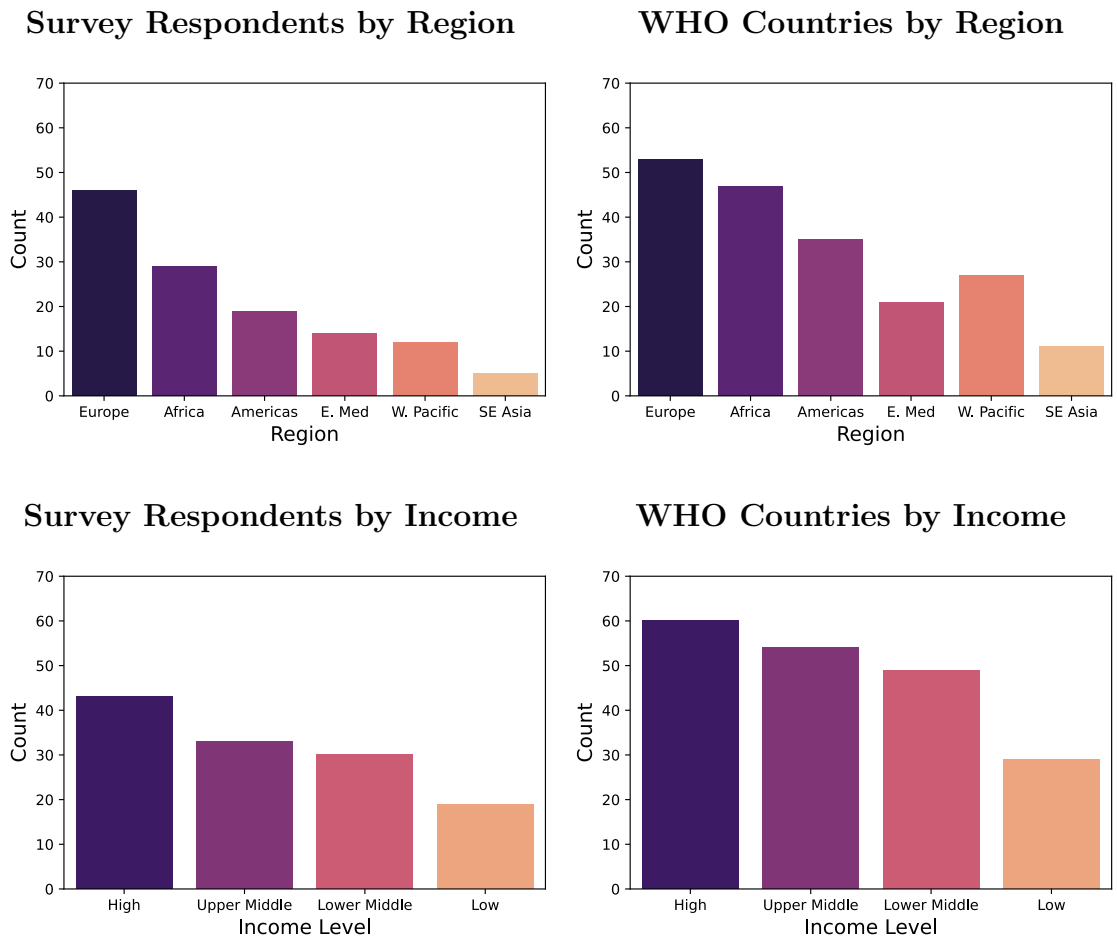

Figure 3.1: Count comparisons, by income level and region, of the WHO members who responded to the 2015 WHO eHealth survey and all WHO members [11]. While there are a few discrepancies in proportion between survey respondents and members, the survey still has value as a representative sample.

years; however, note that, as discussed in Section 2.4, its scores strongly correlate with other cybersecurity indexes. Note also that while more recent indexes exist, the 2015 index scores were used in order to ensure that the data was contemporary with the WHO eHealth survey results. While the 2020 index includes higher scores across the board and a slightly different scoring method (out of 100 rather than out of 1.0), in many cases the relative placements of countries remained quite similar. This is shown by the results in Table 3.1, which includes the Pearson's correlation coefficients between the 2015 and 2020 GCI ranks and scores. The symbols ***, **, and * next to the coefficients indicate significance levels of below 0.001, 0.01, and

0.05, respectively

	Rank 2015	**Rank 2020**	**Score 2015**	**Score 2020**
Rank 2015	1.0***	-	-	-
Rank 2020	0.809***	1.0***	-	-
Score 2015	-0.999***	-0.809***	1.0***	-
Score 2020	-0.800***	-0.986***	0.800***	1.0***

Table 3.1: Pearsons's correlation coefficients of the GCI ranks and scores between 2015 and 2020. Note that the negative correlations exist because higher scores mean lower ranks (e.g., the country with the rank of one will have the highest score). While most countries have higher GCI scores in 2020 than in 2015, the relative ranks and scores of countries over the five-year difference are still strongly correlated with one another.

The GCI is discussed in Section 2.4; in sum, it is an index of a country's commitment to cybersecurity efforts along five dimensions based on a combination of survey results (where available) and expert research. The 2015 GCI covered 195 countries, 104 of which responded to the survey. The five dimensions of the index are as follows:

- *Legal Measures* - legislation and institutions targeting cybercrime, data protection, and cybersecurity standards
- *Technical Measures* - defense mechanisms against cyber threats, including a national response team and standards and certifications for cybersecurity
- *Organizational Measures* - policies, agencies, and benchmarks indicating strategic cybersecurity effort and governance
- *Capacity Building* - cybersecurity standards and certifications, as well as efforts to promote cybersecurity education
- *Cooperation* - information and capacity sharing between agencies and nations, as well as public-private partnerships

Figure 3.2 displays a histogram of the 2015 GCI scores of represented countries, exhibiting a score range from 0.0 to 0.824 (out of a high score of 1.0). The histogram shows that, in 2015, the majority of countries had extremely low scores. Nine

countries received a score of 0.0, indicating little-to-no progress on any of the five dimensions.

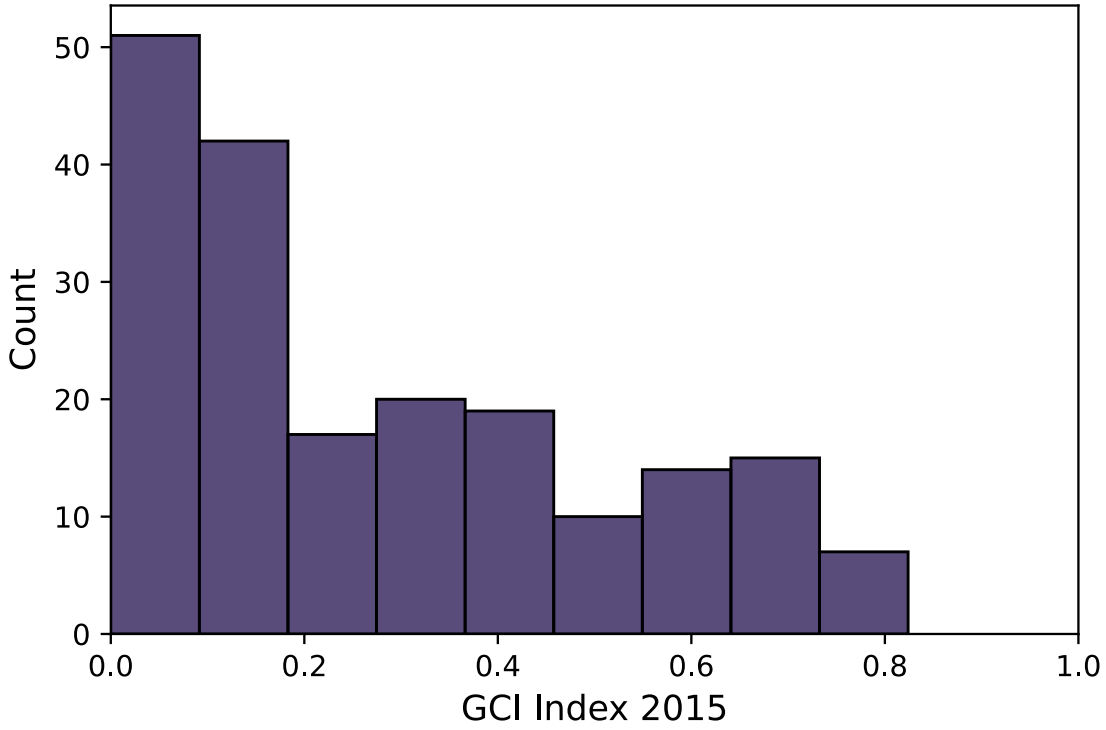

Figure 3.2: Histogram of 2015 Global Cybersecurity Index (GCI) scores [54]. The majority of countries in 2015 had quite low scores, with a number receiving a score of 0.0 to indicate little-to-no progress in any of the GCI's five dimensions.

Figure 3.3 displays six histograms with more detail on the counts for each sub-index score, with the overall score histogram displayed for reference. These histograms indicate the most progress on the legal index, which has the largest number of high scores across all categories. Most other indexes, particularly cooperation and capacity building, suffer from a dearth of high scores. This is sensible: creating laws against cybercrime may require fewer resources than other governance initiatives, such as establishing robust information sharing partnerships or maintaining a national cyber defense team.

Our final datasets are the GDP per capita in current US dollars and the percentage of Internet users in a given country, according to the World Bank (WB) [55]. We will call these "wealth" and "connectivity" in line with Creese et. al. [24]. Again,

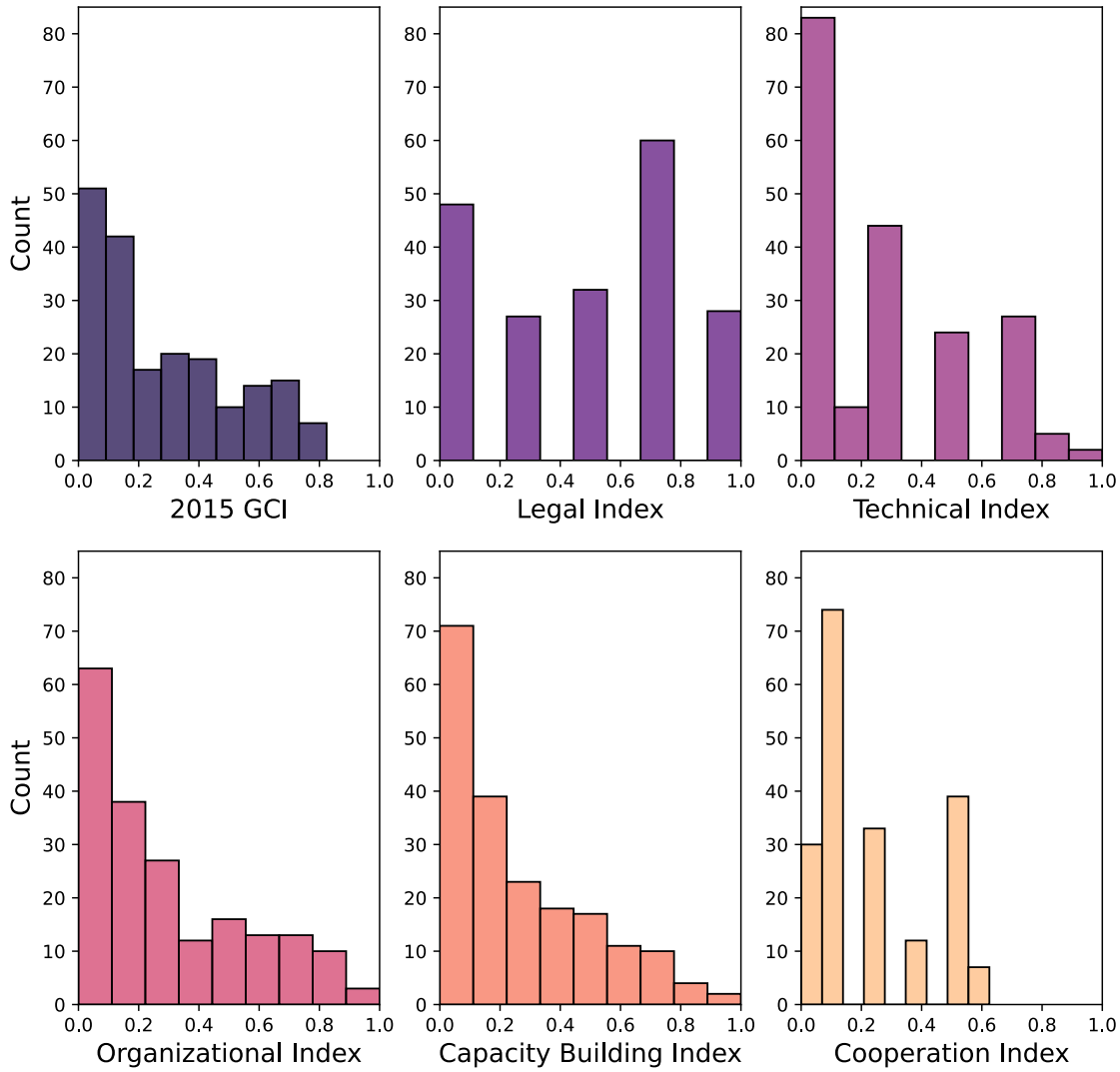

Figure 3.3: Histograms of the 2015 GCI and its five subindexes [54]. While in all categories low scores were still highly represented, the highest proportions of high scores appears in the legal index.

data is taken from 2015 in order to remain contemporary with the survey results. All of the datasets are described in Table 3.2.

3.2 Methods and Results

We begin our data analysis by examining the responses to the WHO's eHealth survey. The heatmap in Figure 3.4 displays the relative strength of the Pearson's correlation coefficients between the binary (yes/no) answers of the survey: essen-

Name	N	Mean	Std Dev	Min	Max	Source	Desc
eHealth	125	0.448	0.210	0.000	0.928	WHO	Proportion yes answers to the 2015 WHO eHealth survey
GCI	195	0.284	0.228	0.000	0.824	ITU	2015 score measuring cybersecurity engagement
Wealth	208	3.807	0.636	2.468	5.224	WB	Natural log of the 2015 GDP per capita, in current USD
Connectivity	203	48.365	28.524	1.084	98.324	WB	2015 Percent Internet users

Table 3.2: A summary of the data sources used in this analysis [11, 54, 55]. In order to remain contemporary with the latest WHO eHealth survey, data from 2015 was used.

tially, how likely a country was to mark two different questions as both "yes" or both "no". Note that where no answer was provided, either due to an inapplicable question or a lack of response, a "no" was filled into the dataset. This was done because of the inconsistency of responses to inapplicable questions in the survey; in some cases a proper "N/A" marking was used, while in others the questions were simply left blank; a blanket policy was used in order to reduce inaccuracies and potentially inaccurate case-by-case judgements. The eight rectangular frames in the figure surround questions in the eight questions categories mentioned in Section 3.1. These are, in left-to-right / up-to-down order, eHealth foundations, legal frameworks, telehealth, EHRs, elearning, mHealth, social media, and big data.

This figure shows the expected result that correlations between answers in the same category are (generally) relatively strong. For example, the Pearson's correlation coefficient between elearning programs for pre-medicine students and elearning programs for pre-public health students is 0.8324, with a p-value statistically signif-

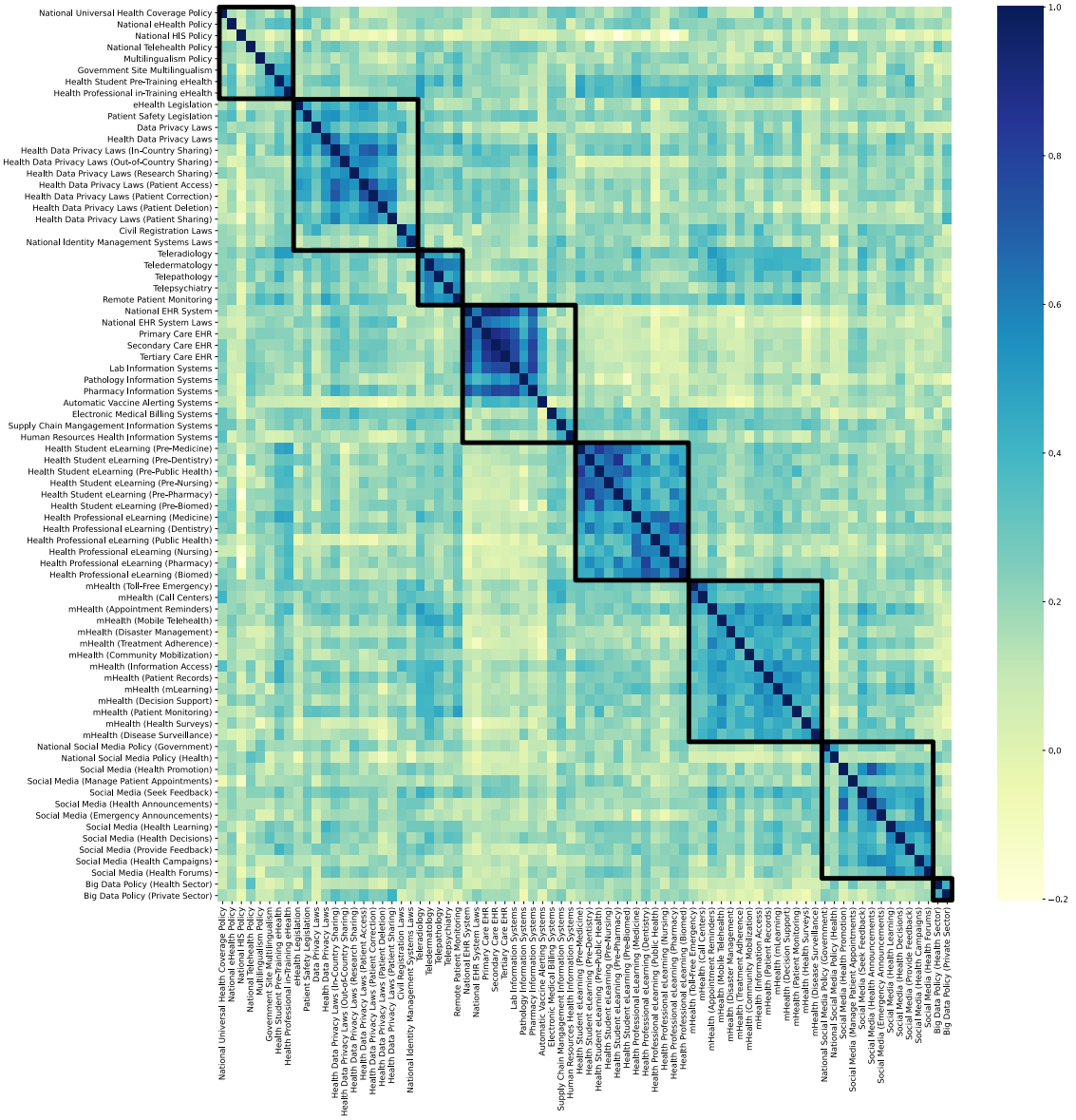

Figure 3.4: Heatmap of the Pearson's correlation coefficients of the binary yes/no responses to the 2015 WHO eHealth survey [11]. The black boxes represent (in left-to-right / up-to-down order) the eight distinct categories of the survey: eHealth foundations, legal frameworks, telehealth, EHRs, elearning, mHealth, social media, and big data. The heatmap shows that generally, the strongest correlations were found within categories.

icant at the 0.001 level. This points to the sensible conclusion that countries which implement elearning programs for one field in the health sector are highly likely to apply them to other fields in the health sector. Broadening the example, countries which invest resources in technologies, programs, or legislation related to eHealth will likely attempt to use these for a wide variety of applications.

However, the figure also shows that correlations between questions from different question categories are more moderate, and sometimes quite weak. For example, the Pearson's correlation coefficient between national EHR systems and teleradiology programs is only 0.0846, and this value is not statistically significant. This indicates that healthcare digitization is not a monolithic or binary process: countries do not necessarily pursue all aspects of eHealth at the same time. Different technologies or governance efforts will have different barriers to implementation, and once each is overcome more progress within the same category can be made.

To get a rough idea of how the question categories relate to each other, we calculated normalized scores for each by adding up the number of "yes" answers and dividing by the total number of questions in the category. The questions considered for each category are the ones present on the x and y axes of Figure 3.4 - in other words, we have simply condensed each rectangular frame into one cell. We then calculated the Pearson's correlation coefficient between each of these normalized scores. The resulting heatmap is displayed in Figure 3.5. The Pearson's correlation coefficient is visible in each cell, along with the symbols ***, **, and * to indicate significance levels of below 0.001, 0.01, and 0.05, respectively.

This heatmap shows that category scores are generally weakly-to-moderately positively correlated with one another. This indicates that while separate barriers to entry do exist for each category (as supported by Figure 3.4), countries that invest in one area of eHealth are relatively likely to invest in others. The strongest correlation in the heatmap is between mHealth and telehealth (r-value 0.5987, p-value <0.001), which is expected given that both categories make use of remote communication technologies - investment in mHealth programs may carry over to telehealth applications, and vice versa. In contrast, making progress in both mHealth and EHRs (r-value 0.2898, p-value <0.01) requires a significant amount of distinct resources and time. Interestingly, eHealth foundations have moderate-to-strong correlations with every category other than Big Data (which only included two yes/no questions,

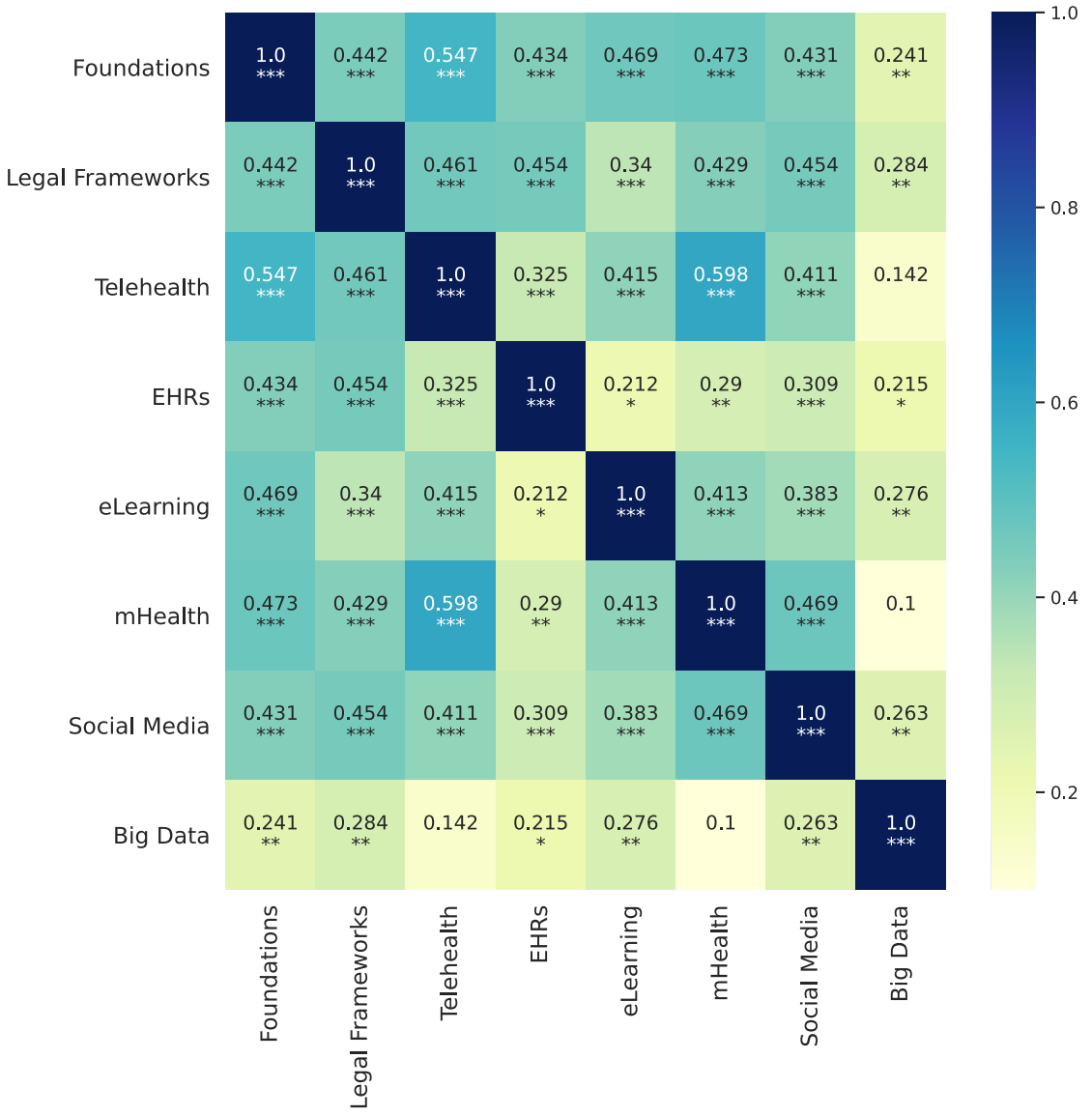

Figure 3.5: Heatmap of the Pearson's correlation coefficients of the percentage of "yes" answers in each category of the 2015 WHO eHealth survey [11]. The heatmap shows that correlations between categories were typically low-to-moderate, with the strongest correlations between mHealth and telehealth.

and thus likely has skewed results). This indicates that strong foundational efforts, such as national policies and strategies, are associated with progress in eHealth across the board. We will explore this concept further in Chapter 4.

In order to discover how the survey results map onto the regions and income levels discussed in Section 3.1, we have created bar charts (visible in Figure 3.6) breaking down the percentage of "yes" responses to key questions and groups of

questions by these categories. The questions / questions groups in the charts are, from left to right:

- Existence of a national eHealth policy or strategy, a health information system (HIS) policy or strategy, and/or a telehealth policy or strategy
- Existence of a data privacy law applicable to patient data held in electronic format (e.g., EHRs)
- Existence of at least one of five telehealth programs
- Existence of a national EHR system
- Existence of at least one of fourteen mHealth programs

These questions were chosen as representative "summary" questions for five of the eight broad survey categories: foundations, legislative frameworks, telehealth, EHRs, and mHealth.

This chart is broadly positive about the state of eHealth internationally: for all region and income level categories, over half of countries had some sort of national policy or strategy related to digital health and had at least one telehealth and mHealth program in place.

The largest area of discrepancy between regions and income levels appear to be the existence of data privacy laws related to patient data stored electronically. The majority of high income and upper middle income countries, as well as the majority of countries in Europe, the Americas, and the Western Pacific responded affirmatively to having a law that would fit this category. However, significantly fewer than half of lower income, low income, African, Eastern Mediterranean, and South-East Asian countries responded in the same way - even those these countries were likely to have at least some eHealth policies and programs in place. In fact, lower middle income and Eastern Mediterranean countries were more likely to have a national EHR system than to have privacy legislation applicable to it. This indicates that there may exist a governance gap for privacy legislation and considerations of how privacy and security fit into the newly forming health digitization space.

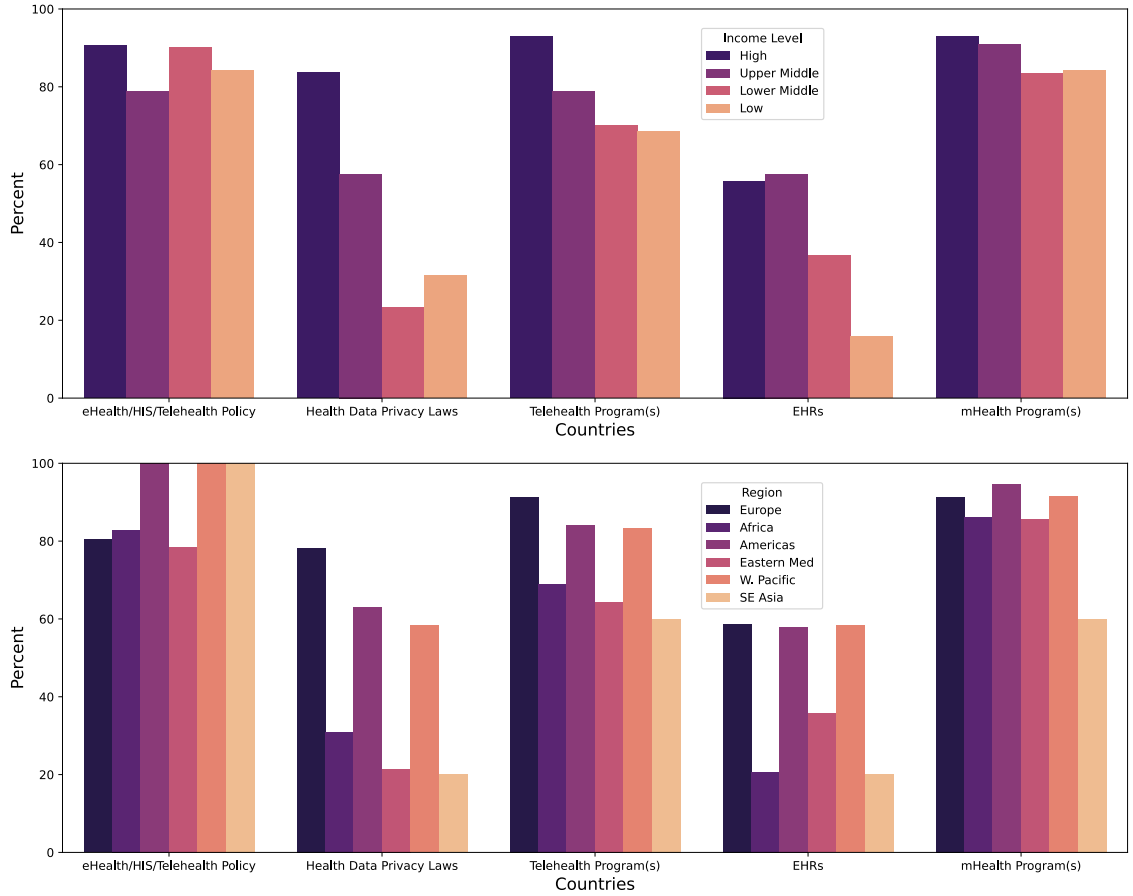

Figure 3.6: Based on the 2015 WHO eHealth survey, a breakdown of the following questions by region and income level: the percentage of countries with an eHealth, health information system, or telehealth policy; the percentage of countries with a data privacy law applicable to electronically held patient data; the percentage of countries with at least one telehealth program; the percentage of countries with a national electronic health record (EHR) system; and the percentage of countries with at least one mHealth program. This indicates that while significant progress has been made on many aspects of eHealth, there may exist a legislative and privacy / security gap in low and lower middle income countries.

Given that health data privacy is a concern in low income and developing countries, as discussed in Section 2.5, it is relevant to consider ways in which this gap may be addressed without harming the progress of newly developed eHealth programs. Note, however, that the survey results are from 2015, and since then health data privacy laws may have been passed in many of these countries - a fact examined in Chapter 5.

Finally, for most groups of countries, national EHR systems received the fewest

"yes" responses - likely because these systems are deeply complex to create and maintain, even for countries with well-established healthcare systems and eHealth programs. However, it may be possible to "leapfrog" over these challenges by building a national EHR system into a developing healthcare system.

From here, it is relevant to consider how cybersecurity capacity fits into our model. As a country grows, becomes more wealthy, and expands its eHealth capabilities, does its cybersecurity appear to grow as well? Or does a gap exist between eHealth capacity and cybersecurity capacity?

To begin, we will compare the growth of eHealth capacity with GDP per capita. To measure eHealth capacity, we calculate the number of "yes" answers in the survey divided by the total number of questions - the same method used to calculate the sub-scores in Figure 3.5. The resulting scatterplot is depicted in Figure 3.7, with regions represented by the colors of the datapoints.

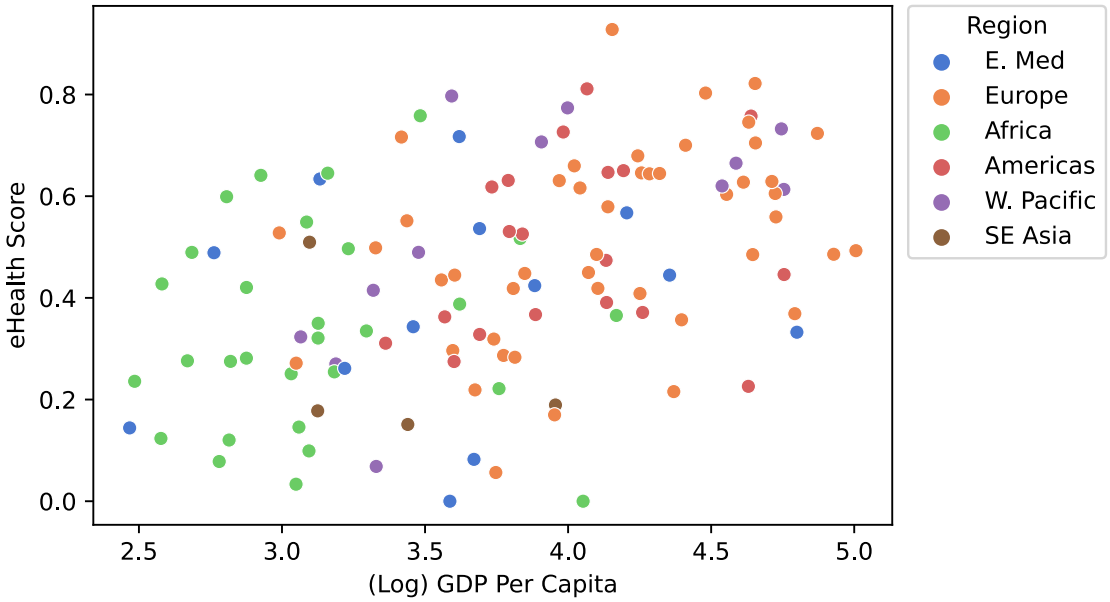

Figure 3.7: Scatterplot of the percentage of "yes" answers to the 2015 WHO eHealth survey versus the natural log of GDP per capita, broken down by region. This chart indicates that while a higher level of GDP does increase the likelihood of additional investment into eHealth, significant progress can be made even at lower incomes.

The figure demonstrates that the percentage of "yes" answers in the survey does increase slightly with GDP per capita: at a general level, more money to spare seems

to mean more investment in eHealth. European and Western Pacific countries are more likely to appear at the top right corner of the graph, enjoying both a high GDP and a large number of eHealth policies and programs. The bottom left corner of the graph, with a low GDP and a small amount of investment in eHealth, appears to comprise primarily countries in the African and Eastern Mediterranean regions. However, the data does not have a completely linear relationship: there are countries from all regions with a moderate-to-high eHealth score and a low GDP per capita, and vice versa.

More details on the relationship between eHealth and GDP per capita are available in Table 3.3. Ordinal Least Square (OLS) linear regressions were run with each of the eHealth scores (generated as per Figure 3.6) as dependent variables and the natural log of the GDP per capita as an independent variable. OLS regressions allow for the prediction of a dependent variable from one or more independent variables, each of which receives a coefficient indicating its impact on the dependent variable. The symbols ***, **, and * next to the coefficients indicate significance levels of below 0.001, 0.01, and 0.05, respectively.

Score Category	**N**	R^2	**Coefficient**
Overall	123	0.195	0.1449***
Foundations	123	0.110	0.1308***
Legal Frameworks	123	0.413	0.3033***
Telehealth	123	0.122	0.2047***
EHRs	123	0.096	0.1533***
eLearning	123	0.072	0.1543**
mHealth	123	0.020	0.0719
Social Media	123	0.038	0.0859*
Big Data	123	0.017	0.0552

Table 3.3: Ordinal Least Square (OLS) regressions, with the percentage of "yes" answers in each category of the 2015 WHO eHealth survey as the dependent variables and the natural log of GDP per capita as the independent variable. These results indicate that GDP per capita has varied levels of explanatory power for different categories of eHealth, implying that income levels may have an effect on which programs or policies are easy to implement.

All of the R^2 values are quite low, indicating that GDP per capita on its own is

not a particularly good explainer of the eHealth survey results. This suggests that a variety of complex factors are at play here, rather than simply "more money = more eHealth." The largest R^2 and coefficient values represent the legal frameworks score: a 1 unit increase in our measurement of a country's wealth (the natural log of their GDP per capita) results in a .3 unit increase in a country's eHealth legal frameworks score (the percentage of "yes" answers in that survey category). This could be due to the complexity of the questions asked in this category: in order to achieve a high number of "yes" answers, a country needs to have sophisticated health data privacy laws that govern the sharing of patient data within and outside of the country and allow patients to view, modify, and even delete that data. This may be a challenging ask for countries that are still moving to electronic formats to store patient data. mHealth, on the other hand, received a low R^2 value and a coefficient that is not statistically significant. This may be because mHealth programs often work well in countries with limited resources as a way to easily offer medical services to a growing number of individuals with mobile broadband subscriptions - an idea we discuss in Chapter 6.

GCI, on the other hand, appears to correlate a little more "neatly" with GDP per capita: there are fewer outliers in the top left corner of the scatterplot in Figure 3.8 - it appears that it is difficult to have a high GCI score without a moderate-to-high GDP per capita. There are, however, a fair number of countries with a relatively high GDP per capita and a low GCI score. The majority of these are small nations, such as Lichtenstien, Monaco, Palau, and Seychelles. However, there exist countries in all regions with a moderate GDP per capita and low GCI scores. This may indicate a lag between increasing wealth and investment in cybersecurity capacity. For the most part, the region breakdown in the chart is similar to Figure 3.7, with primarily European and Western Pacific countries in the top right corner and primarily African and Eastern Mediterranean countries in the bottom left corner.

Once again, we delve into futher detail with Table 3.4, which includes the re-

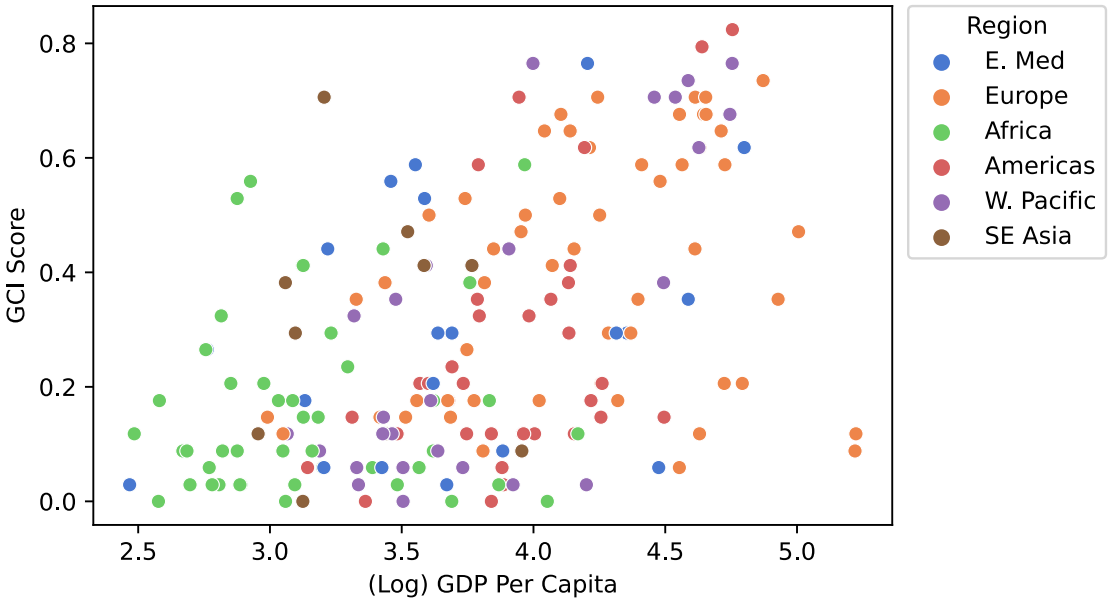

Figure 3.8: Scatterplot of the 2015 GCI scores versus the natural log of GDP per capita, broken down by region. This chart indicates that high GCI scores are much more likely at high levels of GDP and very rare at low levels of GDP.

sults of additional OLS Regressions with the natural log of GDP per capita as the independent variable and the GCI and its sub-indexes as dependent variables. The symbols ***, **, and * next to the coefficients indicate significance levels of below 0.001, 0.01, and 0.05, respectively.

Score Category	**N**	R^2	**Coefficient**
Overall	191	0.243	0.1819***
Legal Measures	191	0.227	0.2728***
Technical Measures	191	0.153	0.1737***
Organizational Measures	191	0.119	0.1619***
Capacity Building	191	0.191	0.1845***
Cooperation	191	0.168	0.1225***

Table 3.4: Ordinal Least Square (OLS) regression, with the 2015 GCI and subindex scores as the dependent variables and the natural log of GDP per capita as the independent variable. These results indicate that GDP per capita has some explanatory power for each of GCI category, with statistically significant results in all regressions.

While again GDP per capita does not tell nearly the full story of a country's GCI, it does typically have more explanatory power than it did for eHealth, and coefficients are always statistically significant at the 0.001 level. Other than the

overall score, the highest R^2 and coefficient values were for the legal measures sub-index - an interesting result given that, for eHealth, legal frameworks also had the strongest relationship to GDP per capita.

Finally, we plot GCI against eHealth in Figure 3.9. One interesting feature of this graph is the increase in variance of region in the top right and bottom left corners. Additionally, the bottom right corner is entirely empty, indicating that a country with a high GCI score is essentially guaranteed to also have a significant number of eHealth policies and programs in place. However, there are also a large number of countries in or near the top left corner, indicating that they have made significant progress in eHealth but do not have a comparable cybersecurity capacity. This indicates that many countries may be putting eHealth "first": as they grow their wealth, they are developing their healthcare sectors with priority over increasing their cybersecurity capacity. As discussed in Section 2.5, this is not necessarily a bad thing: a perfectly secure health system that is too expensive to build and too difficult to maintain does not serve a population as well as one that can be deployed quickly and cheaply to treat as many people as possible. However, countries that lag behind for too long may find that the gaps in their cybersecurity could lead to real dangers: data theft, ransomware, and other attacks on well-connected but poorly-protected hospital systems. Additionally, it may in some cases be more challenging and expensive to add cybersecurity into a healthcare system "after the fact" rather than building in a security mindset throughout, incorporating security considerations into national eHealth strategies, digital healthcare legal frameworks, interoperability considerations, and technical guidance.

Over the next few chapters, we will discuss in more detail the relationship between cybersecurity and five of the eight categories of the WHO eHealth survey: eHealth foundations, legal frameworks, mHealth and telehealth, and electronic health records. These topics were chosen for their clear cybersecurity applications and for their representation of both the governance and technical aspects of eHealth.

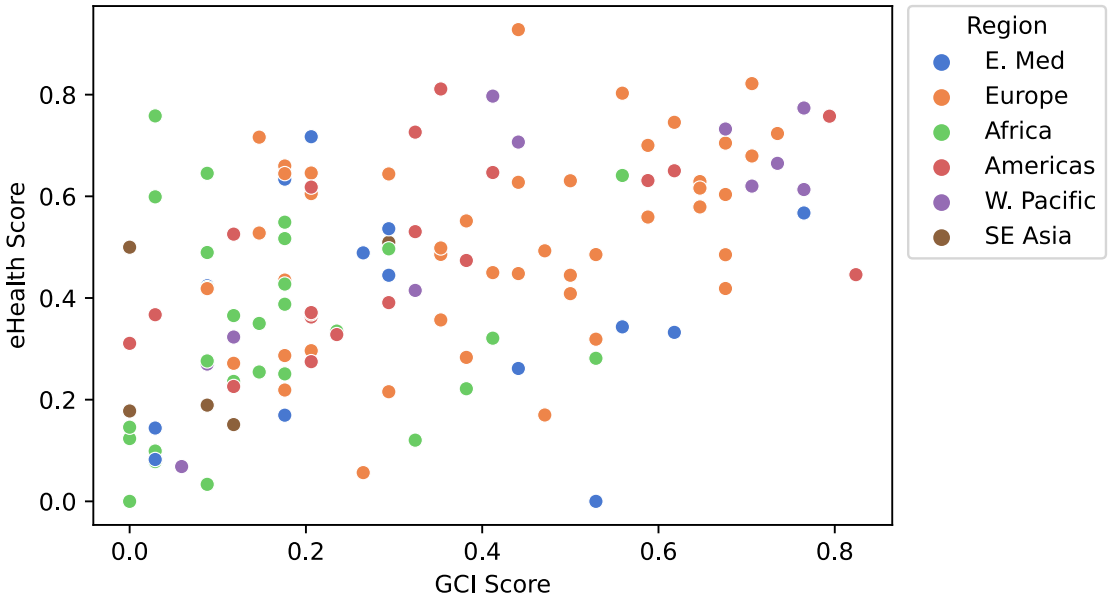

Figure 3.9: Scatterplot of the percentage of "yes" answers to the 2015 WHO eHealth survey versus the 2015 GCI, broken down by region. This chart indicates that few countries achieve high GCI scores without achieving high eHealth scores, while many countries achieve high eHealth scores without achieving high GCI scores.

Each chapter will review relevant literature, consider the data at hand, examine relevant case studies, and recommend cybersecurity controls. Our goal is to examine ways in which cybersecurity can be built into developing eHealth systems, avoiding a "security gap" without hindering the benefits offered by ICT.

Chapter 4

eHealth Foundations

4.1 Introduction

This chapter will discuss eHealth Foundations through the lens of national eHealth policies and strategies. National eHealth strategies represent an excellent jumping off point for a country to consider their cybersecurity posture in the context of their eHealth goals and set intentions for future progress. We will begin with a brief review of relevant literature and an analysis of data on national eHealth and national cybersecurity strategies, supporting our conclusion from Section 3.2 that there may exist a security gap with regards to eHealth. We will then examine in detail the eHealth strategies of four African countries in order to generate a series of relevant security controls and considerations for these foundational measures.

4.2 Literature

National policies and strategies are key to eHealth efforts for the reasons discussed in Section 2.2: it is crucial for states to have a clear plan and direction in order to reap the rewards of ICT. The goal of a national eHealth strategy, according to the WHO, is to "set out, in the context of the health priorities of the country, a vision, a plan of action for delivering the vision and arrangements for monitoring and

evaluation" [11, p. 12]. The strategy should consider all relevant stakeholders, the current eHealth context, and financial and technical requirements for improvement.

In a 2020 review of five African national eHealth strategies, Maina and Singh argue that "inoperable and disjointed systems are a longstanding concern for many eHealth systems" due to the difficulty of maintaining communication and ensuring interoperability - qualities that an overarching national strategy can help to assure [56, p. 673]. However, the authors conclude their review with the concern that "it is not clear whether existing strategies address sufficiently the emerging concerns on privacy, security, and data governance associated with new technologies" [56, p. 675]. This is worth attention, as the relevance of including security considerations in national eHealth strategies is widely recognized. In a 2020 Delphi survey of sixteen health informatics experts reviewing forty potential considerations for eHealth policies, "Technology for Information Security" was one of six to receive a 100% consensus on its importance [57]. Unfortunatly, this consideration also received a high level of consensus on its difficulty: 88% of respondents agreed that information security was a challenging item to implement.

Additionally, the National eHealth Strategy Toolkit, published in 2012 by the WHO and the ITU, includes the creation of "policies for privacy and security of information" as a key focus for national eHealth strategies [58, p. 6]. However, the WHO and the ITU appear to recognize security as a relatively late-stage goal. The Toolkit includes a three-stage eHealth context model (experimentation and early adoption, developing and building up, and scaling up and mainstreaming) which only mentions security at the final stage: the earlier stages are focused on investing in eHealth programs, creating legal frameworks, and ensuring interoperability. This may be because of the same problem of security's perceived difficulty and cost. However, there are a variety of security concerns that are relevant at early stages of eHealth development, particularly with regards to the availability of systems. Additionally, attempting to add security into an eHealth system "after the fact"

may prove both challenging and resource-intensive.

Despite the difficulty, security is not being ignored: many countries do consider security and privacy in their national eHealth policies and strategies. For example, Uganda's 2017-2021 National eHealth Policy includes a number of aims related to information security, most notably to implement the country's National Information Security Framework and Data Protection and Privacy Bill in the health sector [59]. Cameroon's 2020-2024 Digital Health Strategic Plan also sets a number of security-related goals, including completing audits, acquiring certifications, and recruiting talent [60]. Nigeria's 2015-2020 National Health ICT Strategic Framework discusses the intention to set up a National Health ICT Architecture in order to maintain high standards for security and reliability [61]. However, even policies that recognize the need for security in digital health systems are not always specific about what controls are needed or what the "next steps" are: for example, Zambia's 2017-2021 Health Strategy mentions the need to "enhance digital privacy mechanisms to protect data from corruption and enhance monitoring" but does not go into detail about the plans to achieve this or the agencies responsible for doing so [62, p. 13]. This points to the difficulty of creating an effective national eHealth policy that outlines a coherent national direction but also contains definitive, measurable goals. We will explore these countries further in our case study in Section 4.4.

4.3 Data

We begin our data analysis by returning to the 2015 WHO eHealth survey. According to the survey, most nations seem to have made progress in creating national digital health policies and strategies: of the respondents, 58% had a national eHealth policy or strategy, 66% had a national health information system (HIS) policy or strategy, 22% had a telehealth policy or strategy, 86% had at least one of the three, and 14% had all three [51].

While the survey does not include a question about the inclusion of security requirements in these national digital health strategies, we can look at data on the existence of national cybersecurity strategies. Just as national eHealth strategies help to determine the direction of a nation with regards to digital health technologies, national cybersecurity strategies are important to determining the direction of a nation with regards to its security. Having a national cybersecurity strategy indicates that a country has recognized the importance of security to its well-being and may be able to apply the strategy's components to the health context. Here we have analyzed the ITU's Cyberwellness Profiles, part of the 2015 Global Cybersecurity Index (GCI). While the Profiles do not have simple yes/no answers to relevant questions, the responses were analyzed to determine whether a policy was already in place, whether a draft policy or a plan for a future policy was in progress, or whether no policy or plan was existed at all. According to this reading, in 2015 roughly 38% of examined countries had some sort of national cybersecurity policy or strategy, and an additional 16% had a plan to implement one or a draft policy in progress [54].

Of countries covered by both the WHO eHealth survey and the GCI, roughly 6% have neither a national cybersecurity strategy nor any of the three digital health strategies listed above, 7% have a completed or draft national cybersecurity strategy but no eHealth strategies, 31% have no national cybersecurity strategy but at least one eHealth strategy, and 55% have a completed or draft national cybersecurity strategy and at least one eHealth strategy. This supports the assertions in Chapter 3 that countries are likely to prioritize eHealth over cybersecurity, but that both typically become relevant concerns over time.

The barplot in Figure 4.1 displays the percentage of countries with a national or draft cybersecurity strategy and the percentage of countries with at least one of the three digital health strategies, based on the ITU Cyberwellness Profiles and the WHO eHealth survey, broken down by the region and income level categories used

in Section 3.2.

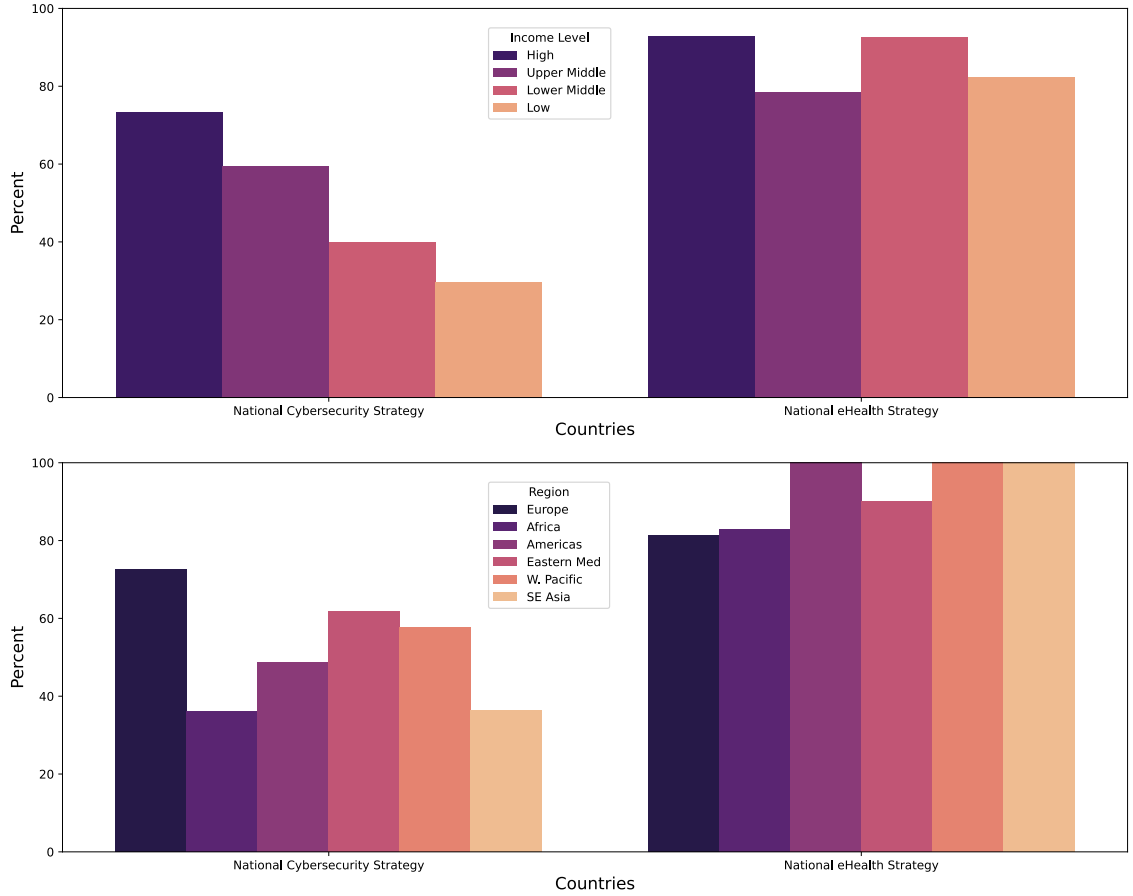

Figure 4.1: Percentage of countries with a national eHealth, health information system, or teleheath policy or strategy and a national cybersecurity strategy, broken down by region and income level. In 2015, national digital health strategies were significantly more common than national cybersecurity strategies across all regions and income levels.

The figure shows that at all regions and income levels, national cybersecurity strategies lag behind national eHealth strategies. European and high income countries have the smallest gap, indicating that for these countries both cybersecurity and eHealth are high priorities at a governance level. South East Asian and low income countries have the largest gap, indicating that for these countries eHealth is a higher (or easier to address) priority than cybersecurity.

Finally, Table 4.1 displays the Pearson's correlation coefficients between the existence of the national policies discussed above and our measurements of wealth (the natural log of GDP per capita) and connectivity (the percentage of Internet users).

The symbols ***, **, and * next to the coefficients indicate significance levels of below 0.001, 0.01, and 0.05, respectively.

	eHealth	**HIS**	**Tele**	**Cyber**	**Wealth**	**Connect**
eHealth	1.0***	-	-	-	-	-
HIS	0.038	1.0***	-	-	-	-
Tele	0.246**	0.135	1.0***	-	-	-
Cyber	0.250**	-0.110	0.086	1.0***	-	-
Wealth	0.301***	-0.160	0.179*	0.340***	1.0***	-
Connect	0.329***	-0.164	0.124	0.437***	0.905***	1.0***

Table 4.1: Pearson's correlation coefficients of the existence of a national eHealth strategy, a national health information system strategy, a national telehealth strategy, a national or draft cybersecurity strategy, the natural log of the GDP per capita, and the percentage of Internet users (all in 2015).

The table shows that, generally, correlations are low to moderate, with the exception of wealth and connectivity, which has a coefficient of 0.905 - meaning (as asserted in Section 2.2) that the percentage of Internet users is highly correlated with GDP per capita. The next strongest correlations are between the existence of a national cybersecurity strategy and the measurements of wealth and connectivity, indicating that (unsurprisingly) countries with more money to spare and more Internet users are moderately more likely to have a national cybersecurity strategy. Correlation between digital health policies and wealth and connectivity varies: it is moderate (and statistically significant) for eHealth, negative for HIS, and low for telehealth. This suggests that there are a variety of complex factors that go into the creation of national digital health policies and strategies, and that these measures may be seen as useful foundations even for countries with low incomes and a relatively small number of Internet users.

4.4 Case Study

In order to better explore the relationship between cybersecurity and national eHealth strategies, we have selected a number of demonstrative case studies. We will consider

the national eHealth strategies of the four countries we mentioned in Section 4.1: Uganda, Cameroon, Nigeria, and Zambia. We have selected these four examples because their eHealth strategies were published within the last few years, their national health systems and security postures are developing, and they represent a broad variety of regions, populations, and income levels. Details about the countries (their population, GDP per capita in current US dollars, and GCI scores in 2015 and 2020) are shown in the table in Table 4.2. Note that the GCI scale changed between 2015 and 2020: in 2015, the score was between 0 and 1, and in 2020, the score was between 0 and 100. However, as the scale is comparable, we can still see that all four countries have improved their score in the five-year period. Some portion of this may be due to the passage of additional security and privacy legislation, as discussed in Section 4.3.

Country	**Pop. (1000s)**	**GDP Per Capita**	**GCI 2015**	**GCI 2020**
Uganda	45,741.00	817.0	0.559	69.98
Cameroon	26,545.86	1,499.4	0.412	45.63
Nigeria	206,139.59	2,097.1	0.441	84.76
Zambia	18,383.96	1,050.9	0.147	68.88

Table 4.2: Comparisons of countries in the eHealth foundations case study [55, 54, 27].

The four strategies vary in length and structure, the longest being Uganda's at 126 pages and the shortest being Zambia's at 45 pages. Each begins with basic context about the country and its health system before moving into a broad strategic vision for eHealth. Each contains specific goals and methods to monitor whether or not the goals been achieved by the end of the specified timeframe.

The Ugandan, Cameroonian, and Zambian documents all include a SWOT analysis of their strengths, weaknesses, opportunities, and threats in the area of eHealth - and all three include poor cybersecurity controls and capacity as a threat. However, Cameroon also includes "adoption of laws on electronic communications, cybersecu-

rity and cybercrime" as an opportunity [60, p. 22]. This is a validation of Morgus' concept of "security for" discussed in Section 2.3, which asks us to consider the positive benefits of cybersecurity efforts rather than focusing solely on what they are designed to prevent [2].

Two of the strategies discuss in detail security policies and legislation already in place that can be applied to the health sector in order to assure the security and privacy of data and systems. Uganda mentions the National Information Security Framework (NISF), which outlines "mandatory minimum security controls" applicable to organizations that deal with sensitive or personal data, and the Data Protection and Privacy Bill, which details requirements for organizations that process the data of Ugandan citizens [59, 63, 64]. Note that the Bill was passed into law in 2019 (three years after the adoption of the strategy) [64]. Nigeria acknowledges a number of broadly applicable policies: the Medical Code of Ethics, which describes safety requirements for patient data held in electronic form; the Constitution of the Federal Republic of Nigeria, which establishes a right to privacy; and the National Health Law 2014, which details access and storage rules for patient data [61]. Zambia mentions assuring information security in accordance with "CEEGICT rules and regulations"- probably referring to what is now called the Smart Zambia Institute - but is not specific about what these entail [62, p. 13]. Cameroon explicitly states that existing legislation and regulatory frameworks are inadequate for guaranteeing the security and privacy of health data - while unfortunate, this is an important acknowledgement in order to move forward [62].

Two of the strategies discuss "action owners" who are responsible for eHealth security considerations. Uganda primarily calls upon the Ministry of Health (MoH), Ministry of Information and Communications Technology (MoICT), and the National Information Technology Authority (NITA-U) as responsible for assuring information security, monitoring compliance, and developing appropriate plans and programs [59]. Cameroon states that Decree No. 2012/180 of 10 April 2012 on the

Organization and Functioning of the National Agency for Information and Communication Technologies (ANTIC) establishes the agency as responsible, in conjunction with the Telecommunications Regulatory Agency (ART), for "[regulating, controlling, and monitoring] activities related to the security of information systems and electronic communication networks" [60, p. 17].

Three of the strategies include objectives specifically related to the principles of security and privacy. Uganda's goals include creating a Business Continuity and Disaster Recovery Plan for eHealth in order to achieve resilience, an Institutional eHealth Information Privacy Protection Program to define privacy safeguards, and an eHealth Information Security Program to define security safeguards [59]. Nigeria intends to establish a National Health ICT governance structure in order to shepard the integration of ICT into the health sector and establish compliance requirements for privacy and security, which they appear to have done in September 2016 [61, 65]. Cameroon's intentions are less related to policies and agencies and more to practical requirements: for example, objective 7.1 reads "By 2022, ensure the availability and application of ICT standards in 80% of health facilities at all levels of the health pyramid" [60, p. 66]. The objective contains 40 sub-tasks, which include recruiting consultants and coordinating workshops to assist with the development of security standards, completing system audits and acquiring security certificates, and training users in secure data exchange principles [60]. However, Cameroon also includes objectives to create documents for managing guidelines related to availability assurance and incident management [60]. Zambia does not have a specific objective related to security but does mention the issue in the descriptions two other objectives: "To consolidate eHealth structures for efficiency," and "To improve coverage of Health Information Technology (HIS)" [62, p. 17, 19]. The country also does not mention privacy in its objectives section, although it includes the issue under "Strategic Priorities" [62].

Clearly, each country considers security and privacy as important components of

eHealth; however, they vary in how they have addressed these concerns. Uganda and Nigeria have the advantage of existing legislation and frameworks to help guide the security principles of their emerging eHealth systems. As such, they focus heavily on governance in their objectives: assignments for more agencies, policies, and programs to establish specific security requirements for their eHealth systems. Cameroon admits that its legislation in this area is lacking, so its primary focus is practical tasks for developing security standards to which health ICT must comply. Zambia does not make detailed mention of legislation or frameworks; however, at the time of writing there existed the 2009 Electronic Communications and Transactions Act to govern data privacy and security requirements for the public and private sector [66]. Currently, there exists an updated 2021 Electronic Communications and Transactions Act and a 2021 Data Protection Act that the country could draw upon for aid in developing eHealth security and privacy standards [67, 68]. Zambia was also not highly specific about security objectives, with the primary focus of the document being to support the adopting of eHealth systems while ensuring interoperability. To return to the WHO and ITU's National eHealth Strategy Toolkit, this may be because Zambia is primarily concerned with achieving the eHealth goals of Stage 1 and 2 before Stage 3. However, while it is important to consider patient care first, security controls can be implemented at all stages of eHealth development to create assurances of confidentiality, integrity, and availability for patients and medical professionals. Section 4.5 will consider security controls that are relevant to national eHealth strategies and policies, based on those examined during this case study.

4.5 Security Controls

As we have seen in Section 4.4, security is and should be a consideration of national eHealth strategies and policies. These documents offer a good opportunity for countries to examine their existing cybersecurity posture in relation to their eHealth

goals and identify areas for growth and investment.

While identifying poor security controls as a threat to the success of digital health programs is a good first step, it is valuable to consider specific threats that are relevant to the unique context of a country's healthcare sector. The concerns relevant to a country with a well-established eHealth system are likely different to those in a country with a disparate or developing eHealth system. On a related note, it would also be prudent to define the goals of security in the eHealth context. How important to the particular country is the availability of systems versus the confidentiality of data? What should the considerations be for a small, regional pilot program versus one that is being integrated into the national eHealth system? As a national eHealth strategy is a goal-oriented document, it is important to consider where security fits into the identified aims and how it can exist as a supportive component of the overall eHealth system.

An additional important security-related factor in an effective eHealth strategy is the identification of existing laws, frameworks, and standards that are relevant to the health sector, as demonstrated by the Ugandan and Nigerian strategies. eHealth certainly has its own unique security concerns and considerations, but this does not mean that all its requirements must be built from scratch. Acknowledging the existing security and privacy context of a country is an important step towards creating a framework that works for eHealth. If existing legislation is incomplete or inadequate, than a country can look towards its neighbors for relevant examples, adapt them to its own needs, and update the strategy as new laws are passed.

However, existing legislation cannot always be copied-and-pasted to the health sector with ease. If laws and standards have not yet been applied to the healthcare sector, it is important to ensure that their adoption goes smoothly, and that new and more specific ones are created as applicable. For this, a country should be able to appoint or create agencies to draft plans for secure data exchange, system availability and resilience, and incident response with regards to the health sector. There should

also be agencies broadly responsible for assuring the security of eHealth. Identifying "action owners," as per the example of Uganda and Cameroon, is important towards achieving eHealth strategy objectives and ensuring that responsibility is taken for all tasks.

Finally, as shown by the Cameroonian strategy, it is good to define some practical, measurable security-related tasks and indicators for their achievement by a specified date. These can include creating standards and guidelines, achieving security certifications for some percentage of major hospitals and healthcare centers, and offering basic security training to some percentage of healthcare workers. A mechanism should be specified for these tasks to be tracked and revisited.

Table 4.3 summarizes the above security controls for easy reference.

Security Control	**Description**
Identify Threats	Conduct a SWOT analysis, identifying the particular threats to the country's health sector due to poor security: attacks affecting the availability of systems, the confidentiality / integrity of patient data, etc.
Define Security Goals	Define the important security goals of the health sector, taking into account programs at different levels of maturity: creating new privacy laws, training healthcare workers, etc.
Identify Existing Laws	Identify existing laws, frameworks, and standards related to security and privacy that can be relevant to the health sector.
Adapt Existing Laws	If relevant, create a plan for adapting identified laws and frameworks into a health context.
Appoint Agencies	Appoint or create agencies responsible for handling the security of ICT in eHealth, adapting or creating policies and standards, and training healthcare workers.
Define Practical Tasks	Define measurable security goals related to training, certifications, auditing, etc.

Table 4.3: Security controls for eHealth foundations, as identified by analysis of the literature and a case study.

4.6 Conclusion

In this chapter, we have established that eHealth policies and strategies are important spaces to define the overarching threats, goals, contexts, and objectives of security and privacy in eHealth in order to govern progress and development in this sector. They serve as solid foundations on which to build eHealth programs, as they establish where a country is and where it would like to go. Additionally, we have shown that demonstrating a commitment to eHealth security in a national policy document does not require a country to diminish other crucial considerations of ICT in healthcare, such as increasing coverage or consistency. In many contexts, making progress in security can actually support these goals by helping to guarantee availability or resilience. It is up to the individual nation to define what their security and privacy intentions are and how those should be achieved - and in fact, many countries already include security in their national eHealth policies in order to help realize the benefits of ICT in healthcare.

In the next chapter, we will build on our foundation by discussing the role of security in the next step in eHealth governance: legal and regulatory frameworks.

Chapter 5

Legal Frameworks

5.1 Introduction

While national policies and strategies serve as an excellent foundation for eHealth, their purpose is to facilitate the growth of digital health programs. As such, they are incomplete without strong commitments from the government - and one of these commitments should be in the form of legislation and regulatory frameworks. This chapter addresses the Legal Frameworks section of the WHO eHealth survey, the bulk of which comprises questions about privacy legislation applicable to patient data. We will begin by examining the importance of eHealth and eHealth privacy legislation in the literature before moving on to consider the data at hand, concluding that the existence of eHealth and eHealth privacy legislation have relatively strong correlations with income levels and Internet usage. We will then examine the existing eHealth security and privacy legal framework of two countries before concluding with a discussion of relevant security controls and considerations for such legislation.

5.2 Literature

Strong legal and regulatory frameworks are critical to the success of healthcare programs and the achievement of universal health coverage [11]. Yet in a 2011 European

Commission report on European eHealth progress, Stroetmann et.al. states that "[l]egal and regulatory issues are among the most challenging aspects of eHealth" [69, p. IX]. This is likely due to the multidimensional aspect of the topic: according to the report, good eHealth frameworks should address "privacy, confidentiality, liability and data protection...in order to enable a sustainable implementation and use of eHealth applications" [69, p. IX]. The WHO's 2016 Global Diffusion of eHealth report adds even more legal considerations, including technology acquisition, interoperability, and compliance with standards [11]. These are difficult tasks to undertake: the European Commission report noted that, at the time of writing, few European countries had a coherent legislative framework addressing eHealth and relied instead on existing precedent related to health and privacy (though the majority or EU member states were engaged in drafting legislation) [69].

Without effective governance and regulation, even countries with significant technological capacity can struggle to realize the full benefits of eHealth. A 2015 review of Denmark's eHealth system argued that "despite Denmark's high levels of eHealth deployment across the health sector, the Danish healthcare system faces significant interoperability challenges stemming from the country's governance structures decentralized and centralized approaches to eHealth implementation...In hindsight, Denmark could have avoided these interoperability challenges from an early stage if the state had issued regulations designed to ensure the harmonization of the technical requirements for EHRs in conjunction with the launch of the initial national IT strategies" [70, p. 43].

Interestingly, over-regulation may cause problems as well. A 2019 analysis of German and United States telemedicine legislation suggests that while some restrictions on the practice are necessary to protect patients, others may unnecessarily hinder access to medical treatment [71]. Additionally, in a 2021 paper Jočić argues that Solvenia's strict data protection regulations have at times negatively impacted the availability of patient data to medical professionals who legitimately need access,

particularly during the 2020-2021 COVID-19 pandemic [72]. Says Jočić, "exhaustive legislation did not help to resolve uncertainty" - in fact, it may have increased it, as medical professionals were not always aware of what level of access themselves or their colleagues should have to patient data [72]. This brings us back to the notion of balance discussed in Section 2.5: security and privacy in eHealth are designed to serve patients, and these considerations must not take away from issues of accessibility and quality of care. Additionally, legislation must be clearly and carefully worded in order to properly serve its purpose.

A 2019 case study of efforts by Unjani Clinics to offer health care to underserved rural populations in South Africa discusses the 2014 National Health Normative Standards Framework for Interoperability in eHealth (HNSF), which attempts to support interoperability and access to relevant patient data while still complying to South African privacy legislation such as the Protection of Personal Information Act of 2013 [73]. The HNSF outlines detailed processes for the electronic storage of and access to patient information, including requirements for authentication, authorization, and secure communication based on the ISO/TS 22600-1 and ISO/TS 27527 standards on health informatics [74]. The case study includes the ways in which Unjani Clinics attempts to comply with these laws and frameworks, include the use of two-factor authentication, the application of the principle of least privilege, and the maintenance of confidentiality [73]. Once again, however, we are reminded by the case study's authors that "the question of whether South Africa's legislation and Unjani's measures are sufficient to protect privacy and patient data stands against the question of the alternative: in a remote rural setting, a teleconsultation with a doctor is likely to be the only way to get access to a doctor at all and could easily become a lifeline" [73, p. 114]. Yet in some cases failing to address privacy can decrease trust and prevent patients from accessing medical care anyway: says the WHO, "experience in stigmatized diseases such as HIV has shown that unless privacy is addressed very clearly by public authorities, patients are often unwilling to

seek treatment" [11, p. 109]. In order to ensure that eHealth technologies are trusted and used, countries must therefore be prepared to develop legislation that addresses its eHealth security and privacy needs at a given time, from data transmission and storage requirements to availability and resilience considerations.

5.3 Data

Once again, we look to the 2015 WHO eHealth survey. The questions asked in the Legal Frameworks section cover much of the important legislative qualities discussed in Section 5.2: liability, privacy, and data protection, as well as patient care [51]. Of respondents, 31% claimed to have legislation defining liability and authority for eHealth programs, 46% claimed to have legislation applicable to data integrity as related to patient care, 78% claimed to have broadly applicable privacy protections, and 54% claimed to have privacy protections applicable to electronically stored patient data.

We will also look at legal frameworks broadly applicable to cybersecurity, again taking data from the 2015 ITU Cyberwellness Profiles [54]. These are relevant because legislation broadly focused on security and privacy can often be used as a basis for legislation covering security and privacy in the context of eHealth. Additionally, privacy or security laws may already have direct applicability to patient data and systems used in healthcare. A review of the Cyberwellness Profiles indicates that, in 2015, 72% of countries had a law pertaining to cybercrime and an additional 6% had a draft in progress or a plan to implement such legislation in the future. This legislation indicates a commitment to taking data breaches and cyberattacks seriously. Additionally, 62% of countries had some sort of legislation addressing "regulation and compliance" (cybersecurity standards, privacy, and/or notification of data breaches), and an additional 6% had a draft in progress or a plan to implement such legislation in the future. 62% of countries had existing legislation, draft

legislation, or planned legislation for both categories, and 17% of countries had no legislation, drafts, or plans for either.

Finally, Table 5.1 displays the Pearson's correlation coefficients between the existence of the eHealth, patient safety, privacy, cybercrime, and cybersecurity regulation laws discussed above and our measurements of wealth (the natural log of GDP per capita) and connectivity (the percentage of Internet users). The symbols ***, **, and * next to the coefficients indicate significance levels of below 0.001, 0.01, and 0.05, respectively.

	eHealth Laws	**Safety Laws**	**Privacy Laws**	**Health Privacy**	**Cyber Crime**	**Cyber Laws**	**Wealth**	**Connect**
eHealth Laws	1.0 ***	-	-	-	-	-	-	-
Safety Laws	0.481 ***	1.0 ***	-	-	-	-	-	-
Privacy Laws	0.270 **	0.371 ***	1.0 ***	-	-	-	-	-
Health Privacy	0.443 ***	0.530 ***	0.495 ***	1.0 ***	-	-	-	-
Cyber Crime	0.175	0.177 *	0.319 ***	0.294 ***	1.0 ***	-	-	-
Cyber Laws	0.285 **	0.322 ***	0.256 **	0.462 ***	0.511 ***	1.0 ***	-	-
Wealth	0.444 ***	0.538 ***	0.327 ***	0.480 ***	0.318 ***	0.460 ***	1.0 ***	-
Connect	0.405 ***	0.477 ***	0.408 ***	0.543 ***	0.396 ***	0.528 ***	0.905 ***	1.00 **

Table 5.1: Pearson's correlation coefficients of the existence of eHealth legislation, patient safety legislation, data privacy legislation, health data privacy legislation, (existing or draft) cybercrime legislation, (existing or draft) regulation and compliance legislation, the natural log of the GDP per capita, and the percentage of Internet users (all in 2015).

In contrast with Section 4.3, correlations are generally stronger in this category. Health-related legislation generally correlates moderately with other types of

health-related legislation, and cybercrime legislation correlates strongly with cybersecurity regulations. Additionally, across the board wealth and connectivity correlate moderately-to-strongly with the presence of any of the six types of legislation considered, with the strongest correlations between health data privacy laws and connectivity, cybersecurity regulations and connectivity, and patient safety laws and wealth. This indicates a stronger connection between these factors and the existence of legislation than policies or strategies, which may be due to the complexity of this requirement. While it is possible - and recommended - to create a national eHealth strategy at even the earliest stages of eHealth development, creating effective legislation is suggested by the National eHealth Strategy Toolkit as a focus for the second stage, developing and building up [58].

5.4 Case Study

In order to engage further with the topic of eHealth legislation, we will examine two case studies. We will begin with the example of Canada, then move on to discuss Kenya. Canada was chosen because of its well-established healthcare system and legal framework, while Kenya was chosen because of its recent commitments to the privacy of personal data, particularly with regards to the passage of the 2019 Data Protection Act [75]. Details about the countries, including population, GDP per capita in current US dollars, and the GCI index scores in 2015 and 2020, are shown in Table 5.2. As above, note that the scale of the GCI rankings has changed between 2015 and 2020; however, it is still possible to see that both countries have increased their rankings significantly over the five-year period.

Canada employs a universal health care system: citizens and permanent residents may apply for public health insurance, which covers the cost of most health care procedures [76]. However, the system is provided for at a province / territory level, rather than at a federal level. As such, many provinces and territories have

Country	Pop. (1000s)	GDP Per Capita	GCI 2015	GCI 2020
Canada	38,005.24	43,241.6	0.794	97.67
Kenya	53,771.30	1,838.2	0.412	81.7

Table 5.2: Comparisons of countries in the legal frameworks case study [55, 54, 27]

passed their own health laws to override or supplement federal laws. The federal law addressing publicly funded health insurance is the Canada Health Act, first adopted in 1984, which describes the conditions that each province and territory must fulfil in their administration of healthcare services to their populations [77, 78]. These conditions are primarily related to access, coverage, and payment; they do not include mentions of quality of treatment, digital health technologies, or security. However, the annual reports discussing province compliance to the law do make mention of responsible agencies in each province and their respective commitments to high standards of care, health and information technologies, and data privacy [77].

From a security perspective, Canada's criminal code defines "knowingly [intercepting] a private communication" (without consent) as a crime, while its "Anti-Spam Law" prevents commercial entities from "[installing]...a computer program on any other person's computer system or...[causing] an electronic message to be sent from that computer system" (again, without consent) [79, 80]. Canada's federal data protection law is the Personal Information Protection and Electronic Documents Act (PIPEDA), which was first passed in 2000 but last amended in 2019 [81]. However, in Alberta, British Columbia, and Quebec, PIPEDA has been superseded by provincial data protection laws [82]. Broadly, the act requires private-sector organizations which collect users' personal data to attain appropriate consent from these users, as well as disclose any security breaches and compromises of personal data in a timely fashion. It also includes principles from the National Standard of Canada Entitled Model Code for the Protection of Personal Information, such as "personal

information shall be protected by security safeguards appropriate to the sensitivity of the information" [81, p. 53]. The principle states that these safeguards should comprise physical, organizational, and technical controls. Finally, the act states that "the Governor in Council may, on the recommendation of the Treasury Board, make regulations prescribing technologies or processes for the purpose of the definition secure electronic signature" [81, p. 44-45] - something that was accomplished in 2005 via the Secure Electronic Signature Regulations, which addressed the signing of documents via asymmetric cryptography and cryptographic hash functions, as well as appropriate signature validation methods [83].

From a health perspective, PIPEDA defines the term "personal health information" as (among other things) "information concerning the physical or mental health of the individual" [81, p. 3]. However, it is clear that the law is a broadly applicable data privacy law rather than one tailored to a healthcare context. That said, four provinces - Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador - have defined their own privacy legislation particularly related to personal health data [82]. Details of these laws are in Table 5.3.

Province	**Law**	**Date**
Ontario	Personal Health Information Protection Act (PHIPA)	2004
New Brunswick	Personal Health Information Privacy and Access Act (PHIPAA)	2009
Nova Scotia	Personal Health Information Act (PHIA)	2010
Newfoundland and Labrador	Personal Health Information Act (PHIA)	2008

Table 5.3: Health data protection laws in Canadian provinces, superseding the considerations of Canada's federal privacy legislation [84, 85, 86, 87].

The four acts are generally similar to one another, and in some cases it is clear that later acts were inspired by earlier ones. They are all explicitly stated to apply

to "health information custodians," such as health care professionals, who process personal health data. Each defines the conditions of a patient's right to access and correct their health information. Each considers the mechanisms of patient consent and the collection, use, and disclosure of data. Each requires the health information custodian to disclose security breaches of patient data. Additionally, each includes some consideration as to the secure storage and transmission of data. Ontario's PHIPA requires that custodians "ensure that the records containing the information are protected against unauthorized copying, modification or disposal" [84], and a 2020 ammendment discusses auditing requirements for access to health data. New Brunswick's PHIPPA necessitates "reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information" based on government-recognized standards, including measures to restrict access to authorized parties and prevent the interception of sensitive communications [85]. Nova Scotia's PHIA and Newfoundland and Labrador's PHIA both include similar statements [86, 87].

Kenya's healthcare system has changed a great deal following the 2010 constitution: since then, many new agencies have been created and laws enacted in the hope of reaching the goal of universal health coverage [88]. The most critical of these is the 2017 Health Act, which attempted "to establish a unified health system, to coordinate the inter-relationship between the national government and county government health systems, [and] to provide for regulation of health care service and health care service providers, health products and health technologies and for connected purposes" [89, p. 420]. The act defines roles and responsibilities for various offices and creates plans to establish public healthcare centers, promote public health, and conduct research. In Part XV, "E-Health,", the act also promises the following:

> 104. The Cabinet Secretary shall, within three years of the operation of this Act, ensure the enactment of legislation that provides for among other things -

(a) administration of health information banks including interoperability framework, data interchange and security;
(b) collection and use of personal health information;
(c) management of disclosure of personal health information;
(d) protection of privacy;
(e) business continuity, emergency and disaster preparedness;
(f) health service delivery through M-health, Elearning and telemedicine;
(g) E-waste disposal; and
(h) health tourism. [75, p. 469-470]

As of the time of writing, the promised legislation was still in draft form [88]. However, there are are still a number of general cybersecurity provisions in Kenya's legislation. The 2018 Computer Misuse and Cybercrimes Act outlawed various computer-related crimes, including hacking, phishing, identity theft, and intercepting electronic communications [90]. It should be noted that this law is not without controversy, and has been criticized for vague language (e.g., outlawing "intentionally publish[ing] false, misleading or fictitious data or misinform[ing] with intent that the data shall be considered or acted upon as authentic" [90, p. 58]) that may open up the doors for censorship and surveillance. Such provisions have kicked off a number of contentious legal battles [91, 92, 93].

Additionally, in 2019 Kenya established the Data Protection Act, which established rules for the processing of personal data, an obligation to notify victims of data breaches, and a right to access one's own personal data. The act also compels data processors to assess potential security risks to the data they maintain and implement safeguards ensuring confidentiality, integrity, availability, and resilience [75]. The law does define "health data" - similarly to Canada, as (among other things) "data related to the state of physical or mental health of the data subject" - and explicitly includes health data as relevant under the law [75, p. 906]. However, the act also recommends that the Data Commissioner "develop sector specific guidelines in consultation with relevant stakeholders in areas such as health" [75, p. 942]. It is possible that the promised future eHealth legislation will include such guidelines.

In the meantime, the government of Kenya has released a number of standards

applicable to health. The 2013 Health Sector ICT Standards and Guidelines document includes detailed requirements for physical and technical security controls such as the following:

- identification badges
- visitor logs recording access to controlled areas
- principle of least privilege
- auditing of failed user logins
- password length and complexity requirements
- secure data backups and recovery procedures
- encryption of sensitive data
- network monitoring [94]

Additionally, the 2010 Standards and Guidelines for Electronic Medical Record Systems in Kenya and 2020 Kenya Health Information Systems Interoperability Framework documents, which respectively aim to facilitate the adoption of EHRs and the interoperability of health systems, make mention of access control, auditing, backups, encryption, and other security controls [95, 96]. While these are not written into law, they still provide useful guidelines to healthcare organizations and may be used as referenced points for future eHealth laws.

It is clear from these two examples that creating effective healthcare legislation is a complex task: it is highly unlikely that a single law, passed once, will be sufficient, but that a variety of evolving laws, standards, and frameworks will need to reference and build off of each other in order to cover all necessary objectives. However, it is also possible for determined countries to make progress quickly, perhaps "leapfrogging" over some of the intermediate steps taken by nations with longer-established eHealth systems. Since 2010, Kenya has made significant progress in centralizing eHealth and establishing a right to the privacy of personal data. In Section 5.5, we will consider what tasks still lie ahead by looking at security and privacy considerations relevant to eHealth legislation.

5.5 Security Controls

We have learned in Section 5.4 that good eHealth legislation is the result of an iterative process, built upon good healthcare and security legislation. In order to address relevant issues in eHealth, a country needs to have strong governance mechanisms already in place to structure their healthcare system and relationship to technology.

Both Canada and Kenya consider cybercrime and data privacy in separate pieces of legislation. While it can be tempting to consider the two issues together, as they both broadly fall under the category of "security," their disparate nature makes it challenging to synthesize their unique requirements and incentives. According to Privacy International,"failing to draw distinction between the two risks undermining security and diluting protection for everyone." [97, p. 3].

Criminalizing hacking, phishing, and other computer-dependent crimes is a minimum requirement to keep people and organizations - including healthcare institutions - safe. Ideally, cybercrime laws should be specific and narrow, focusing only on crimes that require the unauthorized use of a computer (e.g., distributed denial of service attacks) rather than crimes that merely employ a computer (e.g., fraud) [97]. The latter category of crime should be addressed by other legislation. Additionally, governments should take care not to reduce individuals' rights by restricting speech or expanding surveillance in cybercrime laws, as has caused controversy in Kenya [97]. Finally, clear exceptions must be made for penetration testing, red teaming exercises, bug bounty programs, and security research. In order to maintain a "security for" mentality, as discussed in Section 2.3, it is important that such legislation enables rather than hinders the development and expansion of ICT, particularly in an eHealth context.

Once criminal legislation is complete and enforceable, looking to preserving privacy rights is an important next step. The right to privacy is enshrined in Article 12 of the United Nations Universal Declaration of Human Rights and has subsequently been recognized in the constitutions and legal frameworks of many nations [98]. Gen-

erally, privacy and data protection laws should create limits on the collection and processing of personal data; require safeguards for the maintenance of its integrity and confidentiality (such as encryption and auditing); and establish individuals' rights to query, correct, and delete their own information [99].

However, both of the above laws are quite broad and unlikely to include specific provisions for healthcare systems and eHealth technologies. As such, it is sensible to address security and privacy in the context of eHealth legislation, as accomplished by the four Canadian provinces discussed above and as Kenya is currently attempting to do. These should consider the uniquely sensitive nature of health data as well as the contexts in which it is used. Additionally, governments should create security standards and guidelines for the storage of health data and administration of health technologies. These should include measures such as the restricting access to sensitive data, encrypting data in transit and at rest, monitoring networks for alerts, and taking (and testing) backups to maintain resilience in the face of a security incident. eHealth legislation may reference these standards when outlining requirements for healthcare programs and technologies. However, it is also important to note that different standards of security may be relevant for different technologies: for example, a pilot telehealth program targeting rural areas will not have the same security requirements as an administrative department of a large, well-connected hospital. Legislation and guidelines should reflect these differences while maintaining a minimum level of security and privacy in order to avoid hindering new developments in health and expanded access to care.

Table 5.4 summarizes the above controls for easy reference.

5.6 Conclusion

In this chapter, we have established that healthcare legislation is a deeply important but challenging component of achieving national health goals. Such legislation is

Security Control	Description
Cybercrime Legislation	Create specific, narrow legislation criminalizing hacking, phishing, and other computer-dependent crimes and a mechanism to enforce it.
Privacy Legislation	Create legislation guaranteeing a right to privacy, limiting the collection of personal data, and establishing a right of access to one's data.
Health Privacy Legislation	Where gaps exist, create privacy legislation specifically addressing the storage and processing of personal health data.
Health Security Standards	Create clear security standards for various eHealth technologies, such as data stored in EHRs and interoperable systems.
Health Security Legislation	Create legislation addressing the security of health data and technologies, considering both pilot and well-established programs and referencing existing security standards if relevant.

Table 5.4: Security controls for eHealth legal frameworks, as identified by analysis of the literature and a case study.

complex, iterative, and requires effective enforcement mechanisms. While creating a high-quality eHealth legal framework may seem like a similar task to creating an eHealth policy, the latter requires significantly fewer time and resources and a weaker governance commitment: an eHealth policy can exist as a single document created by only a few individuals, whereas an eHealth legal framework requires many laws created over a period of time and approved by a congressional or parliamentary body. However, we have shown through our case studies that it is possible to make significant progress in building and incoporating cybersecurity and privacy considerations into such a framework, even in a relatively short period of time. As more countries attempt this, they may look to their neighbors for guidance on the clarity and effectiveness of their own legislation.

In the next chapter, we will move beyond policy and governance to discuss one of the technical facets of eHealth: mHealth and telehealth programs.

Chapter 6

mHealth and Telehealth

6.1 Introduction

In this chapter, we begin to move on from policy, legislation, and governance to the items these efforts are meant to support: healthcare technologies. Here we will discuss mHealth and teleHealth. The WHO defines mHealth as "the use of mobile devices – such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and wireless devices – for medical and public health practice" and telehealth as "the practice of medicine at a distance" [11, p. 27, 56]. As such, they are rather similar concepts that often overlap; here we will treat them together.

As with previous chapters, we will begin with a review of papers and studies about security concerns in mHealth and telehealth programs and technologies. We will then conduct our own analysis of data from the WHO eHealth survey, determining that in many cases remote healthcare technologies have few correlations with a country's level of wealth, likely due to their perceived benefits to development and healthcare accessibility. We will then review the security of a number of mHealth applications available in India as a case study and conclude with a series of legislative and technical security controls to implement in mHealth and telehealth programs.

6.2 Literature

mHealth and telehealth are two of the most celebrated applications of eHealth to development, as their nature allows for the delivery of care to remote and underserved populations which may not have frequent in-person access to medical professionals [11]. There are a number of success stories in this area, from using a mobile application to track indicators of child health in Uganda to remotely monitoring patients with chronic illnesses in North and South America [8]. Remote health technologies have also become increasingly popular during the COVID-19 pandemic due to the increased difficulty of meeting face-to-face with one's doctor and the need to track the progress of the disease [100]. As worldwide usage of mobile devices expands, it is likely that remote communications technologies will continue to play an even larger role in healthcare [8].

However, increased use of these technologies carries with it increased security and privacy concerns. A 2017 review of research studies on the security and privacy of telehealth systems revealed that while "privacy and security is a concern across all types of specialties such as telerehabilitation, telenursing, teletrauma, and telepsychiatry," a great deal of uncertainty still exists about risk, compliance, and best practices [101]. A 2019 survey of 31 telehealth providers in the United States revealed that while all had some privacy and security policies in place, they varied in the quality of their technical security measures: roughly 10% did not require the use of strong passwords, 19% lacked an incident response plan, and 22% had not had an independent security evaluation [102]. There was also a great deal of uncertainty for many questions: for example, 16% of respondents were unaware whether access controls were in place to prevent unauthorized individuals from accessing patient data.

In a 2017 paper on mHealth security, Sampat and Prabhakar identified six key privacy and security risks to mHealth applications: poor data collection practices, poor data storage practices, disclosure of health information to third parties

and advertisers, unencrypted connections, phone loss or theft, and data security breaches [103]. Yet these issues have not been properly addressed in many applications. During a 2018 review of 20 popular mHealth applications on the Android store, Papageorgiou et. al. found that a number of the apps lacked privacy policies and many requested permissions they did not require, such as microphone or camera access, location data, or approval to read and write SMS messages [104]. Only half of the tested applications used an encrypted HTTPS connection for all communications in which health data was transmitted, and many transmitted health data and user passwords in the URLs of GET requests. Similarly, a 2015 review of 79 mobile health applications certified as safe by the UK NHS Health Library found that none encrypted personally information stored locally, 66% did not encrypt potentially sensitive information sent over the Internet, and 20% had no privacy policy [105].

Theft or loss of mobile devices is also a serious issue: in a 2019 study on the use of mHealth applications to manage and follow up with cervical cancer patients in Cape Town, South Africa, 58% of the 364 participants reported that they had previously experienced loss or theft of their mobile phones, and 28% reported that this had happened within the last year [106]. Additionally, phone sharing with family members, neighbors, and friends was reported as a potential threat to confidentiality. These scenarios could potentially allow unauthorized individuals, whether malicious actors or curious acquaintances, to access unsecured applications or read SMS messages with personal health data.

A 2020 analysis of mHealth security and privacy papers identified three common themes for success in this area: the use of well-tested platforms compliant with existing security and privacy legislation (hence the importance of creating legal frameworks, as discussed in Chapter 5), the establishment of trust through a consent-based model, and the perception by end users that their data is secure [107]. In a 2017 paper, Watzlaf et. al. suggested determining security standards for telehealth systems based on the activities being carried out remotely: for example, caring for

patients directly will require more stringent measures than handling anonymized data for research or administrative purposes [108]. Additionally, some countries have altered their telehealth requirements in light of the COVID-19 pandemic: for example, the United States issued a notification in March 2020 allowing health professionals to use remote communications technologies, such as Zoom or Google Hangouts, that do not ordinarily comply with the Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy Rules [109]. This speaks to the relevance of contextualizing security and privacy requirements, as well as balancing these goals with accessibility.

6.3 Data

The 2015 WHO eHealth survey divided telehealth and mHealth into a variety of programs, asking for each about the level at which the program is managed (i.e., international, regional, national, intermediate, and/or local/peripheral) and the maturity of the program (i.e., informal, pilot, and/or established) [51]. The five considered telehealth programs were teleradiology, teledermatology, telepathology, telepsychiatry, and remote patient monitoring, while the 14 considered mHealth programs included (among others) appointment reminders, disaster management, patient monitoring, and disease surveillance. 80% of countries claimed to have at least one telehealth program, and 89% of countries claimed to have at least one mHealth program. Only ten countries, 8% of respondents, reported no programs in either category. Interestingly, 16 countries (roughly 13% of the total) claimed to have all queried programs in place at some maturity level. These countries represented all regions and income levels, although nine were from the European region and eight were high income.

Unfortunately, the survey does not request further details of these programs, whether related to security, privacy, or other domains. As such, we will simply use the 2015 GCI score in our data analysis. As this score is a reflection of a country's

overall cybersecurity capacity - the existence of national strategies, legislation, national certification standards, incident response teams, and more - it is a reasonable reflection of how prepared a country may be towards managing emerging threats in the health sector.

Table 6.1 shows the Spearman's correlation coefficients between the number of mHealth and telehealth programs in place in a given country, the country's GCI score, and the country's wealth (natural log of the GDP per capita) and connectivity (percentage of Internet users). Note that Spearman's correlation was used instead of Pearson's correlation for this analysis due to the fact that the number of mHealth programs and the number of telehealth programs are count data rather than continuous or binary data following a normal distribution. The symbols ***, **, and * next to the coefficients indicate significance levels of below 0.001, 0.01, and 0.05, respectively.

	mHealth	**Telehealth**	**GCI**	**Wealth**	**Connectivity**
mHealth	1.0***	-	-	-	-
Telehealth	0.603***	1.0***	-	-	-
GCI	0.385***	0.450***	1.0***	-	-
Wealth	0.140	0.358***	0.481***	1.0***	-
Connectivity	0.174	0.381***	0.576***	0.906***	1.0***

Table 6.1: Spearman's correlation coefficients of the mHealth program count, telehealth program count, the GCI score, the natural log of the GDP per capita, and the percentage of Internet users (all in 2015).

The coefficients show that while the number of mHealth and telehealth programs present in a country correlate strongly with one another - supporting the behaviour discussed in Section 3.2 - wealth and connectivity do not have statistically significant correlations with the number of mHealth programs. This may indicate that mHealth programs are being initiated in countries at all levels of development due to their perceived benefits to both highly connected and rural, underserved populations. Interestingly, a country's GCI score does have a moderate correlation with both its reported number of mHealth programs and reported number of telehealth programs,

perhaps pointing to the trend discussed in Section 3.2 that countries with advanced GCIs have typically already invested heavily in eHealth.

These effects are further demonstrated by the scatterplots in Figure 6.1, which plot the count of mHealth and telehealth programs in respondents to the 2015 WHO eHealth survey against the natural log of their GDP per capita and their 2015 GCI score. Regions are denoted by the hue of the data points.

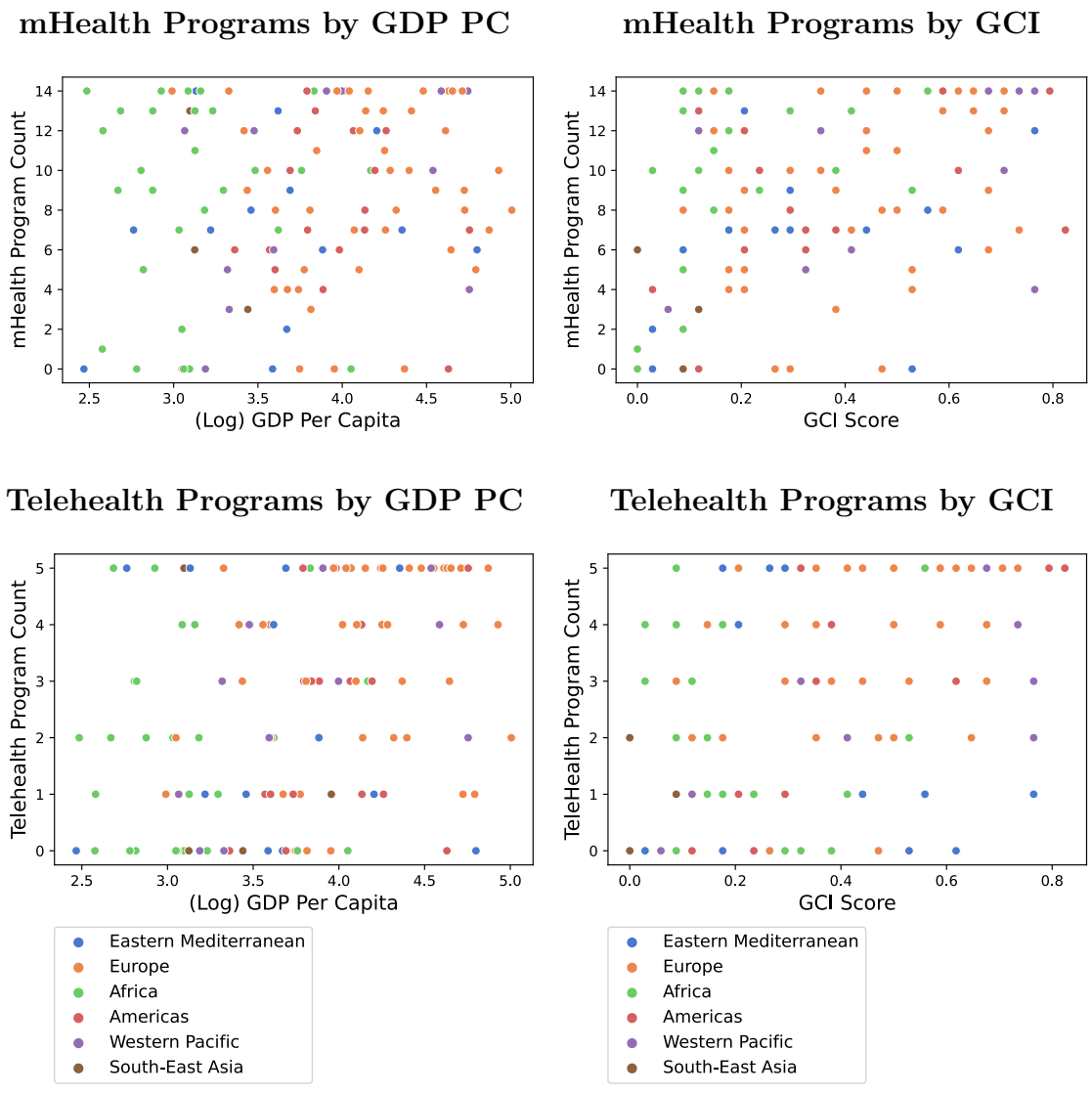

Figure 6.1: Scatterplot of the number of mHealth and telehealth programs versus the natural log of GDP per capita. These charts show that mHealth and telehealth progress is possible (and even common) at all national income levels due to its accessible nature.

The scatterplots demonstrate visually that telehealth and mHealth programs are

frequently present at low GCI scores and GDP per capita values and at high GCI scores and GDP per capita values. All regions are represented at the highest program counts. This indicates that mhealth and telehealth programs may be highly accessible to countries that are neither wealthy nor have a strong cybersecurity capacity. This is understandable, given that many countries are attempting to exploit the benefits of ICT and expanding mobile broadband access to their developing health sectors, and many nonprofits and nongovernmental organizations are leveraging remote communications programs to offer healthcare to isolated communities. However, as these programs expand and integrate with larger health care systems, it becomes increasingly important to ensure that the security of users' data and the availability of health technologies is maintained. We will explore this idea further in our case study in Section 6.4.

6.4 Case Study

As a case study of the role of mHealth and telehealth security in healthcare systems, we will look to the example of India. Details about India are available in Table 6.2. As above, note that the scale of the GCI rankings has changed between 2015 and 2020; however, it is still possible to see that India has increased its ranking significantly over the five-year period. In particular, India has increased strongly in the cooperative measures tier.

Country	**Pop. (1000s)**	**GDP Per Capita**	**GCI 2015**	**GCI 2020**
India	1,380,004.39	1,900.7	0.706	97.5

Table 6.2: Summary of the mHealth and telehealth case study country. [55, 54, 27]

As of 2019, India had 84 mobile cellular subscriptions per 100 citizens; as of 2020, an estimated 43% of the country's population had used the Internet in the past month [55, 110]. At the same time, inequalities to healthcare access remain

a significant issue: a 2013 paper reported that "the 50 per cent of India that lives beyond a radius of five kilometres from the nearest town faces much greater odds of disease, malnourishment, weakness and premature death" [111, p. 9]. The potential of remote healthcare applications for individuals living far away from hospitals and health clinics is clear; however, effectively deploying ICT is not always a straightforward effort. In 2017, Haenssgen expressed concern that increased usage of mobile phones among wealthier rural individuals may actually disadvantage poorer rural individuals if in-person care options are replaced by remote health services they cannot afford to use [112].

In 2020, India's Ministry of Health and Family Welfare released the Telemedicine Practice Guidelines [113]. The guidelines define telemedicine and telehealth and state their advantages for increasing access to health care, particularly in the case of distance, disasters, or contagious diseases that may make it difficult or dangerous for patients to visit health care providers in person. Unfortunately, the guidelines do not include any standards for managing the security of data. In fact, the document can be a little misleading: it lists "privacy ensured" as a strength of audio-based telemedicine, when in reality phone calls and VOIP can be vulnerable to eavesdropping if security is ignored [114, 115]. However, the guidelines do reference the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, which require organizations to maintain or comply with a "comprehensive documented information security programme and information security policies" such as ISO 27001 [116]. While the Rules include some limited data protection considerations, India's full Data Protection Bill 2019 was still in draft form at the time of writing [117].

In a 2020 paper, Agarwal and Biswas survey a selection of 22 mHealth applications offering online consultations with doctors in India [118]. The authors discuss the benefits these applications can offer to increasing healthcare access; however, like Haenssgen, they also express concerns related to cost: "modern mHealth apps run

on smartphones, which are often expensive" and impossible to afford for a family living below the poverty line [118, p. 155]. Smartphone applications are an even larger barrier than SMS-based programs, such as Rwanda's Babyl, which can operate on lower-cost feature phones [119]. However, they have significantly enhanced functionality.

There are a few security concerns with SMS-based mHealth programs: for example, SMS is unencrypted and prone to social engineering attacks [120]. However, these are difficult issues to resolve as they are "baked-in" to the protocol: if a person does not have a smartphone, they may have few alternative options for remote healthcare, and the benefits of access to medical consultations may trump these particular security concerns. However, the enhanced and varied functionality of smartphone applications creates a larger attack surface and more opportunities for application developers to influence the security of the final product.

Taking inspiration from the security review by Papageorgiou et. al. discussed above, we have used the Mobile Security Framework, an open source, automated security testing tool available on GitHub, to conduct a static code analysis of the APKs of a selection of 13 of the Indian mHealth applications discussed in the survey by Agarwal and Biswas [104, 121, 118]. All of the applications were publicly available on the Google Play Store as of the time of testing. They are as follows:

- Ask Apollo
- Ask A Doctor
- CallDoc
- docOPD
- India Dental World
- India Health Line
- I Online Doctor
- Lifecare Health
- Lybrate
- Medibuddy
- Netmeds
- Practo
- Wayu MD

All of the applications offer online video, audio, and/or text consultations with doctors, as well as additional functionalities ranging from booking appointments to ordering medication to storing medical data. As such, secure coding, data storage,

and data transmission practices are a concern.

A summary of the issues identified by the Mobile Security Framework and the percentage of affected applications is available in Table 6.3. Note that in some cases these issues are less severe than others, and many of them are dependent on the specific configurations and use cases of the applications in question.

Unsurprisingly, the static code analysis identified many issues similar to those found by Papageorgiou et. al, indicating that secure application coding practices are challenging for many developers. The main issues identified were related to poor cryptography, such as the use of weak hashing algorithms and encryption modes, poor random number generation, and acceptance of SSL certificate errors. While in some cases cryptographic weaknesses may be difficult to exploit, they can lead to serious consequences for data confidentiality and integrity, and as established in Section 2.5 medical data is particularly valuable to attackers. Additionally, there are many well-researched best practices that application developers can follow when incorporating cryptographic controls into their applications without adding significant time or cost to a development project [122, 123].

Other issues primarily related to the potential leakage of data. This described either data that could be used to compromise the application or its infrastructure, such as hardcoded keys or credentials, or that could be used to steal sensitive information about the application user, such as data written to external storage or a log. Hardcoded data identified included keys for a wide variety of external services, from APIs to payment gateways to encrypted chat programs - even when the documentation of these services emphasizes the importance of keeping these keys a secret. While many services offer options to restrict the use of keys, such as defining whitelisted IP addresses, this may not always be the case, and these options may not always be used. Like cryptography, poor data storage issues may be hard to exploit, but a determined attacker or a malicious application could take advantage of them in order to gather users' personal or medical data. Also like cryptography, strong

Per.	Severity	Issue
85	High	App can read/write to External Storage.
46	High	The App uses the encryption mode CBC with PKCS5/PKCS7 padding.
38	High	Insecure Implementation of SSL.
38	High	WebView ignores SSL Certificate errors and accept any SSL Certificate.
23	High	Calling Cipher.getInstance("AES") will return AES ECB mode by default.
23	High	Weak Encryption Algorithm Used.
15	High	Remote WebView Debugging is enabled.
15	High	This App may request root (Super User) privileges.
7	High	The file is World Readable.
85	Warning	Files may contain hardcoded sensitive information.
85	Warning	The App uses an insecure Random Number Generator.
77	Warning	App creates temp file. Sensitive information should never be written into a temp file.
77	Warning	App uses SQLite Database and executes raw SQL queries. Untrusted user input in raw SQL queries can cause SQL Injection.
70	Warning	IP Address disclosure.
70	Warning	MD5 is a weak hash known to have hash collisions.
70	Warning	SHA-1 is a weak hash known to have hash collisions.
62	Warning	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.
92	Info	The App logs information. Sensitive information should never be logged.
69	Info	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.
23	Info	App can write to App Directory. Sensitive Information should be encrypted.

Table 6.3: Results of the static code analysis of 13 mHealth applications available in India using the Mobile Security Framework, citing the issue (as written), the severity level, and the percentage of applications affected [121].

best practices exist for proper data storage that could be followed and verified by developers [122, 123].

Additionally, in some cases insecure coding practices, such as improper escaping of SQL queries were used. An example of one potentially dangerous query identified is as follows (with indentations added for readability):

```
Cursor rawQuery = sQLiteDatabase.rawQuery(
 "SELECT * from supporttable
 WHERE patient_name = '" + string2 + "'
 AND doctor_name = '" + string4 + "'"
 , null);
```

Using string concatenation, rather than preparing the query using question marks in place of the variables, can open the door to SQL injection attacks if user input is included in the query. Note that in this particular case the local Android SQLite database appears to be in use; however, this does not mean that sensitive information cannot be discovered by the user.

In addition to the static code analysis, an analysis of the applications' manifest files revealed that six of the 13 applications (46%) set the variable "usesCleartext-Traffic" to "true", indicating an intention to use or fall back to unencrypted traffic, which could result in the leakage of sensitive data to eavesdroppers.

The majority of the apps also requested significant permissions from its users, which are described in Table 6.4. Note that many of the permissions identified are likely necessary for the functioning of the application: for example, an application that allows for video calling with doctors will require access to the camera, while one that allows for locating the nearest pharmacy will require access to GPS location. However, in some cases these permissions may not be required for normal functioning of the application. Additionally, it is always relevant to consider how applications requesting permissions such as these handle sensitive user data. Users may not be aware of the amount of data an mHealth application may be able to collect or how that data is being protected, so it is important to ensure that data protection laws are in place to promote good practices and user trust.

Per.	Permission	Description
58	ACCESS_COARSE_LOCATION	coarse (network-based) location
69	ACCESS_FINE_LOCATION	fine (GPS) location
15	ACTIVITY_RECOGNITION	allow application to recognize physical activity
8	AUTHENTICATE_ACCOUNTS	act as an account authenticator
53	CALL_PHONE	directly call phone numbers
77	CAMERA	take pictures and videos
38	GET_ACCOUNTS	list accounts
8	GET_TASKS	retrieve running applications
15	READ_CALENDAR	read calendar events
15	READ_CONTACTS	read contact data
85	READ_EXTERNAL_STORAGE	read external storage contents
54	READ_PHONE_STATE	read phone state and identity
69	RECORD_AUDIO	record audio
23	SYSTEM_ALERT_WINDOW	display system-level alerts
8	USE_CREDENTIALS	use the authentication credentials of an account
23	WRITE_CALENDAR	add or modify calendar events and send emails to guests
8	WRITE_CONTACTS	write contact data
85	WRITE_EXTERNAL_STORAGE	read/modify/delete external storage contents

Table 6.4: Sample of permissions requested by the 13 analyzed mHealth applications, as described by the Mobile Security Framework [121]. While many of these permissions are likely required by the application, some may be unnecessary, and it is important to consider how the application is protecting the potentially sensitive data it collects.

Finally, privacy policies listed on the Google Play Store pages for these applications were sometimes seen to be insufficient. Three of the 13 applications had links to policies that resulted in a 404 error, and one had a link that (at the time of writing) gave a security warning due to an expired SSL certificate. Additionally,

while many applications had relatively long and detailed privacy policies, others had only one or two paragraphs describing the applications' data collection activities in vague terms. Oddly, one privacy policy focused almost entirely on the user's use of the application's graphics or logos rather than the applications' use of the user's personal data.

All told, this reflects a similarity with the results of the security analysis by Papageorgiou et. al., indicating that mobile application developers can often fall victim to common security pitfalls, even when working in areas where the protection of personal data is vital. However, in many cases there are "easy wins" here, in which issues can be resolved or mitigated without excessive cost or time to benefit application users. We will discuss these further in Section 6.5.

6.5 Security Controls

For the same reason that mHealth and telehealth programs and technologies are more accessible to countries with developing healthcare systems, they can also be harder to regulate. Individual nonprofits, businesses, and healthcare clinics can operate these technologies outside of a national healthcare structure, potentially allowing more individuals to access medical care but also raising the risk of insufficient considerations of security and privacy. As such, it is important to have data protection legislation in place that is applicable to organizations running these programs. This legislation should cover the principles discussed in Section 5.5, from appropriate data collection to the right of access to the requirement to notify victims of data breaches.

Additionally, states should publish clear guidelines and/or regulations for mHealth and telehealth programs. These could be similar to India's Telemedicine Practice Guidelines, but they should point developers and organizations toward clear security and privacy requirements based on existing standards and the need to preserve the

confidentiality, integrity, and availability of data.

Security controls for healthcare professionals and organizations will likely depend on the technology in use: an SMS-based service, a mobile application, and a website will all have different security needs. However, all of these will require strong privacy policies that are easily located and understood by users. Additionally, organizations will need to maintain a firm commitment to the secure collection and storage of users' data. Mobile application developers should also make clear which permissions they're requesting from users and why these are necessary for the functioning of their application.

When developing a mobile or web application, it is critical to consider existing standards and guidelines such as the Open Web Application Security Project's (OWASP) Secure Coding Practices, Web Security Testing Guide, and Mobile Security Testing Guide [124, 125, 122]. These discuss strong cryptographic configurations, appropriate logging techniques, secure coding practices, and tools and methods for testing. At a basic level, all communications should be encrypted using well-established algorithms and protocols, the application should not leak data in ways that may be accessed by malicious applications, and developers should be aware of common vulnerabilities, such as SQL injection, and ways to defend against them, such as input sanitization and prepared queries. Following these guidelines and verifying security as part of the development cycle (both through internal audits and external testing) is a crucial step towards protecting against attacks.

Finally, we should consider clinics selecting existing technologies, such as video conferencing platforms, in order to consult patients remotely. In these cases, it is important to ensure that the tool selected is compliant with any relevant legislation and follows the best practices described above: strong privacy policies, encrypted communications, and secure coding standards.

A summary of these controls is available in Table 6.5.

Security Control	Description
Applicable Privacy Laws	Ensure that strong data protection legislation exists and is applicable to mHealth and telehealth technologies.
Applicable Guidelines	Ensure that guidelines, standards, and/or regulations exist that cover minimum security and privacy standards for mHealth and telehealth programs operating in the country.
Privacy Policies	mHealth and telehealth applications, technologies, and programs should have strong and clear privacy policies with a commitment to good data collection and storage practices.
Secure Development Practices	Developers should follow existing guidelines and standards to ensure that they adhere to best practices in cryptography, secure coding, and the management of sensitive information. Regular testing should be conducted for verification of these efforts.
Technology Vetting	Clinics should ensure that any third-party technologies used for remote health practices follow the above standards.

Table 6.5: Security controls for mHealth and telehealth programs, as identified by analysis of the literature and a case study.

6.6 Conclusion

In this chapter, we have discussed the disparate topic of mHealth and telehealth as a mechanism of ensuring that healthcare is more accessible to individuals who live in remote areas or have otherwise limited access to in-person consultation and treatment. The nature of these technologies means that they can scale from trial programs run by a nonprofit to mobile applications used by doctors in a handful of clinics to nationally supervised efforts governed by strict legislation. This means that it can be difficult to define an overarching strategy, but that national guidelines and data protection legislation can be important for ensuring that a minimum commitment to security and privacy is maintained. Additionally, there are a number of

ways in which developers can build security into applications without overspending on time or resources. While in some cases tradeoffs may exist between security and access, there are a number of "quick wins" organizations can score in order to ensure the safety of users' data while providing a high standard of care: strong privacy policies, attention to secure coding and cryptographic practices, and an avoidance of data leakage.

In the next chapter, we will combine the governance and technical lessons we have learned from examining national eHealth policies, eHealth legal frameworks, and mHealth and telehealth programs in order to discuss electronic health records.

Chapter 7

Electronic Health Records

7.1 Introduction

In this chapter, we will explore the security of electronic health records (EHRs). The WHO defines EHRs as "real-time, patient-centred records that provide immediate and secure information to authorized users...[and] typically contain a patient's medical history, diagnoses and treatment, medications, allergies, immunizations, as well as radiology images and laboratory results" [11, p. 94]. As with the chapters above, we will consider the literature relating to their security, explore available data, examine the EHR systems of two countries as a case study, and conclude with a list of relevant security controls for EHR systems.

7.2 Literature

The WHO argues that EHRs "can play a pivotal role in [universal health coverage] by providing insight into health care costs, utilization and outcomes, promoting quality of care, reducing costs, supporting patient mobility, increasing reliability of information and providing access to patient information to multiple health care providers" [11, p. 94]. As such, EHRs are a significant player in the achievement of the third Sustainable Development Goal - and ensuring their confidentiality, in-

tegrity, and availability is critical to guaranteeing a high standard of care and protecting patients.

The wealth of information available in EHRs makes them popular targets of hacking and data theft. In the first ten months of 2020, 513 healthcare organizations reported a breach of 500 or more patient records to the US Department of Health and Human Services Office for Civil Rights - an increase in reports over the entire year of 2019 [126]. These attacks create significant threats to patient privacy, while the increase in ransomware attacks on hospitals threatens the availability of patient records when medical professionals require them to make critical treatment decisions.

Additionally, popular EHR systems can be affected by vulnerablities and insecure configurations. Static code analyses conducted on the OpenEMR and OpenClinic EHR applications in 2018 and 2019 identified a number of vulnerabilities, including file inclusion, cross-site scripting, and SQL injection [127, 128]. A similar security review of OpenEMR in 2019 found additional vulnerabilities, including remote code execution [129].

Security concerns over EHRs may be a barrier to their use. A 2012 paper interviewing 32 community behavioral health providers on their willingness to use EHRs found that all worried about the privacy and security of EHR technologies, and a third believed that their patients would have concerns as well [130]. However, seven providers also noted that EHRs may bring with them security improvements over pen-and-paper systems: said one consultant, "I call Walgreens and I say, "I'm an RN from this hospital, and I need to verify John Smith's meds." Well, Walgreens doesn't know who I am, [yet they provide patient information over the telephone]" [130, p. 251]. EHRs may offer additional formality and patient privacy protection to the process of administering medical care without increasing barriers of access.

Recently, encrypted cloud storage with fine-grained access control and authentication via single sign-on has gained attention as a way of ensuring the accessibility of EHRs without compromising their security [131, 132, 133]. However, the

most basic needs of EHR security are relatively simple: a 2015 literature review identified a number of common security controls important to EHR applications, including access control, cryptography and digital signatures, continuity planning, monitoring and auditing techniques, and compliance with relevant standards and legislation [134]. The review addressed the relevance of regulations to ensuring each aspect of EHR security, reinforcing the need for appropriate legal frameworks as discussed in Chapter 5. The review also found that while issues such as encryption and signing were well addressed, issues such as "documented operating procedures, controls against malwares, technical vulnerability management, control of operational software, and checks and updates" were less discussed despite their importance [134, p. 29]. As elsewhere, the security of EHRs depends not only on controls implemented once but also strong policies and procedures followed over time.

In the next section, we will explore the adoption of EHRs in the data offered by the WHO eHealth survey.

7.3 Data

The 2015 WHO eHealth survey asks a number of questions about EHRs: whether the responding country has a national EHR system, whether that country has applicable laws governing said EHR system, and which types and rough percentages of health facilities (primary, secondary, and tertiary) use EHRs [51]. Roughly 46% of respondents reported having to have a national EHR system, of which 54% claimed to have applicable legislation. The importance of such legislation is discussed in Chapter 5: it aids in establishing security and privacy requirements to ensure the protection of valuable personal medical data. Where EHRs existed, they were generally widely used: 89% of countries with a national EHR system used them in at least some primary care contexts (e.g., clinics), 91% used them in at least some secondary care contexts (e.g., hospitals), and 86% used them in at least some ter-

tiary care contexts (e.g., specialists). However, there is clearly a barrier to fully implementing EHRs even in countries with well-developed healthcare systems: only eight countries (out of 125 respondents and 57 with national EHR systems) reported using EHRs in over 75% of primary, secondary, and tertiary care facilities.

Once again, the survey does not specifically ask about security: it is more focused on coverage. However, it is likely that, for most countries, legislation governing the use of EHRs addresses at least basic security considerations such as data confidentiality and integrity. EHRs also occupy a special space for an eHealth technology: in our data analysis in Chapter 3, we saw that the EHR category correlated must more strongly with the foundations and legal frameworks categories than with the more technical categories. This may be because of the complexity of establishing a national eHealth system, which is significantly greater and requires a stronger governance posture than, for example, creating informal mHealth or telehealth programs. However, there are still a variety of complex factors involved in the creation of a national eHealth system, and some "leapfrogging" may still be possible.

Table 7.1 displays the Pearson's correlation coefficients between the presence of a national EHR system and a country's GCI score, wealth, and connectivity. The symbols ***, **, and * next to the coefficients indicate significance levels of below 0.001, 0.01, and 0.05, respectively.

	EHRs	**GCI**	**Wealth**	**Connectivity**
EHRs	1.0***	-	-	-
GCI	0.153	1.0***	-	-
Wealth	0.251**	0.493***	1.0***	-
Connectivity	0.235**	0.572***	0.905***	1.0***

Table 7.1: Pearson's correlation coefficients of the existence of a national EHR program, the GCI score, the natural log of the GDP per capita, and the percentage of Internet users (all in 2015).

The table shows that there is only a small statistically significant correlation between the presence of a national EHR system and wealth and connectivity, and

no statistically significant correlation between the presence of a national EHR system and a country's GCI score. This is represented visually in the scatterplot in Figure 7.1.

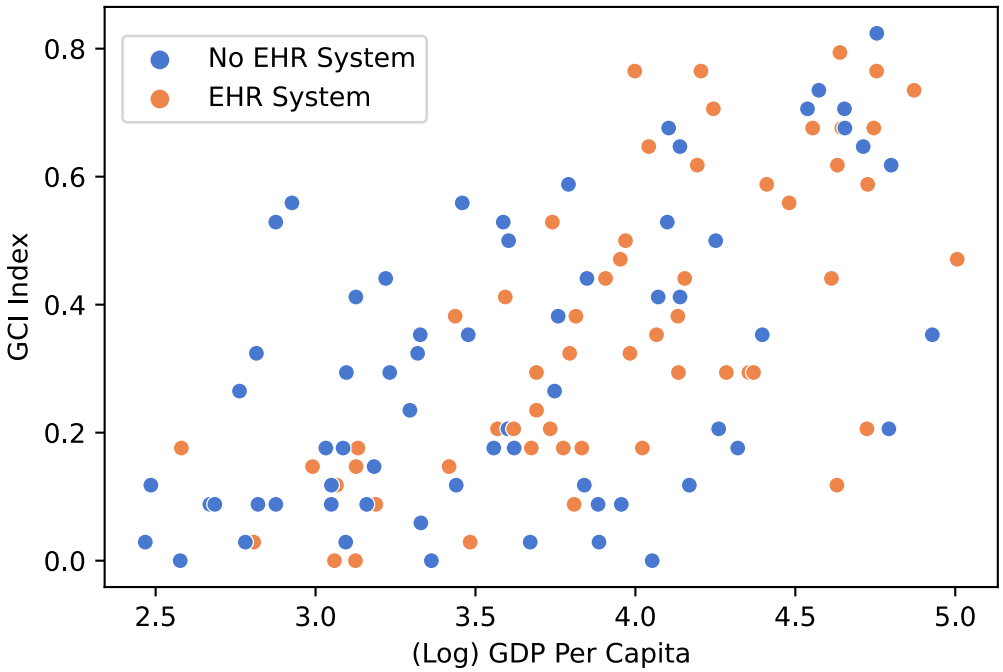

Figure 7.1: Scatterplot of the GCI score versus the natural log of GDP per capita, broken down by the existence of national EHR systems. These charts show that national EHR systems occur at all levels of GDP per capita and GCI scores.

While national EHR systems do appear to be slightly more common at higher levels of GDP per capita, this is not consistent behavior, and there seems to be very little relationship to the GCI score. This could be because building EHR systems into any healthcare system is a complex and resource-intensive endeavor, even for high-income countries, but low-income countries may benefit from incorporating EHRs as they develop more comprehensive digital healthcare systems rather than including them "after the fact."

It is not clear from the survey results what EHR technologies are in use: it is possible that countries with national EHR systems and low GCI scores are using well-tested options with built-in security controls. Yet it is still important to maintain strong security policies and procedures in order to maintain confidentiality, integrity,

and availability over time. In the next section, we will explore this idea further via a case study.

7.4 Case Study

In order to better understand the relationship of EHRs to legislation, security, and privacy concerns, we will examine two case studies of countries which have tried to implement EHR systems at a national level: Australia and Uruguay. Details about these countries are shown in Table 7.2. As above, note that the scale of the GCI rankings has changed between 2015 and 2020; however, it is still possible to see that both countries have increased their rankings over the five-year period. Uruguay has made significant progress in the area of capacity development, whereas Australia has improved most in the area of cooperation.

Country	**Pop. (1000s)**	**GDP Per Capita**	**GCI 2015**	**GCI 2020**
Australia	25,687.04	51,812.2	0.765	97.47
Uruguay	3,473.73	15,438.4	0.618	75.78

Table 7.2: Comparisons of countries in the EHRs case study [55, 54, 27]

Since 1984 Australia has offered Medicare as its public health care option, covering the cost of public hospital visits and some or all of the cost of other health services for Australian citizens and permanent residents [135]. Private health insurance is also available [135]. The federal government oversees Medicare and handles the broad direction of health in Australia; state, territory, and local governments manage the public hospitals in their jurisdiction [135].

Australia established the National E-Health Transition Authority (NEHTA) in 2005 with the mandate of shepherding the country's conversion to a more digitized and interoperable health sector [136]. Three years later, Australia published its National E-Health Strategy, which explored the foundational steps necessary for

implementing a national electronic medical record system - specifically, beginning with an "incremental and distributed" approach that focused on encouraging information sharing among health care providers [137, 136]. Finally, in 2012, Australia passed the Personally Controlled Electronic Health Record Act (now the My Health Records Act), which established the beginnings of its national EHR system [138, 136]. The Act makes specific reference to Australia's 1988 Privacy Act as applicable to organizations which handle EHRs; it also makes these organizations responsible for disclosing any security breaches to affected individuals [138]. While it does not mention any specific required security controls, it does give ministers the ability to create Rules related to "physical and information security" (as well as other topics) [138].

Since 2012, Personally Controlled Electronic Health Records have been renamed to My Health Records, the opt-in system was changed to an opt-out system, and a number of Rules have been passed [136, 139]. The 2016 My Health Records Rule is the greatest source of security requirements, dealing with access control, identity verification, and account management for both healthcare providers and portal operators [140]. Additionally, in 2018 the My Health Records Act was amended to strengthen privacy protections by providing for the secure destruction of data and expanding prohibited usages of health information [141].

As of April 2020, around 23 million of 25.5 million Australians had a MyHealth record; however, only 13.6 million records actually contained any data [142, 143]. 2.5 million individuals opted out of the system entirely [143]. Additionally, while the government allows users to allow or prevent healthcare organizations from viewing their records, place extra restrictions on particularly sensitive documents, or receive notifications when their records are accessed, only a small percentage of users appear to be employing these options [144, 145].

While much of the uptake issue is likely explainable by the difficulties of incorporating complex new technologies into the health sector, security and privacy

concerns appear to have played a role. A review by the Australian National Audit office (ANAO) identified a number of positives in the system, including that the Australian Digital Health Agency (ADHA) "managed risks to the core infrastructure through: establishing a Digital Health Cyber Security Centre; undertaking a series of dedicated cyber security assessments; and implementing the 'Essential Eight' cyber security mitigation strategies and decreasing the number of Information Security Manual (ISM) cyber security controls not implemented" [146]. However, the ANAO added that the ADHA had failed to develop sufficient strategies for managing third-party software and compliance requirements, as well as exhaustively consider the privacy implications of emergency health data access allowances [146]. The report addresses the still-too-high threat of unauthorized access to patient records, offering four recommendations related to risk management - from conducting additional privacy assessments to developing security frameworks for vendor software to completing regular compliance reports [146].

Concerns over these issues have led to a number of criticisms of the program, even thinkpieces and organizations recommending that individuals opt out [147, 148]. This shows how important buy-in from both patients and medical professionals is to successfully launching new eHealth programs - and how security and privacy concerns can hinder this buy-in. However, it is possible that continuing to address the My Health Record's security and privacy shortcomings, as well as growing ease of use for individuals and healthcare providers, will help to increase the integration of the technology into the Australian healthcare system.

Like Australia, Uruguay offers both a private and a public healthcare option. The private option consists of *mutualistas*, in which individuals pay for membership in a hospital's comprehensive healthcare plan; the public option is run by the Administración de Servicios de Salud del Estado (ASSE) and operates similarly to a *multualista* except that coverage is free for low-income citizens and residents [149, 150]. Both fall under the umbrella of the Sistema Nacional Integrado de Salud

(SNIS) [149].

Like Australia's NEHTA, the Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento's (AGESIC) Salud.uy program aims to integrate ICT into the Uruguayan healthcare sector [151, 152]. One of the most important aspects of the program is the Historia Clínica Electrónica Nacional (HCEN), Uruguay's national EHR system [153]. The goal of the program is to allow secure data exchange between health providers via the Plataforma de Historia Clínica Electrónica Nacional [153].

In 2008, Law no. 18,335, "Rights and Obligations of Patients and Users of Health Services," first established the right of patients to have a complete written or electronic history of a patient's health, which they can access or revise at will [154]. This right was refined ten years later in Article 194 of Law no. 19,670, which instructed all health service providers to incorporate HCEN (and gave users the right to opt out of the system if they so chose) [155]. Article 194 also required that health service providers comply with 2008's Law no. 18,331, which governs personal data protection, in their handling of HCEN [155, 156]. Additional legislation has further refined these requirements. 2019's Decree no. 122/019 describes the data required to exist in the record and grants users the right to manage access permissions to their data (similar to the Australian case) [157]. 2017's Decree no. 242/017 establishes the importance of maintaining confidentiality and requires health institutions to appropriately log access to health records [158]. It also makes reference to 2009's Law no. 18,600, which handles requirements for secure digital signatures [158, 159]. Finally, it offers the government further power to define security requirements for health providers [158].

These security requirements exist in the form of the Marco de Ciberseguridad, developed by AGESIC. The Marco de Ciberseguridad is a thorough security reference guide for organizations in all sectors that makes reference to internationally recognized standards (such as ISO 27001 and the NIST security framework) and offers

advice on best practices [160, 161]. Asset management, access control, monitoring, incident response, and continuity planning are all covered in the document [160]. Additionally, the implementation guide, which details how certain sectors should implement the requirements of the Marco de Ciberseguridad, offers specific guidance for healthcare organizations and HCEN infrastructure [162].

Interestingly, uptake to the Uruguayan HCEN appears to be stronger than for the Australian My Health Record: whereas half of My Health Records appeared to be empty as of April 2020, the Uruguayan government claims that 92% of citizens' HCENs contain at least one document [143, 163]. This is paired with a much more neutral-to-positive response to the launch of HCEN in Uruguay. Negative articles on the development were difficult to find, and the most critical one (a thinkpiece by a Uruguayan pediatrician) focused primarily on the failures of other countries at implementing EHRs than on specific complaints about Uruguay's attempt [164]. While the author was clearly concerned about the privacy of his health data - he noted (in Spanish), "I'm afraid that my security is compromised" - a response piece published one month later expressed only confidence in the technology and in the power of Uruguay's data protection laws [165, 164].

The difference in public perception (and, apparently, uptake) of the EHR systems in Australia and Uruguay is interesting, though it is unclear whether this represents disparities in attitudes towards privacy and security, disparities in confidence about legal and technical protections for personal data, or some other distinction in public sentiments towards government handling of the programs. However, it is clear from these case studies that concerns about privacy and security can affect individual opinions of EHRs or decisions about whether to use them. It is therefore imperative that countries establishing national EHR systems do so with appropriate legal frameworks and regulations guarding patient data, thereby helping to inspire confidence and gain the most benefits to national health. Important security controls for this endeavor are discussed in Section 7.5.

7.5 Security Controls

When it comes to the security of EHRs, a crucial component appears to be public perception: the individuals using the system, whether patients or healthcare professionals, should have confidence in the safety and privacy of their data. As such, national EHR systems should be designed based on consultations with stakeholders and security experts, and regular testing should be conducted to ensure compliance with expectations and requirements.

First, it is important to ensure that strong data protection legislation exists (see Chapter 5 for more details) and is applicable to EHRs. Users should, at minimum, have the right to access and correct their records. Providers should be obligated to report breaches and to store data securely. Legislation establishing EHRs should make these rights and responsibilities clear and should create a precedent of consent by offering users the ability to opt out of the program.

As seen in both the Australian and the Uruguayan model, users should be permitted to define fine-grained restrictions on access to their own data. However, it is critical to ensure that users are aware of this ability and how to use it. If controlling access to one's record is too complex or confusing, particularly for users who are not highly familiar with technology, the existence of these controls will offer little benefit.

On the provider side, it is critical to define security controls spanning the entire threat lifecycle, consisting of - as defined by the US National Institute of Standards and Technology (NIST) - identification, protection, detection, response, and recovery [166].

In the context of EHRs, identification of assets, context, and risk requires a strong understanding of the EHR platform(s) and the third-party vendors and software upon which its(their) implementation relies. This must go deeper than a surface level. For example, the open source OpenEMR platform uses a variety of embedded components and third-party libraries, including old versions of jQuery and an

access control library called PHPGacl that has not been updated since 2006 [167, 168]. Any risk assessment of using OpenEMR (or any other EHR system) would be incomplete without acknowledging its dependencies. Additionally, it is important to keep in mind the healthcare professionals that would use this system and any security shortcuts they may be inclined take due to lack of time or understanding. This facilitates the development of additional controls as well as the identification of compromises between ease of use and security. For example, the UK National Cyber Security Centre (NCSC) now recommends against enforcing regular password changes by default due to the tendency of users to only mildly alter their password (for example, by incrementing a number) and instead encourages strong account lockout and monitoring techniques [169]. The results of this process of contextualizing and assessing the EHR software will allow for a better understanding of what security controls to enforce and where to direct monitoring efforts. However, it is critical that this step should not be completed once: the risk assessment resulting from the identification process should be re-evaluated as the EHR software and the threat landscape changes.

Protection concerns the defense against attack: attempting to ensure that an attacker does not gain unauthorized access to data or systems. It is discussed in detail in the context of EHRs by Rezaeibagha et. al., including a consideration of authentication, access control models, communications protocols, and secure storage [134]. What is most critical here is not so much which choices to make - this will likely depend on the results of the identification process - but that choices are based on well-established standards such as those defined by Health Level 7 and ISO/IEC 27002 [134]. In some cases, protections may be defined based on earlier laws and regulations, such as Uruguay's requirements for digital signatures. Security training for healthcare professionals should also fall under this category.

When protection fails, detecting and responding to attacks becomes critical. In the case of EHRs, logging access to records is important for identifying unusual be-

havior. Individuals should be able to see this log as well, and there should be a clear point of contact for reporting discrepancies. This auditing is also useful for sorting out non-security related bugs with the system. The Australian Digital Health Agency's annual report for 2018-2019 states that 38 security incidents related to My Health Records were reported to the Office of the Australian Information Commissioner during that year; however, due to good auditing processes they discovered that most of these events were caused by administrative errors rather than malicious behavior [170]. The next year, only 2 incidents were reported, indicating that the system was running more smoothly [171]. Additionally, monitoring should be enabled on the EHR system infrastructure to better detect unusual activities and conduct post-incident analysis.

Finally, resilience is an important characteristic for recovering from attacks. Secure backups should be taken, restore tests should be conducted, and continuity plans should be created to ensure that availability is quickly restored following an incident and healthcare organizations are able to operate in the meantime. The distributed nature of cloud computing is also a potential advantage, making it less likely for a system facing a high volume of traffic to become overloaded [134].

Finally, regular tests and audits should be conducted to identify any issues and ensure the system's ongoing security. Once issues are resolved, the resulting reports should be made available to the public to facilitate transparency and trust.

A summary of these controls is available in Table 7.3.

7.6 Conclusion

In this chapter, we have established that a national EHR system is a complex undertaking because it combines the legislative, policy, and technical aspects of eHealth discussed in prior chapters. While it may be possible for developing countries to "leapfrog" over early stages by studying existing implementations and standards,

Security Control	Description
Applicable Privacy Laws	Ensure that strong data protection legislation exists and is applicable to EHRs.
User-Defined Access Controls	Allow users to define restrictions on their own records or on certain documents. Ensure that users are aware of this ability and how to use it.
Identify Context	Conduct a risk assessment of the EHR software and the way(s) it will be used to inform future security controls, as well as directions for monitoring efforts
Define Protections	Create protections based on existing standards to guarantee the confidentiality, integrity, and availability or records and ensure that all users accessing them are authenticated and authorized.
Detect & Respond to Attacks	Employ logging and monitoring techniques to identify unauthorized access to users' records or to the EHR system infrastructure.
Ensure Resilience	Ensure that availability is maintained in case of an incident due to regular backups, distributed storage, and continuity planning.
Testing	Test and audit the EHR system on a regular basis to identify issues and guarantee security and privacy.

Table 7.3: Security controls for EHRs, as identified by analysis of the literature and a case study.

success in this area still requires strong governance and technical capacity. Additionally, this is one of the areas of eHealth in which security is most critical, as medical records contain extremely sensitive information valuable to malicious actors. Concerns about security and privacy may affect the uptake of EHRs and thereby reduce their benefits. However, attempting to establish a national EHR system is still an important goal for many countries wishing to provide a better standard of care for their populations. Over time, we will likely see even more national EHR systems building off of one another and evolving over time.

In the conclusion, we will discuss our findings so far and make recommendations for next steps and future work.

Chapter 8

Conclusion

8.1 Reflections and Next Steps

Throughout this thesis, we have seen that eHealth systems are composed of a variety of components, each with their own unique security needs. We have also seen that while cybersecurity maturity often lags behind eHealth development, it is often possible to build reasonable security measures into eHealth systems fairly quickly and without sacrificing other goals, such as increased access to care.

One of the most significant limitations of this thesis has been the lack of current data. The WHO has not completed an eHealth survey since 2015. Since that year there have been significant advancements in eHealth governance and programs in many countries, as discussed in our case studies. A new survey with up-to-date information on current practices may reveal new connections between eHealth maturity and other national factors, such as GDP per capita and Internet use.

Additionally, there is insufficient data specifically related to the privacy and security of digital health programs around the world. The WHO survey asked about the existence of various eHealth policies, legislation, and programs, but gathered specific details only about health data privacy laws. This makes it difficult to discern the maturity of and commitment to the measures in question for more fine-grained

analysis. In Table 8.1, we suggest new questions related to security and privacy consideration in each survey category that may be offer useful insights in a future survey.

Generally speaking, these questions are derived from the security controls present in Chapters 4, 5, 6, and 7. They primarily concern national governance: the existence of various laws, standards, and frameworks surrounding eHealth security and privacy, as well as agencies responsible for maintaining the confidentiality, integrity, and availability of patient information and digital healthcare systems. Collecting additional data about the state of security in eHealth could enable further quantitative analysis about existing practices and their determinants. Collecting answers to these questions over a period of time will also help to determine the existence of a "security gap" that is closed as countries become more wealthy and develop more mature eHealth systems, or whether building security considerations into developing healthcare systems is becoming more common as best practices evolve.

Additionally, it is relevant to further determine and quantify the ways in which public concerns about security and privacy intersect with movements to incorporate ICT into eHealth systems, and the roles that existing legal protections play in shaping these perceptions. This can be accomplished through additional surveys of healthcare providers and individuals in a variety of countries about a variety of programs (e.g., mHealth, telehealth, and EHRs) in order to gather a better understanding of attitudes towards and concerns about security and privacy in disparate contexts. Uptake and adoption are crucial considerations when expanding access to care, and security protections can influence individual decisions about the use of eHealth technologies. Understanding the requirements of both patients and providers will help to maximize the benefits of ICT integration in eHealth.

Finally, further security testing and privacy reviews of mHealth applications, open source EHR systems, and other publicly available eHealth technologies can help to identify vulnerabilities and non-optimal practices whose resolution can offer

Category	**Question**
Foundations	Does the national eHealth strategy identify relevant security threats to the country's (digital) health sector?
Foundations	Does the national eHealth strategy identify existing laws and standards for ensuring the security and privacy of patient data?
Foundations	Does the national eHealth strategy appoint parties responsible for creating standards for or maintaining eHealth security?
Foundations	Does the national eHealth policy or strategy define realistic and measurable goals for enhancing eHealth security and privacy?
Legal Frameworks	Is there legislation outlawing computer-dependent crimes applicable to patient data and digital healthcare systems?
Legal Frameworks	Are there government standards, frameworks, and/or legislation addressing the security of electronically stored patient data and eHealth technologies?
mHealth & Telehealth	Is there data privacy legislation applicable to mHealth and telehealth programs?
mHealth & Telehealth	Are there clear, specific government data security guidelines applicable to mHealth and telehealth programs?
EHRs	Is there data privacy legislation applicable to EHRs?
EHRs	Do patients have a right to access and correct their EHRs?
EHRs	Do patients have a right to restrict access to their EHRs?
EHRs	Is there an agency responsible for national EHR security?
EHRs	Is there legislation or a national standard governing specific security controls for the national EHR system?
eLearning	Are relevant laws and best practices for maintaining the security and privacy of patient data and healthcare systems part of the remote learning curriculum for healthcare professionals?
Social Media	Does the national social media strategy govern controls for maintaining the privacy of potentially sensitive data?
Big Data	Does the national policy or strategy governing the use of big data in the health sector consider the security and privacy of patient data, including anonymization and pseudonymization?

Table 8.1: Recommended questions to include in a future survey on eHealth security, such as the next WHO eHealth survey, based on the findings of this thesis.

additional assurances of data confidentiality and integrity. This is especially important when these technologies are used in contexts in which legislation is insufficient to enforce proper data security and protection standards.

With the help of the additional data discussed above, a strong next step for this thesis would be to adapt the proposed security controls into a framework for evaluating the security of eHealth systems at different stages of maturity. We have recommended in Sections 4.5, 5.5, 6.5, and 7.5 measures related to governance (e.g., strong policy commitments, national security guidelines, and responsible agencies), legislation (e.g., cybercrime, compliance, and data protection laws), technical capacity (e.g., secure development, situational awareness, and threat management), and education (e.g., healthcare provider training and user/patient understanding). However, in addition to the dimensions of the framework, it is important to consider the scale: where a country's eHealth-cybersecurity capacity is at a given time, based on relevant indicators, from non-existent to mature. Importantly, a "one-size-fits-all" approach to scale won't work: an effective framework would need to evaluate the relationship of security to the technologies and programs in place, rather than the technologies and programs themselves. As a country expands their eHealth systems, their eHealth-cybersecurity capacity must be re-evaluated, and the country may move *down* the scale if security is not properly considered as part of this expansion. The complexity of this process likely means that such a framework would require expert analysis and multi-stakeholder reviews based on primary sources, along the lines of the Cybersecurity Capacity Maturity Model (CMM) discussed in Section 2.4.

8.2 In Sum

Throughout this thesis, we have offered evidence that, while security progress can lag behind eHealth progress, many countries are tackling these goals simultaneously by

building security into developing eHealth systems - whether by considering security threats in national eHealth policies, introducing privacy and security legislation applicable to eHealth, outlining best practice guidelines for mHealth and telehealth programs, or establishing privacy and security requirements for electronic health records.

In Chapter 2, we laid the foundation for this thesis by examining the relationships between the Sustainable Development Goals (SDGs) to ICT and, by extension, to security. We discussed the case of eHealth specifically and found that, which healthcare security is a popular topic of research, less attention is paid to developing healthcare systems despite evidence that security and privacy concerns may decrease trust and affect uptake.

In Chapter 3, we identified a potential "security gap," in which countries may mature their eHealth systems before developing a strong cybersecurity posture. However, we also found that many countries do consider both eHealth and cybersecurity to be important areas for investment and growth. We considered the possibility of "leapfrogging" the gap by building security into a healthcare system as it grows.

In Chapters 4 through 7, we examined this possibility through the lens of different areas of eHealth: national policies and strategies, legislation, mHealth and telehealth programs, and electronic health records. We saw that while security gaps exist, it is possible to consider security alongside eHealth development to exploit its benefits to availability, trust, and the protection of sensitive data.

Security does not have to work in opposition to the third SDG: in fact, it can work for it. As countries build ICT into their health systems, considering security from a governance and technical perspective can help to assure the benefits of increased access to care. Over time, this can support the development of robust and resilient healthcare systems that have earned patient trust by preserving their privacy and ensuring the availability of the health technologies they use.

Bibliography

[1] United Nations. *THE 17 GOALS — Sustainable Development*. United Nations Department of Economic and Social Affairs Sustainable Development. URL: https://sdgs.un.org/goals (visited on 04/19/2021).

[2] Robert Morgus. *Securing Digital Dividends: Mainstreaming Cybersecurity in International Development*. Washington, D.C., USA: New America, 2018. URL: http://newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends (visited on 04/19/2021).

[3] United Nations. *2030 Agenda for Sustainable Development*. 2015. URL: https://sdgs.un.org/sites/default/files/publications/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf.

[4] United Nations. *United Nations Millennium Development Goals*. URL: https://www.un.org/millenniumgoals/bkgd.shtml (visited on 05/04/2021).

[5] A. Min Tjoa and Simon Tjoa. "The Role of ICT to Achieve the UN Sustainable Development Goals (SDG)". In: *ICT for Promoting Human Development and Protecting the Environment*. Ed. by Francisco J. Mata and Ana Pont. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2016, pp. 3–13. ISBN: 978-3-319-44447-5. DOI: 10.1007/978-3-319-44447-5_1.

[6] T. Ono, K. Iida, and S. Yamazaki. "Achieving Sustainable Development Goals (SDGs) through ICT Services". In: *Fujitsu Scientific and Technical Journal* 53 (Oct. 1, 2017), pp. 17–22.

[7] Jinsong Wu et al. "Information and Communications Technologies for Sustainable Development Goals: State-of-the-Art, Needs and Perspectives". In: *IEEE Communications Surveys Tutorials* 20.3 (Mar. 2018), pp. 2389–2406. ISSN: 1553-877X. DOI: 10.1109/COMST.2018.2812301.

[8] Jeffery D. Sachs et al. *ICT & SDGs: How Information and Communications Technology Can Accelerate Action on the Sustainable Development Goals*. The Earth Institute, Columbia University and Ericsson, 2016. URL: https://www.ericsson.com/assets/local/news/2016/05/ict-sdg.pdf.

[9] Olivera Kostoska and Ljupco Kocarev. "A Novel ICT Framework for Sustainable Development Goals". In: *Sustainability* 11.7 (7 Jan. 2019), p. 1961. DOI: 10.3390/su11071961. URL: https://www.mdpi.com/2071-1050/11/7/1961 (visited on 04/27/2021).

[10] World Health Organization. *WHA58.28*. 2005. URL: https://www.who.int/healthacademy/media/WHA58-28-en.pdf.

[11] World Health Organization. *Global Diffusion of eHealth: Making Universal Health Coverage Achievable*. Report of the third global survey on eHealth. Geneva, Switzerland: World Health Organization, 2016. URL: https://www.who.int/goe/publications/global_diffusion/en.

[12] World Health Organization. *eHealth and Innovation in Women's and Children's Health: A Baseline Review*. Mar. 2, 2014. URL: https://www.who.int/publications/i/item/9789241564724 (visited on 06/24/2021).

[13] Thomas Niebel. "ICT and Economic Growth – Comparing Developing, Emerging and Developed Countries". In: *World Development* 104 (Apr. 1, 2018), pp. 197–211. ISSN: 0305-750X. DOI: 10.1016/j.worlddev.2017.11.

024. URL: https://www.sciencedirect.com/science/article/pii/S0305750X17303868 (visited on 05/07/2021).

[14] International Telecommunication Union. *Fast Forward Progress: Leveraging Tech to Achieve the Global Goals*. 2017. URL: https://www.itu.int/en/sustainable-world/Pages/report-hlpf-2017.aspx.

[15] Niina Maarit Novak and A. Min Tjoa. "ICT as an Enabler for a Society Where No One Is Left Behind". In: *Proceedings of the 20th International Conference on Information Integration and Web-Based Applications & Services*. iiWAS2018. New York, NY, USA: Association for Computing Machinery, Nov. 19, 2018, pp. 3–7. ISBN: 978-1-4503-6479-9. DOI: 10.1145/3282373.3282381. URL: https://doi.org/10.1145/3282373.3282381 (visited on 05/07/2021).

[16] Katina Michael et al. "Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals". In: *2019 IEEE International Symposium on Technology and Society (ISTAS)*. 2019 IEEE International Symposium on Technology and Society (ISTAS). Medford, MA, USA: IEEE, Nov. 2019. DOI: 10.1109/ISTAS48451.2019.8937956.

[17] Joshua Davis. "Hackers Take Down the Most Wired Country in Europe". In: *Wired* (Aug. 21, 2007). ISSN: 1059-1028. URL: https://www.wired.com/2007/08/ff-estonia (visited on 04/28/2021).

[18] US Cybersecurity and Infrasture Security Agency. *Cyber-Attack Against Ukrainian Critical Infrastructure*. 2016. URL: https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01 (visited on 04/28/2021).

[19] William Smart. *Lessons Learned Review of the WannaCry Ransomware Cyber Attack*. Feb. 2018. URL: https://www.england.nhs.uk/wp-content/

uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.

[20] Brencil Kaimba. *Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line*. Nairobi, Kenya: Serianu, 2017. URL: https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf.

[21] World Bank. *World Development Report 2016: Digital Dividends*. Washington, D.C.: World Bank, 2016. URL: 10.1596/978-1-4648-0671-1.

[22] Oxford Analytica. *Hierarchy of Cybersecurity Needs: Developing National Priorities in a Connected World*. 2013. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmca.

[23] Ipsos. *CIGI-Ipsos Global Survey on Internet Security and Trust*. Centre for International Governance Innovation, 2019. URL: https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust.

[24] Sadie Creese et al. "Cybersecurity Capacity Building: Cross-National Benefits and International Divides". In: The Research Conference on Communications, Information, and Internet Policy 48. Feb. 2021. DOI: http://dx.doi.org/10.2139/ssrn.3658350.

[25] Jonathan Dolan. *Digital Inclusion and a Trusted Internet: The Role of the International Development Community in Balancing Internet Access and Cybersecurity*. Oct. 2018. URL: https://www.dai.com/cda-cybersecurity.pdf.

[26] Global Cyber Security Capacity Centre. *CMM Reviews around the World*. Global Cyber Security Capacity Centre. 2021. URL: https://gcscc.ox.ac.uk/cmm-reviews (visited on 04/19/2021).

[27] International Telecommunication Union. *Global Cybersecurity Index 2020*. Geneva, Switzerland: International Telecommunication Union, 2020. URL:

https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020.

[28] e-Governance Academy Foundation. *National Cyber Security Index*. URL: https://ncsi.ega.ee.

[29] Australian Strategic Policy Institute International Cyber Policy Centre. *Cyber Maturity in the Asia-Pacific Region*. 2017. URL: https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017.

[30] Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model For Nations*. Oxford, USA: Global Cyber Security Capacity Centre, 2021. URL: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf.

[31] Melissa Hathaway et al. *Cyber Readiness Index 2.0*. Arlington, VA, USA: Potomac Institude for Policy Studies, 2015. URL: https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

[32] Anastasiia Strielkina et al. "Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case-Oriented Assessment". In: *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). May 2018, pp. 67–73. DOI: 10.1109/DESSERT.2018.8409101.

[33] Salem T. Argaw et al. "The State of Research on Cyberattacks against Hospitals and Available Best Practice Recommendations: A Scoping Review". In: *BMC Medical Informatics and Decision Making* 19.1 (Jan. 11, 2019), p. 10. ISSN: 1472-6947. DOI: 10.1186/s12911-018-0724-5. URL: https://doi.org/10.1186/s12911-018-0724-5 (visited on 05/21/2021).

[34] Jeff Tully et al. "Healthcare Challenges in the Era of Cybersecurity". In: *Health Security* 18.3 (June 1, 2020), pp. 228–231. ISSN: 2326-5094. DOI: 10.

1089/hs.2019.0123. URL: https://www.liebertpub.com/doi/full/10.1089/hs.2019.0123 (visited on 04/28/2021).

[35] Soumitra Sudip Bhuyan et al. "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations". In: *Journal of Medical Systems* 44.5 (Apr. 2, 2020), p. 98. ISSN: 1573-689X. DOI: 10.1007/s10916-019-1507-y. URL: https://doi.org/10.1007/s10916-019-1507-y (visited on 04/28/2021).

[36] Lynne Coventry and Dawn Branley. "Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward". In: *Maturitas* 113 (July 1, 2018), pp. 48–52. ISSN: 0378-5122. DOI: 10.1016/j.maturitas.2018.04.008. URL: https://www.sciencedirect.com/science/article/pii/S0378512218301658 (visited on 04/28/2021).

[37] Guy Martin et al. "Cybersecurity and Healthcare: How Safe Are We?" In: *BMJ* 358.j3179 (July 6, 2017). ISSN: 0959-8138, 1756-1833. DOI: 10.1136/bmj.j3179. pmid: 28684400. URL: https://www.bmj.com/content/358/bmj.j3179 (visited on 04/28/2021).

[38] Chon Abraham, Dave Chatterjee, and Ronald R. Sims. "Muddling through Cybersecurity: Insights from the U.S. Healthcare Industry". In: *Business Horizons* 62.4 (July 1, 2019), pp. 539–548. ISSN: 0007-6813. DOI: 10.1016/j.bushor.2019.03.010. URL: https://www.sciencedirect.com/science/article/pii/S0007681319300436 (visited on 04/28/2021).

[39] Cyber Security Policy. *Securing Cyber Resilience in Health and Care*. 2018. URL: https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update.

[40] Check Point Software. *Attacks Targeting Healthcare Organizations Spike Globally as COVID-19 Cases Rise Again*. Check Point Blog. Jan. 5, 2021. URL: https://blog.checkpoint.com/2021/01/05/attacks-targeting-

healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/ (visited on 05/12/2021).

[41] Emmanuel Eze, Rob Gleasure, and Ciara Heavin. "Reviewing mHealth in Developing Countries: A Stakeholder Perspective". In: *Procedia Computer Science*. International Conference on ENTERprise Information Systems/International Conference on Project MANagement/International Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN / HCist 2016 100 (Jan. 1, 2016), pp. 1024–1032. ISSN: 1877-0509. DOI: 10.1016/j.procs.2016.09.276. URL: https://www.sciencedirect.com/science/article/pii/S1877050916324450 (visited on 04/29/2021).

[42] Alain B. Labrique et al. "Best Practices in Scaling Digital Health in Low and Middle Income Countries". In: *Globalization and Health* 14.1 (Nov. 3, 2018), p. 103. ISSN: 1744-8603. DOI: 10.1186/s12992-018-0424-z. URL: https://doi.org/10.1186/s12992-018-0424-z (visited on 04/29/2021).

[43] Yara M. Asi and Cynthia Williams. "The Role of Digital Health in Making Progress toward Sustainable Development Goal (SDG) 3 in Conflict-Affected Populations". In: *International Journal of Medical Informatics* 114 (June 1, 2018), pp. 114–120. ISSN: 1386-5056. DOI: 10.1016/j.ijmedinf.2017.11.003. URL: https://www.sciencedirect.com/science/article/pii/S138650561730415X (visited on 04/29/2021).

[44] Salifu Yusif, Abdul Hafeez-Baig, and Jeffrey Soar. "An Exploratory Study of the Readiness of Public Healthcare Facilities in Developing Countries to Adopt Health Information Technology (HIT)/e-Health: The Case of Ghana". In: *Journal of Healthcare Informatics Research* 4.2 (June 1, 2020), pp. 189–214. ISSN: 2509-498X. DOI: 10.1007/s41666-020-00070-8. URL: https://doi.org/10.1007/s41666-020-00070-8 (visited on 04/29/2021).

[45] Maurice Mars and Richard E. Scott. "Global E-Health Policy: A Work In Progress". In: *Health Affairs* 29.2 (Feb. 1, 2010), pp. 237–243. ISSN: 0278-2715. DOI: 10.1377/hlthaff.2009.0945. URL: https://doi.org/10.1377/hlthaff.2009.0945 (visited on 04/29/2021).

[46] Moses Namara et al. "Cross-Cultural Perspectives on eHealth Privacy in Africa". In: *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*. AfriCHI '18. New York, NY, USA: Association for Computing Machinery, Dec. 3, 2018, pp. 1–11. ISBN: 978-1-4503-6558-1. DOI: 10.1145/3283458.3283472. URL: https://doi.org/10.1145/3283458.3283472 (visited on 04/29/2021).

[47] Samuel S. Furusa and Alfred Coleman. "Factors Influencing E-Health Implementation by Medical Doctors in Public Hospitals in Zimbabwe". In: *South African Journal of Information Management* 20.1 (2018), pp. 1–9. ISSN: 1560-683X. DOI: 10.4102/sajim.v20i1.928. URL: http://www.scielo.org.za/scielo.php?script=sci_abstract&pid=S1560-683X2018000100010&lng=en&nrm=iso&tlng=en (visited on 05/17/2021).

[48] Ernest Adu, Nelly Todorova, and Annette Mills. "Do Individuals in Developing Countries Care about Personal Health Information Privacy? An Empirical Investigation". In: *CONF-IRM 2019 Proceedings* (2019). URL: https://aisel.aisnet.org/confirm2019/16.

[49] Wendy Burke et al. "Cybersecurity Indexes for eHealth". In: *Proceedings of the Australasian Computer Science Week Multiconference*. ACSW 2019. New York, NY, USA: Association for Computing Machinery, Jan. 29, 2019. ISBN: 978-1-4503-6603-8. DOI: 10.1145/3290688.3290721. URL: https://doi.org/10.1145/3290688.3290721 (visited on 04/28/2021).

[50] Niki O'Brien et al. *Safeguarding Our Healthcare Systems: A Global Framework for Cybersecurity*. Doha, Qatar: World Innovation Summit for Health, 2020. ISBN: 978-1-913991-03-6.

[51] World Health Organization. *Atlas of eHealth Country Profiles*. Jan. 1, 2016. URL: https://www.who.int/publications/i/item/9789241565219.

[52] World Health Organization. *Countries Overview*. URL: https://www.who.int/countries (visited on 08/23/2021).

[53] World Bank. *Countries and Economies*. URL: https://data.worldbank.org/country (visited on 06/24/2021).

[54] International Telecommunication Union. *Global Cybersecurity Index 2015*. Geneva, Switzerland: International Telecommunication Union, 2015. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

[55] World Bank. *World Bank Open Data*. URL: https://data.worldbank.org/ (visited on 07/27/2021).

[56] Anthony M. Maina and Upasana G. Singh. "Why National eHealth Strategies Matter - An Exploratory Study of eHealth Strategies of African Countries". In: *2020 International Conference on Electrical and Electronics Engineering (ICE3)*. 2020 International Conference on Electrical and Electronics Engineering (ICE3). Gorakhpur, India, Feb. 2020, pp. 670–675. DOI: 10.1109/ICE348803.2020.9122831.

[57] Mona Choi et al. "Building Consensus on the Priority-Setting for National Policies in Health Information Technology: A Delphi Survey". In: *Healthcare Informatics Research* 26.3 (July 31, 2020), pp. 229–237. DOI: 10.4258/hir.2020.26.3.229. URL: https://synapse.koreamed.org/articles/1144871?viewtype=pubreader (visited on 07/14/2021).

[58] World Health Organization and International Telecommunication Union. *National eHealth Strategy Toolkit*. 2012. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH.05-2012-PDF-E.pdf (visited on 07/14/2021).

[59] Government of Uganda. *Uganda National eHealth Strategy 2017-2021*.

[60] Government of Cameroon. *Cameroon 2020-2024 National Digital Health Strategic Plan*. URL: https://www.minsante.cm/site/?q=en/content/2020-2024-national-digital-health-strategic-plan.

[61] Government of Nigeria. *Nigeria 2015-2020 National Health ICT Strategic Framework*. Mar. 2016. URL: https://www.who.int/goe/policies/Nigeria_health.pdf?ua=1.

[62] Government of Zambia. *Zambia 2017-2021 Health Strategy*. URL: https://www.moh.gov.zm/?wpfb_dl=150.

[63] Government of Uganda. *Uganda National Information Security Policy*. 2014. URL: https://www.nita.go.ug/sites/default/files/publications/National%20Information%20Security%20Policy%20v1.0_0.pdf.

[64] Government of Uganda. *Uganda Data Protection and Privacy Act 2019*. 2019. URL: https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf.

[65] Boade Akinola. *FG Inaugurates National Ehealth Steering Committee To Address Nigeria's Health Sector Challenges*. PRNigeria News. Sept. 15, 2016. URL: https://prnigeria.com/2016/09/15/fg-inaugurates-national-ehealth-steering-committee-address-nigerias-health-sector-challenges/ (visited on 07/17/2021).

[66] Government of Zambia. *Zambia Electronic Communications and Transactions Act, 2009*. 2009. URL: https://www.zicta.zm/storage/sites/attachments/M9jCaLuJ7Vin4Pe9lcuAYeTQuV0oGLHb0KZynsKD.pdf.

[67] Government of Zambia. *Zambia Electronic Communications and Transactions Act 2021*. 2021. URL: https://www.parliament.gov.zm/node/8842.

[68] Government of Zambia. *Zambia Data Protection Act 2021*. 2021. URL: https://www.parliament.gov.zm/node/8853.

[69] Karl A. Stroetmann, Jorg Artmann, and Veli N Stroetmann. *eHealth Strategies: European Countries on Their Journey towards National eHealth Infrastructures*. European Commission Information Society, Jan. 2011. URL: http://dx.doi.org/10.2759/47528.

[70] Patrick Kierkegaard. "Governance Structures Impact on eHealth". In: *Health Policy and Technology* 4.1 (Mar. 1, 2015), pp. 39–46. ISSN: 2211-8837. DOI: 10.1016/j.hlpt.2014.10.016. URL: https://www.sciencedirect.com/science/article/pii/S2211883714000896 (visited on 07/25/2021).

[71] Alina Wernick and Irma Klünker. "Prohibitions on Long Distance Treatment: Historical Roots and Continuities in Limiting the Use of Electronic Telemedicine". In: *The Futures of eHealth: Social, Ethical and Legal Challenges*. Berlin, Germany: Alexander Von Humboldt Institute For Internet And Society, 2019, pp. 169–177. URL: https://www.hiig.de/wp-content/uploads/2019/07/Ehealth2040_web.pdf#page=169.

[72] Lucija Tepej Jočić. "Impact of Data Protection Regulation on Slovenian eHealth". In: *Journal of Global Health* 11 (), p. 03063. ISSN: 2047-2978. DOI: 10.7189/jogh.11.03063. pmid: 33828841. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8005304/ (visited on 07/25/2021).

[73] David Rudner, Lydia Toussaint, and Nao Sipula. "Unjani Nurses Lead the Way: How eHealth Can Improve Access to Healthcare in Rural South Africa". In: *The Futures of eHealth: Social, Ethical and Legal Challenges*. Berlin, Germany: Alexander Von Humboldt Institute For Internet And Society, 2019,

pp. 109–114. URL: https://www.hiig.de/wp-content/uploads/2019/07/Ehealth2040_web.pdf#page=109.

[74] Council for Scientific Research. *National Health Normative Standards Framework for Interoperability in eHealth in South Africa*. Mar. 2014. URL: https://www.colleaga.org/sites/default/files/attachments/hnsf-complete-version%201.pdf.

[75] Government of Kenya. *The Data Protection Act*. Nov. 11, 2019. URL: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf.

[76] Government of Canada. *Understand How Health Care Works in Canada*. May 31, 2009. URL: https://www.canada.ca/en/immigration-refugees-citizenship/services/new-immigrants/new-life-canada/health-care-card.html (visited on 07/27/2021).

[77] Government of Canada. *Canada Health Act Annual Report 2019-2020*. Feb. 22, 2021. URL: https://www.canada.ca/en/health-canada/services/publications/health-system-services/canada-health-act-annual-report-2019-2020.html (visited on 07/27/2021).

[78] Government of Canada. *Canada Health Act*. 1984. URL: https://laws-lois.justice.gc.ca/eng/acts/c-6/FullText.html (visited on 07/27/2021).

[79] Government of Canada. *Criminal Code*. May 6, 2021. URL: https://laws-lois.justice.gc.ca/eng/acts/c-46/FullText.html (visited on 07/27/2021).

[80] Government of Canada. *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities That Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-Television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic

Documents Act and the Telecommunications Act. Jan. 15, 2015. URL: https://laws-lois.justice.gc.ca/eng/acts/E-1.6/FullText.html (visited on 07/27/2021).

[81] Government of Canada. *Personal Information Protection and Electronic Documents Act*. June 21, 2019. URL: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html (visited on 07/27/2021).

[82] Office of the Privacy Commissioner of Canada. *PIPEDA in Brief*. Office of the Privacy Commissioner of Canada. Jan. 9, 2018. URL: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ (visited on 07/27/2021).

[83] Government of Canada. *Secure Electronic Signature Regulations*. Mar. 10, 2011. URL: https://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/FullText.html (visited on 07/27/2021).

[84] Government of Ontario. *Personal Health Information Protection Act*. 2004. URL: https://www.ontario.ca/laws/statute/04p03 (visited on 07/27/2021).

[85] Government of New Brunswick. *Personal Health Information Privacy and Access Act*. 2009. URL: http://laws.gnb.ca/en/showfulldoc/cs/P-7.05//20210727 (visited on 07/27/2021).

[86] Government of Nova Scotia. *Personal Health Information Act*. 2010. URL: https://nslegislature.ca/legc/bills/61st_2nd/3rd_read/b089.htm (visited on 07/27/2021).

[87] Government of Newfoundland and Labrador. *Personal Health Information Act*. 2008. URL: https://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm (visited on 07/27/2021).

[88] Regina Mbindyo et al. "Legal and Institutional Foundations for Universal Health Coverage, Kenya". In: *Bulletin of the World Health Organization* 98.10 (Oct. 1, 2020), pp. 706–718. ISSN: 0042-9686. DOI: 10.2471/BLT.19.237297. pmid: 33177760. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7652562/ (visited on 07/27/2021).

[89] Government of Kenya. *The Health Act*. July 27, 2017. URL: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/HealthActNo.21of2017.pdf.

[90] Government of Kenya. *Computer Misuse and Cybercrimes Act*. 2018. URL: https://ictpolicyafrica.org/en/document/pb8w26fcso (visited on 07/28/2021).

[91] Mercy Muendo. "Kenya's New Cybercrime Law Opens the Door to Privacy Violations, Censorship". In: *The Conversation* (May 29, 2018). URL: http://theconversation.com/kenyas-new-cybercrime-law-opens-the-door-to-privacy-violations-censorship-97271 (visited on 07/28/2021).

[92] Dominic Indokhomi and John Syekei. *The Computer Misuse and Cybercrimes Act*. Bowmans. Mar. 6, 2020. URL: https://www.bowmanslaw.com/insights/finance/the-computer-misuse-and-cybercrimes-act/ (visited on 08/24/2021).

[93] Evans Monari. *The Nullification of "Senate" Laws - The Decision in the Senate vs The Speaker of the National Assembly & Another*. Bowmans. Nov. 6, 2020. URL: https://www.bowmanslaw.com/insights/dispute-resolution/the-nullification-of-senate-laws-the-decision-in-the-senate-vs-the-speaker-of-the-national-assembly-another/ (visited on 08/24/2021).

[94] Kenya Ministry of Health. *Health Sector ICT Standards and Guidelines*. June 2013. URL: https://www.medbox.org/pdf/5e148832db60a2044c2d2895 (visited on 07/27/2021).

[95] Kenya Ministry of Medical Services and Kenya Ministry of Public Health and Sanitation. *Standards and Guidelines for Electronic Medical Records Systems in Kenya*. 2010. URL: https://www.ghdonline.org/uploads/Standards_and_Guidelines_for_Electronic_Medical_Record_Systems.pdf.

[96] Kenya Ministry of Health. *Kenya Health Information Systems Interoperability Framework*. 2020. URL: https://www.data4sdgs.org/sites/default/files/services_files/Kenya%20Health%20Information%20Systems%20Interoperability%20Framework.pdf.

[97] Privacy International. *After the Gold Rush: Developing Cyber Security Frameworks and Cyber Crime Legislation to Safeguard Privacy and Security*. Aug. 2018. URL: https://privacyinternational.org/sites/default/files/2018-10/Web_After%20the%20Gold%20Rush-Cybersecurity_0.pdf.

[98] United Nations. *Universal Declaration of Human Rights*. 1948. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights (visited on 07/28/2021).

[99] Privacy International. *The Keys to Data Protection*. Aug. 2018. URL: https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf.

[100] Oleg Bestsennyy et al. "Telehealth: A Post-COVID-19 Reality?" In: *McKinsey* (). URL: https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality# (visited on 07/28/2021).

[101] Valerie J. M. Watzlaf et al. "A Systematic Review of Research Studies Examining Telehealth Privacy and Security Practices Used by Healthcare Providers". In: *International Journal of Telerehabilitation* 9.2 (Nov. 20, 2017), pp. 39–59. ISSN: 1945-2020. DOI: 10.5195/ijt.2017.6231. pmid: 29238448. URL:

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5716616/ (visited on 07/28/2021).

[102] Leming Zhou et al. "A Telehealth Privacy and Security Self-Assessment Questionnaire for Telehealth Providers: Development and Validation". In: *International Journal of Telerehabilitation* 11.1 (June 12, 2019), pp. 3–14. ISSN: 1945-2020. DOI: 10.5195/ijt.2019.6276. pmid: 31341542. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6597150/ (visited on 07/28/2021).

[103] Brinda Hansraj Sampat and Bala Prabhakar. "Privacy Risks and Security Threats in mHealth Apps". In: *Journal of International Technology and International Management* 26.4 (Dec. 1, 2017). URL: https://scholarworks.lib.csusb.edu/jitim/vol26/iss4/5?utm_source=scholarworks.lib.csusb.edu%2Fjitim%2Fvol26%2Fiss4%2F5&utm_medium=PDF&utm_campaign=PDFCoverPages.

[104] Achilleas Papageorgiou et al. "Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice". In: *IEEE Access* 6 (Jan. 29, 2018), pp. 9390–9403. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2799522.

[105] Kit Huckvale et al. "Unaddressed Privacy Risks in Accredited Health and Wellness Apps: A Cross-Sectional Systematic Assessment". In: *BMC Medicine* 13.1 (Sept. 25, 2015), p. 214. ISSN: 1741-7015. DOI: 10.1186/s12916-015-0444-y. URL: https://doi.org/10.1186/s12916-015-0444-y (visited on 07/29/2021).

[106] Jennifer Moodley et al. "Exploring the Feasibility of Using Mobile Phones to Improve the Management of Clients with Cervical Cancer Precursor Lesions". In: *BMC Women's Health* 19.1 (Jan. 7, 2019), p. 2. ISSN: 1472-6874. DOI: 10.1186/s12905-018-0702-1. URL: https://doi.org/10.1186/s12905-018-0702-1 (visited on 07/29/2021).

[107] Javad Pool, Saeed Akhlaghpour, and Farhad Fatehi. "Towards a Contextual Theory of Mobile Health Data Protection (MHDP): A Realist Perspective". In: *International Journal of Medical Informatics* 141 (Sept. 1, 2020), p. 104229. ISSN: 1386-5056. DOI: 10.1016/j.ijmedinf.2020.104229. URL: https://www.sciencedirect.com/science/article/pii/S1386505620305645 (visited on 07/29/2021).

[108] Craig E. Kuziemsky et al. "Balancing Health Information Exchange and Privacy Governance from a Patient-Centred Connected Health and Telehealth Perspective". In: *Yearbook of Medical Informatics* 27.1 (Aug. 2018), pp. 48–54. ISSN: 0943-4747, 2364-0502. DOI: 10.1055/s-0038-1641195. URL: http://www.thieme-connect.de/DOI/DOI?10.1055/s-0038-1641195 (visited on 07/28/2021).

[109] United States Office for Civil Rights. *Notification of Enforcement Discretion for Telehealth*. Mar. 17, 2020. URL: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html (visited on 07/29/2021).

[110] KANTAR Group. *Internet Adoption in India ICUBE 2020*. June 2021. URL: https://images.assettype.com/afaqs/2021-06/b9a3220f-ae2f-43db-a0b4-36a372b243c4/KANTAR_ICUBE_2020_Report_C1.pdf.

[111] Anirudh Krishna and Kripa Ananthpur. "Globalization, Distance and Disease: Spatial Health Disparities in Rural India". In: *Millennial Asia* 4.1 (Apr. 1, 2013), pp. 3–25. ISSN: 0976-3996. DOI: 10.1177/0976399613480879. URL: https://doi.org/10.1177/0976399613480879 (visited on 08/09/2021).

[112] Marco J. Haenssgen. "The Struggle for Digital Inclusion: Phones, Healthcare, and Marginalisation in Rural India". In: *World Development* 104 (Apr. 1, 2018), pp. 358–374. ISSN: 0305-750X. DOI: 10.1016/j.worlddev.2017.

12.023. URL: https://www.sciencedirect.com/science/article/pii/S0305750X17304163 (visited on 08/09/2021).

[113] Indian Ministry of Health and Family Welfare. *Telemedicine Practice Guidelines*. Mar. 25, 2020. URL: https://www.mohfw.gov.in/pdf/Telemedicine.pdf.

[114] David Rupprecht et al. "Call Me Maybe: Eavesdropping Encrypted {LTE Calls With ReVoLTE". In: 29th {USENIX Security Symposium ({USENIX Security 20). 2020, pp. 73–88. ISBN: 978-1-939133-17-5. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/rupprecht (visited on 08/10/2021).

[115] Diego Perez-Botero and Yezid Donoso. "VoIP Eavesdropping: A Comprehensive Evaluation of Cryptographic Countermeasures". In: *2011 Second International Conference on Networking and Distributed Computing*. 2011 Second International Conference on Networking and Distributed Computing. Sept. 2011, pp. 192–196. DOI: 10.1109/ICNDC.2011.46.

[116] Indian Ministry of Communications and Information Technology. *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011*. Apr. 11, 2011. URL: https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf.

[117] M. Ramesh. "WhatsApp and the Wait for Data Protection Bill". In: *The Hindu. Business Laws* (July 11, 2021). URL: https://www.thehindubusinessline.com/business-laws/whatsapp-and-the-wait-for-data-protection-bill/article35266846.ece (visited on 08/09/2021).

[118] Neeraj Agarwal and Bijit Biswas. "Doctor Consultation through Mobile Applications in India: An Overview, Challenges and the Way Forward". In: *Healthcare Informatics Research* 26.2 (Apr. 2020), pp. 153–158. ISSN: 2093-3681. DOI: 10.4258/hir.2020.26.2.153. pmid: 32547812. URL: https:

//www.ncbi.nlm.nih.gov/pmc/articles/PMC7278514/ (visited on 08/09/2021).

[119] *Babyl – Rwanda's Digital Healthcare Provider*. URL: https://babyl.rw/ (visited on 08/09/2021).

[120] Alex Weinhart. *It's Time to Hang Up on Phone Transports for Authentication*. Microsoft Tech Community. Nov. 10, 2020. URL: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/it-s-time-to-hang-up-on-phone-transports-for-authentication/ba-p/1751752 (visited on 08/09/2021).

[121] Ajin Abraham et al. *Mobile-Security-Framework*. URL: https://github.com/MobSF/Mobile-Security-Framework-MobSF (visited on 08/09/2021).

[122] Open Web Application Security Project. *OWASP Mobile Security*. URL: https://owasp.org/www-project-mobile-security/ (visited on 08/09/2021).

[123] Michael Ogata et al. *Vetting the Security of Mobile Applications*. NIST Special Publication (SP) 800-163 Rev. 1. National Institute of Standards and Technology, Apr. 19, 2019. DOI: 10.6028/NIST.SP.800-163r1. URL: https://csrc.nist.gov/publications/detail/sp/800-163/rev-1/final (visited on 08/09/2021).

[124] Open Web Application Security Project. *OWASP Secure Coding Practices Quick Reference Guide*. 2010. URL: https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf.

[125] Open Web Application Security Project. *OWASP Web Security Testing Guide*. URL: https://owasp.org/www-project-web-security-testing-guide/ (visited on 08/10/2021).

[126] Fortified Health Security. *2021 Horizon Report: The State of Cybersecurity in Healthcare*. Dec. 2020. URL: https://fortifiedhealthsecurity.com/

wp-content/uploads/2020/12/Fortified-Health-Security-2021-Horizon-Report.pdf.

[127] Maryam Farhadi, Hisham Haddad, and Hossain Shahriar. "Static Analysis of HIPPA Security Requirements in Electronic Health Record Applications". In: *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Vol. 02. July 2018, pp. 474–479. DOI: 10.1109/COMPSAC.2018.10279.

[128] Maryam Farhadi, Hisham Haddad, and Hossain Shahriar. "Compliance Checking of Open Source EHR Applications for HIPAA and ONC Security and Privacy Requirements". In: *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). Vol. 1. July 2019, pp. 704–713. DOI: 10.1109/COMPSAC.2019.00106.

[129] Zakina McGee and Subrata Acharya. "Security Analysis of OpenEMR". In: *2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*. 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM). Nov. 2019, pp. 2655–2660. DOI: 10.1109/BIBM47256.2019.8983178.

[130] Nancy Shank et al. "Electronic Health Records: Eliciting Behavioral Health Providers' Beliefs". In: *Community Mental Health Journal* 48.2 (Apr. 1, 2012), pp. 249–254. ISSN: 1573-2789. DOI: 10.1007/s10597-011-9409-6. URL: https://doi.org/10.1007/s10597-011-9409-6 (visited on 08/02/2021).

[131] Pradeep Deshmukh. "Design of Cloud Security in the EHR for Indian Healthcare Services". In: *Journal of King Saud University - Computer and Information Sciences* 29.3 (July 1, 2017), pp. 281–287. ISSN: 1319-1578. DOI:

10.1016/j.jksuci.2016.01.002. URL: https://www.sciencedirect.com/science/article/pii/S1319157816300118 (visited on 08/02/2021).

[132] Yong Wang et al. "Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain". In: *IEEE Access* 7 (2019), pp. 136704–136719. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2943153.

[133] Raghavendra Ganiga et al. "Security Framework for Cloud Based Electronic Health Record (EHR) System". In: *International Journal of Electrical and Computer Engineering* 10.1 (Feb. 2020), pp. 455–466. ISSN: 2088-8708. DOI: 10.11591/ijece.v10i1.pp455-466.

[134] Fatemeh Rezaeibagha, Khin Than Win, and Willy Susilo. "A Systematic Literature Review on Security and Privacy of Electronic Health Record Systems: Technical Perspectives". In: *Health Information Management Journal* 44.3 (Oct. 1, 2015), pp. 23–38. ISSN: 1833-3583. DOI: 10.1177/183335831504400304. URL: https://doi.org/10.1177/183335831504400304 (visited on 08/02/2021).

[135] Australian Government Department of Health. *The Australian Health System*. Australian Government Department of Health. Aug. 10, 2018. URL: https://www.health.gov.au/about-us/the-australian-health-system (visited on 08/04/2021).

[136] Steven J. Hambleton and John Aloizos AM. "Australia's Digital Health Journey". In: *Medical Journal of Australia* 210.6 (Mar. 31, 2019). ISSN: 0025-729X. URL: https://www.mja.com.au/journal/2019/210/6/australias-digital-health-journey#12 (visited on 08/03/2021).

[137] Australia Health Ministers' Conference. *National E-Health Strategy*. Dec. 2008. URL: https://www1.health.gov.au/internet/main/publishing.nsf/content/69B9E01747B836DCCA257BF0001DC5CC/$File/Summary%20National%20E-Health%20Strategy%20final.pdf.

[138] Government of Australia. *My Health Records Act 2012*. June 2013. URL: https://www.legislation.gov.au/Details/C2020C00372 (visited on 08/03/2021).

[139] Australian Digital Health Agency. *Legislation and Governance*. My Health Record. Feb. 26, 2018. URL: https://www.myhealthrecord.gov.au/about/legislation-and-governance (visited on 08/03/2021).

[140] Government of Australia. *My Health Records Rule 2016*. Apr. 2016. URL: https://www.legislation.gov.au/Details/F2016C00607 (visited on 08/03/2021).

[141] Government of Australia. *My Health Records Amendment (Strengthening Privacy) Act 2018*. Dec. 2018. URL: https://www.legislation.gov.au/Details/C2018A00154 (visited on 08/03/2021).

[142] Asha Barbaschow. "Nearly 23 Million Aussies Have a My Health Record, but Only 13 Million Are Using It". In: *ZDNet* (Apr. 8, 2020). URL: https://www.zdnet.com/article/nearly-23-million-aussies-have-a-my-health-record-but-only-13-million-are-using-it/ (visited on 08/03/2021).

[143] Josh Taylor and Amy Corderoy. "My Health Record: Almost $2bn Spent but Half the 23m Records Created Are Empty". In: *the Guardian. Australia news* (Jan. 22, 2020). URL: http://www.theguardian.com/australia-news/2020/jan/23/my-health-record-almost-2bn-spent-but-half-the-23m-records-created-are-empty (visited on 08/03/2021).

[144] Australian Digital Health Agency. *Control Access to Your Record*. My Health Record. Feb. 12, 2019. URL: https://www.myhealthrecord.gov.au/for-you-your-family/howtos/control-access-your-record (visited on 08/03/2021).

[145] Chris Duckett. *My Health Record Access Controls Used Only 214 Times in Million Record Trial*. Sept. 5, 2018. URL: https://www.zdnet.com/article/my-health-record-access-controls-used-only-214-times-in-million-record-trial/ (visited on 08/03/2021).

[146] Australian National Audit Office. *Implementation of the My Health Record System*. Nov. 25, 2019. URL: https://www.anao.gov.au/work/performance-audit/implementation-the-my-health-record-system (visited on 08/03/2021).

[147] Bruce Baer Arnold, David Vaile, and Katharine Kemp. "My Health Record: The Case for Opting Out". In: *The Conversation* (), pp. 2018-07–18. URL: http://theconversation.com/my-health-record-the-case-for-opting-out-99302 (visited on 08/03/2021).

[148] The Australian Privacy Foundation. *My Health Record*. URL: https://privacy.org.au/Campaigns/MyHR/index.html (visited on 08/03/2021).

[149] Daniel Aran and Hernán Laca. "Sistema de salud de Uruguay". In: *Salud Pública de México* 53.2 (Jan. 2011), pp. 265–274. ISSN: 0036-3634. URL: http://www.scielo.org.mx/scielo.php?script=sci_abstract&pid=S0036-36342011000800021&lng=es&nrm=iso&tlng=es (visited on 08/04/2021).

[150] David Hammond. *Healthcare in Uruguay*. International Living. URL: https://internationalliving.com/countries/uruguay/health-care/ (visited on 08/04/2021).

[151] Uruguay Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. *Iniciativas de Salud.uy*. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/proyectos/iniciativas-de-saluduy (visited on 08/04/2021).

[152] Laura González et al. “Data Quality Management in E-Health Integration Platforms: The Case of Uruguay”. In: *CLEI Electronic Journal* 21.2 (Aug. 1, 2018). DOI: 10.19153/cleiej.21.2.5.

[153] Uruguay Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. *Historia Clínica Electrónica Nacional*. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/node/312 (visited on 08/04/2021).

[154] Government of Uruguay. *Ley No 18335*. Aug. 26, 2008. URL: https://www.impo.com.uy/bases/leyes/18335-2008 (visited on 08/04/2021).

[155] Government of Uruguay. *Ley No 19670*. Oct. 25, 2018. URL: https://www.impo.com.uy/bases/leyes/19670-2018 (visited on 08/04/2021).

[156] Government of Uruguay. *Ley No 18331*. Aug. 11, 2008. URL: https://www.impo.com.uy/bases/leyes/18331-2008 (visited on 08/04/2021).

[157] Government of Uruguay. *Decree No. 122/019*. May 13, 2019. URL: https://www.impo.com.uy/bases/decretos-originales/122-2019 (visited on 08/04/2021).

[158] Government of Uruguay. *Decreto No 242/017*. Sept. 7, 2017. URL: https://www.impo.com.uy/bases/decretos/242-2017 (visited on 08/04/2021).

[159] Government of Uruguay. *Ley No 18600*. Nov. 5, 2009. URL: https://www.impo.com.uy/bases/leyes/18600-2009 (visited on 08/04/2021).

[160] Uruguay Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. *Marco de Ciberseguridad*. Nov. 2019. URL: https://archivos.agesic.gub.uy/nextcloud/index.php/s/pFXtSiWT47Kdaaz (visited on 08/04/2021).

[161] Uruguay Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. *Marco de Ciberseguridad*. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. July 14, 2021. URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad (visited on 08/04/2021).

[162] Uruguay Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. *Guía de Implementación*. Nov. 2019. URL: https://archivos.agesic.gub.uy/nextcloud/index.php/s/qmAqzYpqJN2F35r (visited on 08/04/2021).

[163] Uruguay gencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. *Presentación Avances HCEN 2019*. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. Jan. 10, 2019. URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/presentacion-avances-hcen-2019 (visited on 08/04/2021).

[164] Jorge Repiso. "Historias Clínicas Electrónicas: ¿ctrl + alt + supr?" In: *Epidauro. Actualidad en salud* (Oct. 8, 2019). URL: http://epidauro.com.ar/historias-clinicas-electronicas-ctrl-alt-supr/ (visited on 08/04/2021).

[165] Ida Oreggioni. "Nuestra Historia Clínica Electrónica Nacional". In: *La Diaria. Posturas* (Nov. 7, 2019). URL: https://ladiaria.com.uy/opinion/articulo/2019/11/nuestra-historia-clinica-electronica-nacional/ (visited on 08/04/2021).

[166] National Institude of Standards and Technology. *The Five Functions*. National Institude of Standards and Technology. Apr. 12, 2018. URL: https:

//www.nist.gov/cyberframework/online-learning/five-functions (visited on 08/05/2021).

[167] *OpenEMR Wiki Home Page*. OpenEMR Wiki. URL: https://www.open-emr.org/wiki/index.php/OpenEMR_Wiki_Home_Page (visited on 08/05/2021).

[168] Brian LaVallee. *Poing/phpGACL*. Oct. 13, 2017. URL: https://github.com/poing/phpGACL (visited on 08/05/2021).

[169] National Cyber Security Centre. *Password Policy: Updating Your Approach*. National Cyber Security Centre. URL: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach (visited on 08/05/2021).

[170] Australian Digital Health Agency. *Australian Digital Health Agency Annual Report 2019-20*. 2020. URL: https://www.digitalhealth.gov.au/about-us/annual-reports (visited on 08/05/2021).

[171] Australian Digital Health Agency. *Australian Digital Health Agency Annual Report 2018-19*. 2019. URL: https://www.digitalhealth.gov.au/about-us/annual-reports.