2023 10th International Conference on Future Internet of Things and Cloud (FiCloud) | 979-8-3503-1635-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/FiCloud58648.2023.00013

A Novel Approach to Measure and Predict Digital Health Data Protection Compliant (DPC)

Davies C Ogbodo*
Department of Computer Science
University of Bradford
D.C.Ogbodo@student.bradford.ac.uk

Irfan Ullah-Awan‡
Department of Computer Science
University of Bradford
I.U.Awan@bradford.ac.uk

Andrea Cullen†
Department of Computer Science
University of Bradford
A.J.Cullen@bradford.ac.uk

***Abstract*—Many health institutions and government agencies have struggled to combat the challenges of digital health data protection. A prevailing issue with current strategies to effectively counter this threat is their incapacity to provide robust digital health data protection mechanisms. To varying degrees, the obstacles hinge significantly on the quality of IT infrastructure, regulatory frameworks, healthcare practices, proper data governance, and ethical frameworks underpinned by four principles: respect for persons, data fairness, privacy, and accountability. Thus, we have approached these challenges utilising a risk-based prioritisation framework. Our proposed contribution involves scientific observations and measurements derived from data analysis, as well as modelling and design of algorithms and systems that can be employed in digital health data protection, based on six identified domains or pillars of technology, cybersecurity, digital health data governance, data protection legislation, policies, and risk assessment, in the novel approach of measuring and forecasting compliance with digital health data protection.**

Keywords—Digital health, Data Protection, Digital Health Data, Cybersecurity, Policy, Data Governance, Support Vector Machine, Risk Assessment

I. INTRODUCTION

Digitalisation has become the bane of the modern world, and there is an enormous race to explore the digital space and technology for efficient and effective healthcare delivery; however, this has resulted in an increase in risk due to exposure to cybercrime [1] [2] [3] [4]. It is well known that digitalisation is shaking every industry and disrupting traditional business approaches. The world is adjusting to an increasingly rapid pace of change amidst the current highly technology-connected world [1] [5] [6] [7].

As we move toward an increasingly digitised world of healthcare, the most pertinent thinking is how all involved in its management uphold their responsibilities, follow relevant laws and regulations, and maintain the trust of patients and users when it comes to privacy and how to operate under the highest standards in healthcare [3] [4] . Furthermore, data and digital health are significant components that will become defining factors soon because of the enormous amount of human health-related data that will be generated and the struggle that the world will face in ensuring that the data are both secured and protected[1] [5] [6] [7].

This study aims to identify and discuss the recurring themes surrounding the field of data protection within the context of digital data protection as one of the most critical areas for health-related information. The focus of this research is to examine data protection, privacy, and cybersecurity in an ever-changing world of digital health, exploring convenient and efficient ways to ensure the protection of patient digital data without compromising easy access by all relevant persons [8] [9] [10].

[7]It is both essential and relevant to point out that the World Health Organisation (WHO) recommends that to ensure full compliance with applicable data protection laws and regulations, processing health-related personal data should adhere to the following data protection principles:

- Fair, lawful, and transparent: Personal data shall be processed fairly, lawfully, and transparently concerning the data subject.
- Purpose limitation: Personal data should be obtained only for one or more specified and lawful purposes.
- Accuracy: Personal data should be accurate and, where necessary, kept up to date.

Accordingly, research has shown that a substantial investment in technology security has not translated to reductions in health data cybersecurity breaches [11] [12] [13]. The effects and challenges of non-compliance with data protection laws in handling digital health data worldwide could be dangerous waiting to unleash its catastrophe. Several strategies have been employed to bridge the gaps inherent in digital health data protection non-compliance. However, none have adequately addressed the gaps, so this research hopes to address the gaps using six sufficiently identified integrated critical pillars of technology, legislation, governance, cybersecurity, policy, and risk assessment as encapsulated in the health data ecosystem [11] [12] [13].

II. LITERATURE REVIEW

This critically reviews the literature on data protection and digital health, emphasising state-of-the-art cybersecurity and its effects on digital health data. In addition, a detailed review of the research works conducted in this area will be discussed with its attendant applications. Given the lack of structurally organised information on digital health data protection with dependence on legislation, cybersecurity, technology, policy, digital data governance framework, and risk assessment, we hope that this research will provide insights that are not easily accessible otherwise [11] [12] [13].

Although many research papers are not available in this field, many individual topics have been studied by different communities. However, at this stage, it becomes essential to organise the topics in such a way that the relative importance of digital health data protection with the different vital variables, factors, or dependences as enunciated above within this research area is finally recognised [1] [11] [12] [13].
It is pertinent to note that for 11 years running, the healthcare sector has succumbed to the costliest data breaches of all

979-8-3503-1635-3/23/$31.00 ©2023 IEEE
DOI 10.1109/FiCloud58648.2023.00013

sectors. In the United States, the total average data breaches in 2021 alone cost US$9.23 million, and it worsens as the number of data breaches continues to increase yearly; for instance, from 2020 to 2021, there was a 29% spike in the average total cost of U.S. healthcare data breaches [14].

The stakes in data security in the healthcare sector are incredibly high. It is becoming increasingly difficult to prevent and limit damage from data breaches because of how the industry operates. Data generated and stored in healthcare systems presents many lucrative opportunities for exploitation. Heavy reliance on new technology that is intertwined into healthcare systems and how data flow across different parts of the industry opens countless opportunities for cybercrimes [8] [15].

The key goals of this research are (I) to recognise and sequence the identified variables that influence adequate protection and management of health data, (II) to establish the relationship among the identified variables, and (III) to grasp the results of this research in the management of high dependability of the identified variables and triggers needed and desirable changes to digital health data protection [16].

A. Digital Health and Digital Health Data

Healthcare is one of the most critical industries in the world. However, in recent years, there has been a big push for more investment in healthcare-related information technology to improve healthcare processes' efficiencies and significantly improve healthcare quality of healthcare [8] [15]. However, currently, there is no consensus on the definition of digital health. For instance, the term "digital medicine" resembles digital health, as it also refers to the use of digital technologies. However, according to the US Food and Drugs Administration (FDA), "the broad scope of digital health includes categories such as mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine." These categories rely heavily on human health data [8] [15].

Therefore, digital health is a rapidly expanding medical field premised on the availability of ever-increasing amounts of data about people's lifestyles, habits, clinical histories, and pathophysiological characteristics. However, the defining feature of digital health is data, rather than technology. Simultaneously, for digital health to materialize, several ethical and policy challenges must be overcome [1] [17] [18].

.

B. A Global Ethical Terrain

As we move toward an increasingly digitised world of healthcare, the concern should be how all involved can uphold their responsibilities, follow relevant laws and regulations, and maintain the trust of patients and users regarding digital health data protection. How health data are gathered, handled, and stored everywhere and anywhere in healthcare requires careful ethical attention [1] [17] [18].

[1] [17] [18] Digital health uses computer technologies to harness an enormous collection of related private and other data to deliver enhanced healthcare services. The argument is that innovations in digital health promise vastly improved health care, significant quality of life, and benefits for consumers of health care services.

[19] argues that the common thread that connects almost all these incredible, life-enhancing innovations is that they are made possible by collecting, analysing, and applying all-embracing health and other personal datasets. Personal health data are among the most sensitive types of personal information. The way such data are gathered, handled, and stored requires thorough attention [1] [17] [18].

[20] postulated that the immense promise of digital health, resting on the foundation of extensive personal data, also carries significant concern over personal privacy and data security expectations. These concerns are a source of extensive legal regulations. As more parties in the healthcare system become digital, the size and frequency of data breaches become alarming.

C. Legislation - Data Protection and Privacy

For 150 years, privacy through the trajectories of common law decisions, constitutional reflections, and many species of legislation can be seen as one of the most enigmatic concepts in law and political order. In earlier cases, privacy was intrinsically bound to property rights. This is revealed in the landmark transition theory posited by Warren and Brandeis in their seminal understanding in the late nineteenth century in the US, where privacy was determined as a "right to be let alone' [21] [22].

In 1890, two American lawyers, Samuel D. Warren, and Louis Brandeis, wrote "The right to privacy," an article arguing that individuals have a "right to be left alone," using the phrase as a definition of privacy. In 1948, the Universal Declaration of Human Rights was adopted, including the twelfth fundamental right: the right to privacy. As technological advances have accelerated, legal frameworks for data protection have evolved. In 1980, the Organization for Economic Co-operation and Development issued guidelines on data protection in direct response to the increasing use and power of computers to process data. A year later, the Council of Europe adopted the Data Protection Convention, Convention 108, the first time the right to privacy was enshrined into law for European countries. Initially, the regulatory framework was supposed to protect individual citizens from intrusions into their privacy by the state.

In late 1983, the Federal Constitutional Court of Germany reached a fundamental decision regarding the census judgment. The verdict was considered a milestone in data protection as it shaped the "right to informational self-determination." The German Court's decision would continue to influence the rise of data protection for decades. In 1995, the European Data Protection Directive 95/46/EC was created, reflecting technological advances, and introducing new terms including processing, sensitive personal data, and consent.

The directive specifically targets the increasing power imbalance between private corporations and citizens, clarifying that the right to informational self-determination is universal and can be used against anybody. In 2016, the European Parliament approved the General Data Protection Regulation (GDPR) after four years of discussion. GDPR serves as a blueprint for various data protection acts around

the globe [23]. In 2018, the United Nations enacted the Personal Data Protection and Privacy Principles as the primary source for protecting personal data by all United Nations institutions.

1. Global View and Perspective

Digital health represents a global phenomenon; it is adopted and implemented differently across the globe; not surprisingly, from a global perspective, the governance of digital health data appears patchy, with only about half of the world health organisation (WHO) countries as depicted in Table 1 and figure 1, having specific privacy protections in place for personal health data. Robust national data governance frameworks tailored to the needs of entire populations are thus considered a precondition for digital health to deliver sustained health benefits and to meet global health objectives [24].

Table 1 – Data Protection Worldwide

Data Protection and Privacy Legislation Worldwide	
Countries with Legislation	137
Countries without Legislation	57
Total	194

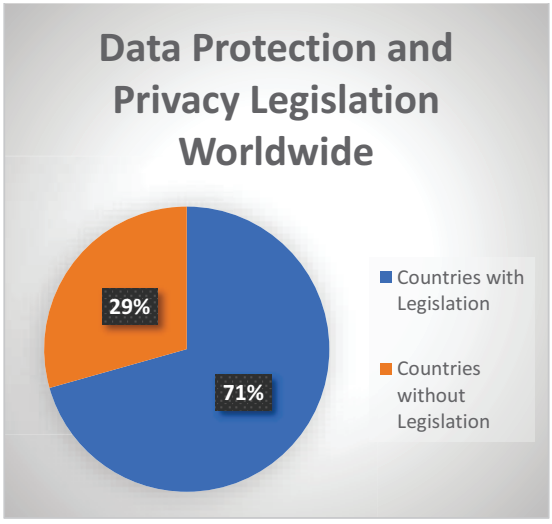

Figure 1 – Data Protection Worldwide

As an increasing number of social and economic activities are digitalised, the importance of privacy and data protection is increasingly recognised, and of equal concern is the collection, use, and sharing of health data. Figure 2 shows that 137(71%) of 194 countries have put in place legislation to secure the protection of data and privacy, while 57(29%) are yet to have legislation in place, according to statistics provided by the United Nations Conference on Trade and Development (UNCTAD) [12].

2. Core Principles of Digital Health Data Protection

In recent years, European countries have implemented new or stricter data protection and cybersecurity laws. These laws continue to substantially impact digital health systems and most public health activities in a broader sense. Notably, data protection is not a rocket science as it requires clearly defined steps to be followed in designing and implementing a digital health system. Equally, data protection is not particularly costly in terms of human resource or technology investments [1] [17] [18].

It is a generally accepted fact core to the heart of the principles of data protection and staring at us, the threatening vista of a digital health data explosion, which for the law, regulatory bodies, and policy analysts looks like an uncontrollable and unmanageable conglomerate, erupting with images lying between an octopus and a volcano. This ominous warning is troubling because of the nature of digital health data that might have to cross borders and come into conflict with more strenuous and cautious governments globally [1] [17] [18].

It is worth noting that over the last three decades, the level of regulation in the field of data protection and cybersecurity has increased, and data protection based on certain principles has also evolved, strengthening digital health systems. Data protection calls for the development and implementation of practices, processes, and procedures, as these will help achieve a maximum level of transparency and democratic legitimacy and ensure strict adherence to IT security standards [25].

D. The State of Digital Health Cybersecurity

Private and public concerns about digital security, cybercrime, and data protection have grown recently. Cybersecurity is defined here as the perceived digital data protection and integrity level. Reducing exposure to cyber risks and promoting best practice security solutions to ensure the confidentiality, integrity, and availability of digital health data when well-articulated and implemented increases resilience [25].

1. Human Factor in Digital Health Data Security

Most modern health organisations rely heavily on digital health. These systems store sensitive health data; therefore, managing the risks of losing these vital health data is essential. Threats to digital health data can come from both external and internal sources. External attacks are typically initiated by hackers seeking political or financial gain. A common way to prevent external attacks is to implement technical security controls, including firewalls, anti-malware software, and authentication controls. Organisations widely employ these measures and are largely effective. On the other hand, an insider threat refers to intentional or unintentional misuse of an organisation's digital health system by employees that may negatively affect the confidentiality, integrity, or availability of vital health data [5] [8].

It is estimated that at least half of health data security breaches are caused by internal personnel. Deviant behaviours are best managed with technical and social measures, ranging from security awareness programs to security education and training approaches that consider deterrent and cognitive

factors. Security countermeasures, including security training, policies, and awareness programs, inform employees about organisational security rules and encourage appropriate behavior [1] [17] [18].

Human factors have always been the weakest link to cybersecurity. For too long, organisations have mandated cybersecurity training for their staff, teaching everyone that security is not just the responsibility of the IT department. However, employee awareness and training can only go so far. For example, a study in the Journal of the American Medical Association found a staggering number of hospital employees falling for phishing attempts; in this simulation, out of three million phishing messages sent, 422,062 or 14% of them were clicked by employees [23].

E. Policy

In its broad sense, a policy is a set of ideas or plans for what to do in any situation, agreed upon officially by a group of people, a business organisation, or a government [1] [17]. Policies always derive authority from legislation that sets their objectives and boundaries. Digital health data protection is a crucial component of the human-centric approach to technology, and a compass for using technology in the digital transition of economies and policymaking [18]. Notably, regulatory pressure has gradually increased over the last decades, forcing the public health sector to adjust its policies and practices regarding enshrining effectiveness in digital health data protection.

A digital health data policy should encapsulate the process or outline steps for end users to optimize health data integrity and data entry practices. Furthermore, it behooves organisations to conduct frequent internal audits and assessments to maintain a high level of digital health data quality and appropriate usage of health data. Finally, it is imperative to state that policies and procedures regarding how devices and employees' access, use, or manage digital health data are critical to contemporary health-system management [23].

F. Digital Health Data Governance

In this context, governance is defined as "the process of distributing authority, power, and influence for decision-making across an organisation's constituencies or structure." These constituencies or structures include the executive board, heads of directorates, heads of departments, IT departments, internal control units, data protection officers, administrators, and other staff members [10].

Digital health data governance helps design, develop, and implement new digital health systems and data protection schemes. Digital health data governance ensures the following:

- Development of a strategy for minimising any implications for data subjects.
- This helps continuously monitor and audit compliance.
- Ensures that health system partners show care and adherence to the required digital health data standards and demonstrate compliance with data protection requirements.

Digital health data governance practices are organisational strategies describing how data is managed throughout its life cycle. These practices comprise three categories: structural, operational, and relational. Additionally, digital health data governance ensures the interface between compliance, IT, and data protection [10].

Digital health data governance helps standardise and ensure that public health authorities effectively manage any risks associated with data protection infringements. From the viewpoint of data, it enables an organisation to realize systematic data standardisation and integrated management, efficient management of health systems, processes, policy formulation, and establishment of encapsulated organisational business processes [10].

It is pertinent to state that strategies must be established together with goals aligned with an organisation's vision and objective to achieve the goals of digital health data governance. Well-aligned digital health data governance will not only mitigate the primary risk because of reputational damage. However, it will ensure that healthcare institutions recognise and mitigate new and emerging risks owing to the transformational influence of digital health systems [10].

G. Risk Assessment

Data protection legislation has globally changed how individuals, organisations, and countries have approached digital health data protection. It increased the onus on organisations to take a proactive approach to data protection, identifying what risks they were creating using data and working to reduce and mitigate them [21] .

The enforcement powers granted to regulatory agencies have helped establish compliance as a board-level issue. Data protection legislation has so far demonstrated that it can work alongside emerging technologies and creative approaches, and it is worth noting that there is no dichotomy between digital innovation and data protection [26].

The essence of the Data Protection Act is to proactively identify and mitigate new or emerging risks arising from technological and societal changes. Therefore, it is pertinent to recognize the interconnected nature of the technological landscape in which digital health operates and the nature of data flows in the expanding digital economy [27].

Data privacy risks relate to unauthorized collection, usage, access, storage, and sharing. These activities might be the reason for personal data leakage and compromise user privacy, particularly concerning health data. In this regard, appropriate protection and security measures are required, and there is no gainsaying that data protection laws are used to protect data and users' privacy. However, these legal frameworks have not produced the intended results. This research examines the scientific, legal, and structural problems of digital health systems in line with digital health data protection concerns [28] [27].

H. Structured Models Framework and AI Algorithm/Machine Learning Models for Healthcare

Health systems are complex adaptive systems; as such, they are characterised by extraordinary complexity in the relationships among highly heterogeneous groups and the processes they create. Systems phenomena of massive interdependencies, self-organizing and emergent behaviour,

non-linearity, time lags, feedback loops, path dependence, and tipping points make health system behaviour difficult and sometimes impossible to predict or manage. Conventional reductionist approaches using research methods are inadequate for tackling the problems posed by health systems [19]. It is increasingly recognised that health systems and policy research need a unique set of approaches, methods, and tools derived from systems thinking perspectives. Health systems encompass a many-tiered system, and evaluating the performance of such a multifaceted structure presents a daunting task [29]. Therefore, mathematical modeling, capable of simulating the behavior of complex systems, is a vital tool to aid the functioning and optimisation of the health system. Research suggests that the healthcare sector generates up to 30% of the global data. Moreover, by 2025, healthcare data will accumulate at a compound annual growth rate (CAGR) of 36%, faster than data from the media and finance. Therefore, AI algorithms in healthcare must increase dramatically to process and make sense of such copious amounts of data.

A digital revolution in healthcare is occurring worldwide. Data explosion has occurred in every facet of our lives, with no end in sight, and data management will become even more significant [29].

III. HYPOTHESIS

The ability to collect, share, and use digital health data is rapidly evolving, and digital health data are produced in various environments with a huge impact. This framework will leverage efficient and effective digital health data protection benefits. During this research, some significant issues around digital health data protection at both national and organisational levels were discovered, and they include but are not limited to the following:

1. In most cases, the absence of legislation or laws that can easily be adaptable for healthcare data protection,
2. The lack of a well-structured cybersecurity framework to guide health organisations on the way forward in ensuring digital health data is protected.
3. A governance framework enshrined within an organisation's structure to promote a culture of ensuring that all digital health data are handled with care and securely.
4. Policies that translate high-level legislation into an easily understood and applicable document.
5. Internal enforcement ensures compliance by implementing policies that support the early detection of inherent vulnerabilities and measures to mitigate identified risks in well-documented and articulated risk-management strategies.

IV. RESULTS

A. Modeling

It is important to point out that, during this research phase, we explored the use of the machine learning approach to address the research problem and questions. We explored multiple Machine Learning models based on the accuracy of the finalised test/validation data, and a support vector machine was selected because of the accuracy of the test/validation data, as shown in Figure 4.

B. Linear Support Vector Model

Support vector machines (SVM) are among the most popular Supervised Learning algorithms for classification and regression problems. However, they are primarily used for classification problems in machine learning. The SVM algorithm aims to create the best line or decision boundary that can quickly segregate n-dimensional space into classes to place the new data point in the correct category. This best decision boundary is called the hyperplane [30]. The SVM chooses the extreme points/vectors that help to create the hyperplane. These extreme cases are called support vectors; hence, the algorithm is termed as a Support Vector Machine.

V. DISCUSSION

If we are given a training dataset of n points of the form.

(X1, Y1),…, (Xn, Yn),

where the Yi are either 1 or −1, each indicating the class to which the point Xi belongs. Each Xi is a p-dimensional real vector. We want to find the "maximum-margin hyperplane" that divides the group of points Xi for which Yi=1 from the group of points for which Yi=-1, which is defined so that the distance between the hyperplane and the nearest point Xi from either group is maximised.

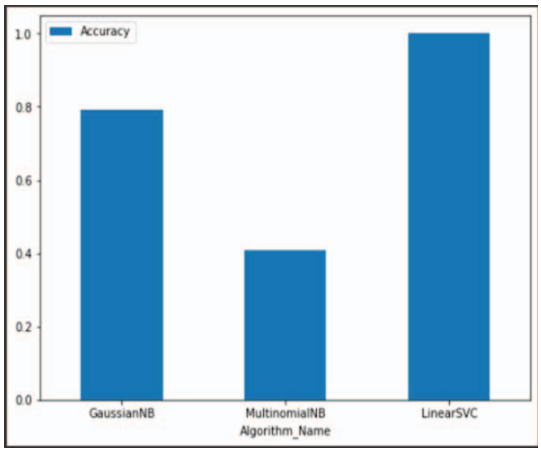

Figure 2 - Validation results

Support vector machines (SVM)) also known as support-vector networks, are supervised learning models with associated learning algorithms that analyse data for classification and regression analysis. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new

examples to one category or the other, making it a non-probabilistic binary linear classifier (although methods such as Platt scaling exist to use SVM in a probabilistic classification setting). SVM maps training examples to points in space to maximize the gap width between the two categories.

Supervised learning is not possible when data are unlabeled. An unsupervised learning approach is required that attempts to find the natural clustering of the data into groups and then map new data to these formed groups. The support vector clustering algorithm, created by Hava Siegelmann and Vladimir Vapnik, applies the statistics of support vectors developed in the support vector machines algorithm to categorize unlabeled data [29]..

A. Linear-Support-Vector-Confusion Matrix

The image below shows that our model (Predicted Label) values are accurately classified compared to the actual values (True Label).

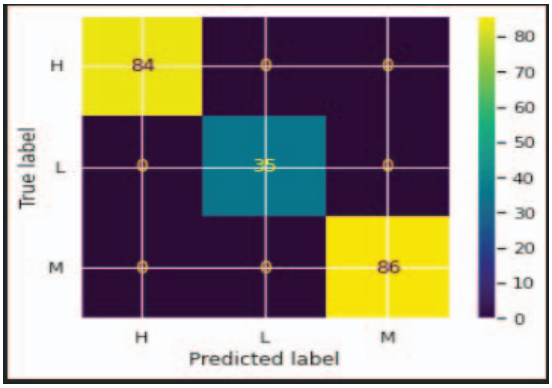

Figure 3 – SVM Confusion Matrix

B. Final Output

Once the risk levels of all the domains are determined, the model can then predict digital health data protection compliance; if all the domains have low risk, then the final output would be compliant else, non-compliant.

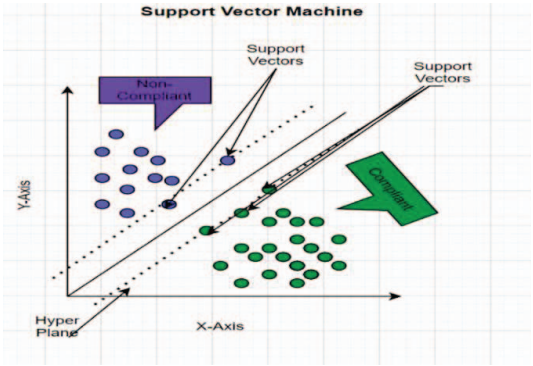

Figure 4 – SVM Representation of DPC

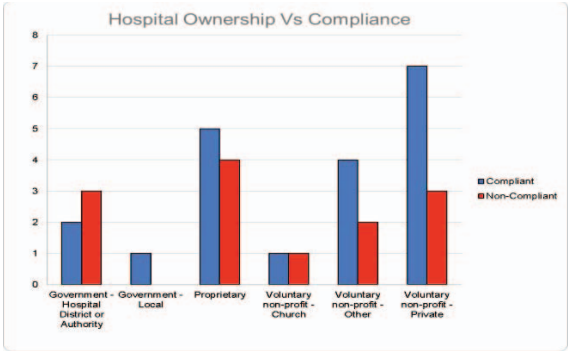

Figure 5 – Hospital Ownership against Data Protection Compliance (DPC)

The preliminary results for the two domains of technology and cybersecurity are shown in Figures 4 and 5, respectively. It is interesting to see how digital health data protection compliance is depicted in figure 6 using the SVM algorithm. Figure 7 shows digital data protection compliance for some hospitals against non-compliance when further classified.

VI. CONCLUSION

In this study, we propose to answer the research questions in designing a digital health data protection framework to leverage the benefits of digital health systems and compliance with data protection requirements, which has been a big challenge for most public health communities and institutions actively managing digital health systems. Therefore, it is essential to demystify data protection and advise setting up measures that fully comply with and serve the digital health community.

Data protection requires legal and technical knowledge; it is not a one-off activity but a continuous effort based on an institutional vision, a governance concept, and a willingness to be accountable [29].

REFERENCES

[1] A. Agrawal, "harnessing digital technologies for better health," *The Lancet,* vol. Vol 398, p. 1678, 2021.

[2] Consumers International, "The State of Data Protection Rules Around the World: A briefing FOR CONSUMER ORGANISATIONS," Consumers International, London, 2018.

[3] EUROPEAN UNION AGENCY FOR CYBERSECURITY, "ENISA SINGLE PROGRAMMING DOCUMENT 2022–2024," Publications Office of the European Union, Luxembourg, 2022.

[4] V. Hordern, "Data Protection Compliance in the Age of Digital Health," *European Journal of health law,* vol. 23, pp. 248-264, 2016.

[5] L. Bari and D. P. O'Neill, "Rethinking Patient Data Privacy in the Era of Digital Health.," Health Affairs, 12 December 2019. [Online]. Available: https://www.healthaffairs.org/do/10.1377/forefront.20191210.216658/full/. [Accessed 20 April 2022].

[6] National Data Guardian, "National Data Guardian for Health and Care - Review of Data Security, Consent and Opt-Outs," Crown, London, 2016.

[7] World Health Organization Regional Office for Europe, "The protection of personal data in health information systems – principles and processes for public health," World Health Organization, New York, 2021.

[8] A. Onumo, A. J. Cullen, and I. U. Awan, "Empirical study of the impact of e-government services on cybersecurity Development," in *Seventh International Conference on Emerging Security Technologies (EST).*, Canterbury, Kent, 2017.

[9] Open Access Government, "Data protection in the healthcare sector," 11 December 2019. [Online]. Available: https://www.openaccessgovernment.org/data-protection-in-the-healthcare-sector/79169/.

[10] L. Marelli, E. Lievevrouwa and I. V. Hoyweghena, "Fit for purpose? The GDPR and the Governance of European Digital Health," *Policy Studies - Taylor & Francis Online,* vol. 41, no. 5, pp. 447-467, 2020.

[11] A. KORNAKIEWICZ, "BIG DATA AND MACHINE LEARNING IN HEALTHCARE - NEW TECHNOLOGIES IN THE SERVICE OF HUMAN," Future Processing Healthcare, 2020. [Online]. Available: https://better.future-processing.com/knowledge/big-data-and-machine-learning-in-healthcare-new-technologies-in-the-service-of-human. [Accessed 10 June 2022].

[12] United Nations Conference for Trade and Development, "Data Protection and Privacy Legislation Worldwide," [Online]. Available: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[13] DELOITTE AND THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO), "2020 Deloitte–NASCIO Cybersecurity Study," Deloitte Development LLC, Washington, 2020.

[14] Identity Theft Resource Center, "First Quarter 2022 Data Breach Analysis: Data Compromises Off to Fast Start; Victim Rates Continue to Drop," The ITRC reports, California, 2022.

[15] E. Vayena, "Value from health data: European opportunity to catalyse progress in digital health," *The Lancet,* vol. 397, pp. 652-653, 2021.

[16] The Lancet Commissions, "The Lancet and Financial Times Commission on governing health futures 2030: growing up in a digital world," The Lancet, vol. 398, pp. 1-2, 2021.

[17] Information Commissioner's Office, "Information Commissioner's Annual Report and Financial Statements 2018-19," Crown, Cheshire, 2019.

[18] Information Commissioner's Office, "Big data, artificial intelligence, machine learning and data protection," Information Commissioner's Office, London, 2017.

[19] S. Bathrinath, R. Bhalaji and S. Saravanasankar, "Analysis of risk factors related to patients in healthcare industry using ISM method," in *AIP Conference Proceedings*, Tamilnadu, India, 2019.

[20] S. Duffy, "Demanding Privacy, and Establishing Trust, in Digital Health," 2019. [Online]. Available: www.cio.com. [Accessed 31 January 2022].

[21] R. P. Medhora, "Data Protection: We need a new era of international data diplomacy - Global standards on collection, storage and use would improve health while protecting privacy," 2021. [Online]. Available: https://www.ft.com/content/66f1ff42-fe49-4376-aafb-3943a9f04a1c. [Accessed 20 November 2021].

[22] P. F. Drucker, Landmarks of Tomorrow, New York: Harper; First Edition, 1959.

[23] Institute of Medicine, DIGITAL DATA IMPROVEMENT PRIORITIES FOR CONTINUOUS LEARNING IN HEALTH AND HEALTH CARE, Washington: The National Academies Press, 2013.

[24] World Health Organization, "World health statistics 2022: monitoring health for the SDGs, sustainable development goals," World Health Organization, Geneva, 2022.

[25] United States of America Cyberspace Solarium Commission, "Cybersecurity Lessons from the Pandemic," CSC Whitepaper, Washington DC, 2020.

[26] E. Henriksen, T. M. Burkow, E. Johnsen and. L. K. Vognild, "Privacy and information security risks in a technology platform for home-based chronic disease rehabilitation and education," *BMC Medical Informatics and Decision Making,* vol. 13, no. 85, pp. 1-13, 2013.

[27] R. P. Medhora, "We need a new era of international data diplomacy," 18 January 2021. [Online]. Available: https://www.ft.com/content/66f1ff42-fe49-4376-aafb-3943a9f04a1c.

[28] The European Union Agency for Cybersecurity (ENISA), "COMPENDIUM OF RISK MANAGEMENT FRAMEWORKS WITH POTENTIAL INTEROPERABILITY: Supplement to the Interoperable EU Risk Management Framework Report," The European Union Agency for Cybersecurity, Athens, 2022.

[29] M. Girnyak, "What AI Algorithms Are Used in Healthcare?" 3 December 2021. [Online]. Available: https://postindustria.com/what-ai-algorithms-are-used-in-healthcare/. [Accessed 20 May 2022].

[30] S. K. DURGESH and B. LEKHA, "DATA CLASSIFICATION USING SUPPORT VECTOR MACHINE," *Journal of Theoretical and Applied Information Technology,* pp. 1-6, 2009.