International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Evolving Privacy Right: An Analysis of Tanzania's Legal Scheme in E-Health Data Protection

Gladness Robert Mkumbo

LLM ICT Law Candidate, Iringa University Tanzania

Abstract

Rapid technological developments and globalization have brought new challenges to the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale to pursue their activities. Natural persons increasingly make personal information available publicly and globally.

The importance of the subject of privacy and data protection has gained unprecedented attention in recent years, requiring better and more elaborate rules of protection. Individuals are sometimes exposed to possible abuse and even to harmful consequences as a result of the developments in information and communication technology (ICT) and the role it plays in the collection of personal information, and the tendency of companies and business enterprises to collect and use personal information in making business decisions. It is therefore not surprising that many countries in the West enacted comprehensive legislation on data protection some time ago. Europe in particular, through the recently passed General Data Protection Regulation, 2016, is heading towards the harmonization of data protection laws to have consistency within the region

This article aims to provide an overview of the evolving "right to privacy (Data protection)" in this digital health (e-health) world to give the main key facts to stakeholders in e-health sectors to adapt their practices and ensure compliance with the current evolving legal scheme in Tanzania. The processing of personal health data, genetic data biometric data, and other kinds of sensitive information is strictly regulated and even widely interpreted by justice-dispensing organs.

Keywords: Data Protection, Personal Data Protection, E-Health, Processing of Personal Health Data, Legal Scheme, Data Protection Legislation, Legal Scheme, Tanzania

1. INTRODUCTION AND SCOPE

Introduction

As technological advances accelerated, the legal frameworks of data protection evolved. Data protection is terminology derived from the "right to privacy".[1] In Tanzania, data privacy is a constitutional right,[2]

[1] Tobias Schulte et al, The protection of personal data in health information systems – principles and processes for public health. Copenhagen, at pg. 2: In 1890, two American lawyers, Samuel D. Warren and Louis Brandeis, wrote "The right to privacy", an article that argues that individuals have a "right to be left alone", using the phrase as a definition of privacy.

[2] Article 16 of the Constitution of United Republic of Tanzania of 1977, [CAP 2 of the Laws of Tanzania]

however, since the enactment of the Personal Data Protection Act, of 2022, substantively; personal data (including e-health data) have been protected under the aforementioned law, and procedures for enforcing the same.[3]

The right to privacy in the digital world is tremendously evolving to cover issues of "pass off", and confidentiality of trade secrets.[4] However, when it comes to the health sector, "privacy" is an ethical duty to health practitioners; it is a statutory duty, that attracts both professional disciplinary actions and civil wrongs.

In the health sector, practitioners are duty-bound statutorily, and eternally not to disclose personal health information unless so required by law.[5] Briefly, personal health data in the e-health context entails personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;[6]

Considering the health sector is rapidly growing, there is a growing legal consideration regarding regulating the use of technology in healthcare. Along with confidentiality, privacy, and security, other issues include changes to the standard of care using electronics rather than paper medical records, user training, and ensuring accurate information is provided to the user.[7]

This article aims to explore the evolving concept of "data privacy" and to give some guidance on how specific decisions that are unavoidable to balance the rights and interests at stake should be taken.

2. THE CURRENT E-HEALTH DATA PROTECTION SCHEME IN TANZANIA.

2.1 Introduction

Tanzania has been undertaking reforms in data protection legal framework, by putting in place cyber and other related laws. The landmark legal amendments introduced the legal provisions that allow and recognize the admissibility of electronic evidence through the amendments of Evidence Act No. 15 of 2007, Act No. 3 of 2011, and other amendments. Further, the Government enacted the Electronic and Postal Communications Act No. 3 of 2010; the Universal Communications Service Access Act. No. 11 of 2006, the Cybercrime Act No. 14 of 2015, the Electronic Transactions Act No. 13 of 2015,[8] and now the Personal Data Protection Act, 2022. Various other Regulations were made under these Acts to promote electronic communications, and consumer protection, and to address cyber security issues.

Currently, Tanzania does not yet have a specific law, addressing legal issues arising as a result of using e-health. As such, the existing privacy and data protection requirements in Tanzania are to be found to varying degrees in various pieces of legislation even after the enactment of The Personal Data Protection Act, 2022.

[3] Multichoice (T) Ltd v Alphonce Felix Simbu & two others, Comm. Appeal No. 01 of 2023, in the High Court of Tanzania (Commercial Division), at Arusha: available at https://tanzlii.org/akn/tz/judgment/tzhccomd/2023/344/eng@2023-10-13

[4] Ibid (n3), pg. 26-27

[5] Rule 4 of the Code of Ethics and Professional Conduct for Medical and Dental Practitioners 2005, Section 57 of the Medical, Dental, and Allied Health Professionals Act; Section 65 (1) of the Human DNA Regulation Act [Act No.80 of 2009].

[6] Article 4 (para 15) of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.

[7] Suhaib Hammad, Digital Health Laws and Regulations, Saudi Arabia, (2023), available at https://iclg.com/practice-areas/digital-health-laws-and-regulations/saudi-arabia

[8] National Information and Communications Technology Policy, 2016; pg. 5

2.2 Other Domestic Laws Governing E-Health Data Protection in Tanzania

Several laws are broadly construed to regulate digital health privacy too; these laws were there before the enactment of the Personal Data Protection Act, of 2022:

2.2.1. The Constitution of the United Republic of Tanzania of 1977

According to Article 16 (1)[9] provides that

''Every person is entitled to respect and protection of his person, the privacy of his person, his family and of his matrimonial life, and respect and protection of his residence and private communications.''

According to Article 16, an individual has a right to privacy in his person, family, and matrimonial life. Currently, Tanzania has no comprehensive data privacy legislation that would give effect to the constitutional right to privacy. However, there is a Personal Data Protection Bill, which has been pending since 2014, whose section 9 prohibits the processing and further processing of previously collected personal data unless the data subject authorizes the processing or data processing is provided by law or data is processed about the purpose of collection. Similarly, the Bill prohibits in section 10 (1) disclosure of already collected data to anyone except the data subject. There are only a few exceptions that permit disclosure such as where a data subject has expressly or implicitly consented or under the compulsion of the law or if it is disclosed about the purpose of collection. Nevertheless, the pending draft Personal Data Protection Bill does not sufficiently provide for the processing of health data, which is a concern of e-health applications.

2.2.2. The Medical, Dental, and Allied Health Professionals Act

This is an act that establishes the Allied Health Professions Council, the Medical and Dental Council, the Nursing and Midwifery Council, the Pharmacy Council, and the Psychology Council and provides for related purposes. [10]The code among other things provides for the principle of confidentiality about medical, dental, and allied health.

2.2.3. The HIV and AIDS (Prevention and Control) Act

In 2008 Tanzanian Government enacted the HIV and AIDS (Prevention and Control) Act of 2008. The Act is very comprehensive, covering all aspects of HIV and AIDS prevention, treatment, and community response[11].

An Act to provide for prevention, treatment, care, support, and control of HIV and AIDS, for promotion of public health about HIV and AIDS; to provide for appropriate treatment, care, and support using available resources to people living with or at risk of HIV and AIDS and to provide for related matters.

Section 16 of the Act provides about the confidentiality principle in regards to the HIV results and section 17 provides about the same principle but about medical confidentiality in dealing with the victim of HIV. Therefore, this Act protects data privacy in E-Health but it has dealt only with the victims of HIV/AIDS

2.2.4. The Cybercrimes Act

The Cybercrimes Act, of 2015 is a penal statute intended to deter or discourage privacy and data protection abuses and violations. Being a penal statute, the application of the Cybercrimes Act is not restricted as long as the offenses were committed within the United Republic of Tanzania, including on vessels or aircraft registered in Tanzania. The Act would also apply to Tanzanian nationals residing abroad if the act committed is an offense both in Tanzania and under the laws in the host country. Further, the Act applies to any person, regardless of nationality, if the abuse or violation (i) is committed using a computer

[9] The Constitution of the United Republic of Tanzania of 1977, [Cap 2 of Laws of Tanzania as amended from time to time]
[10] The long tittle of The Medical, Dental and Allied Health Professionals Act
[11] The HIV and AIDS (Prevention and Control) Act, [Act No 28 of 2008]

system, device, or data located within Tanzania; or (ii) is directed against a computer system, device, data or person located in the Republic. Therefore, the Act applies to e-health crimes.

2.2.5. The Human DNA Regulation Act, 2009

This is an Act[12] enacted by the parliament of the United Republic of Tanzania to provide for the management and regulation of the collection, packing, transportation, storage, analysis, and disposal of samples for Human DNA, disclosure of genetic information, and research on Human DNA and to provide for related matters. [13]The Act provides for the principle of confidentiality under 64(1) which provides that: -

‘‘Any person who receives or accesses private genetic information in the performance of his duties or the cause of his employment shall keep such information confidential and shall not divulge it to anybody or make use of it during or after the tenure of employment without the written authorization of the sample source or the sample source representative.’’

Also, the Act provides about the Non-Disclosure of genetic information, this is under section 65(1) which provides that;

The Regulator shall not disclose any genetic information obtained and kept under this Act, except to

(a) The criminal investigation section of police in the course of criminal investigation or proceedings;

(b) The person from whom the genetic information was extracted and such genetic information is requested for his defense; and

(c) A country-making request, which is accepted by the Attorney General for mutual assistance in criminal matters under the provisions of the Mutual Assistance in Criminal Matters Act.

The provision went further and provides for the punishment in case of contravening the said provision to a fine of three million shillings or imprisonment for a term of two years or both.

2.2.6. The Code of Ethics and Professional Conduct for Medical and Dental Practitioners 2005

According to Rule 4.0 provides about the principle of privacy that, this principle is based on the concept that records, interests, and affairs relating to the client’s health condition are confided to the practitioner only. Further Rule 4.1 provides that respect the privacy of a client in the course of providing treatment and any other forms of interaction and shall avoid acts that are degrading, insulting, interfering with, or injuring the self-value of the client. Through the two rules, the code protects privacy and data in the health sector the problem with the code is outdated when created hospitals in Tanzania were not using the E-Health system.

2.3 The New Legal Regime Under the Personal Data Protection Act, 2022

2.3.1 The Personal Data Protection Act

This is the general Act, which provides for principles of protection of personal data to establish minimum requirements for the collection and processing of personal data; to provide for the establishment of a Personal Data Protection Commission; to provide for improvement of protection of personal data processed by public and private bodies; and to provide for matters connected therewith[14].

The Act is divided into nine (9) parts, that is Part I – Part IX. Whereas, for this article, the following parts of the Act are of utmost importance.

[12]The Human DNA Regulation Act [Act No.80 of 2009]
[13] The long title of The Human DNA Regulation Act 2009
[14] The Personal Data Protection Act, 2022

Part I: Interpretational part, this is an important part of the Act that contains guiding terms and principles that are to be used when there is a need to interpret the Act itself.
Part II: Provides for an Institutional and regulatory framework, under this part the Personal Data Protection Commission is established, and its governing Board is vested with power to oversee data protection and matters related thereto.
Part III: This part contains control measures towards "data controllers and data processors." The part introduces the registration compliance requirement to any person termed as a data controller, or data processor[15] before the kick-off of their operational activities. This is what is considered a "green light controlling mechanism."[16] Under this part, the Act deploys prior controlling measures in "data protection."
Part IV: contains what is the so-called "operational measure" deployed by the Act to protect personal data. This part contains minimum standards that ought to be observed by key players in e-health at the time of collecting, using, disclosing, and retention of e-health personal data. It is illegal to befall beyond them, but permissible to go beyond them.
Part V: Contain conditional precedent to meet in cross-border data transfer. The same applies to e-health personal data such as those derived under "Health Insurance Policies" that can be enjoyed by data subjects in several countries. However, this part falls short of adequate controlling measures in cross-border data transfer as it does not mandatorily require key players in cross-border data transfer to obtain approval from relevant authorities before doing so[17].
Part VI: the part contains rights of data subjects, although, the Act considers them as minimum rights to be observed, but the is not structured in harmony with another right such as "confidentiality" as discussed by Agatho, J in **Multichoice (T) Ltd case**.[18]
Part VII: provides for an enforcement Mechanism for the victimized data subjects, which in the theoretical aspect is termed a "red light control mechanism."[19] The available mechanism is still not adequate as discussed in Schrem's case.[20]

2.3.2 The Short Falls of New Legal Regime Under the Personal Data Protection Act, 2022 Compared to the Modern Legal Regimes in Data Protection

The falls short of having legal pre-market requirements on electronic devices, and wearables, mobile phone software to acquire pre-market approval from relevant authorities before the same is shipped within the domestic market for consumption.[21]
Yet, the Act does not provide for the obligations shouldered to the data controller to have internal mechanisms or personnel responsible to safeguard or offer protection of personal data, as it was on the Final version of the Proposed Personal Data Protection Bill.[22]

[15] Section 3 The Personal Data Protection Act, 2022 provides for the definition of Data Controller, and data processor.
[16] Aberham Y. et al, Administrative Law: Teaching Material, (Ethiopia Justice and Legal System Research Institute Publisher 2009): pg. 14-16
[17] See section 32 (5) of the Personal Data Protection Act, 2022
[18] Agatho, J. in the case of Multichoice (T) Ltd v Alphonce Felix Simbu & two others, Comm. Appeal No. 01 of 2023, in the High Court of Tanzania (Commercial Division), at Arusha: available at https://tanzlii.org/akn/tz/judgment/tzhccomd/2023/344/eng@2023-10-13 : Accessed on 24/10/2023
[19] See Red light theory (n16)
[20] Schrems case, which, amongst other things provides a detailed discussion of enforcement, and protection measures that can be adopted by state where there is cross-border violation of personal data.
[21] Part III of the Personal Data Protection Act, 2022, only regulate registration of key players dealing with personal data, but the Act does not provide for measure to regulate devices and software used in processing, storing and retention of personal data.
[22] Part V, and Part VI of the Data Protection and Privacy Model Bill (Final version)

Further, the Act does not have adequate enforcement, and redressing mechanisms against violation of data privacy as discussed in the **Schrems case**[23].

The Act falls short of addressing post-surveillance measures to be adopted by both regulatory authorities, and data controllers that will ensure adequacy in data protection, these measures include Data Controllers submitting a market Surveillance Plan, Periodic Safety Update Report, and Post Market Surveillance Report to the relevant regulatory authority.

Yet, unlike how it was on the final version of the Proposed Personal Data Protection Bill,[24] the Act falls short of harmonizing provision, which harmonizes the Act with other written laws.

3. THE MODERN DATA SUBJECT's LEGAL PROTECTION MECHANISM

3.1 Modern Data Protection Laws

Modern data protection laws aim to empower citizens to exercise their rights in a world increasingly dominated by technology companies and other players that process vast amounts of data relating to citizens. The empowerment of citizens is equally important in the context of medical care and similar health-related settings, such as end-of-life decisions.[25]

The rights of data subjects are, as in the medical setting, intrinsically linked to the principle of transparency, as only educated and empowered citizens are capable of exercising their rights. Responsibility for adherence to the rights of data subject's rests with the data controller. As such, the data controller is also obliged to ensure that any data processor – or, in case of a controller-to-controller transfer, any data recipient – honors the rights of data subjects.[26]

Therefore, as Modern data protection laws aim to empower citizens to exercise their rights, that means a huge burden of liability awaits stakeholders in the e-health sector, for the reason that data protection laws are still evolving; and on several occasions, we have witnessed Tanzanian Jurisprudence borrowing leaves of legal principles from European countries, and sometimes United States of America. This is a case in instances where the court is faced with claims that are not addressed by our domestic laws, thus the court is forced to borrow principles from common law countries[27]. The true reality of the incoming liability can be drawn from the recent claims of violation of privacy rights in Tanzania.[28]

Yet, even though, Tanzania has adopted the Personal Data Protection Act, 2022; the Act falls short of necessary modern measures, which accord a balance between protection of data subject's right to privacy and the right to access health service.

---

[23] Data Protection Commissioner v Facebook Ireland and Schrems, European Court of Justice (Grand Chamber), CASE C-311/18, ECLI:EU:C:2020:559, pg. 40-45

[24] Section 75 of the Data Protection and Privacy Model Bill (its marginal note titled "relationship with other Acts")

[25] Tobias Schulte et al, The protection of personal data in health information systems – principles and processes for public health. Copenhagen, at pg. 8

[26] For details, see: Voigt P, von dem Bussche A. Rights of data subjects. In: The EU General Data Protection Regulation (GDPR). Cham: Springer; 2017: 141–87.

[27] Section 2 (3) of The Judicature and Application of Laws Act, [CAP 358 R.E 2019 of the Laws of Tanzania]

[28] Several case have been instituted in courts of law recently, even before the enactment of the Personal Data Protection Act, 2022; see Jamii Media Company Ltd v. The Attorney General (2017) TLS LR 447; Deogras John Marando v Managing Director, Tanzania Beijing Huayuan Security Guard Service co. Ltd, High Court of Tanzania, Civil Appeal No 110 of 2018 (unreported); Raymond Paul Kanegene and Bob Chacha Wangwe v The Attorney General, High Court of Tanzania, Consolidated Misc. Civil Cause No. 15 OF 2019 & No. 5 OF 2020; Kisonga Ahmed Issa & Another Vs. Republic, Court of Appeal of Tanzania, Consolidated Criminal Appeal No. 17 of 2016 and 362 of 2017, and in Francis Nyandindi v Republic, High Court of Tanzania (at Dar es Salaam), Criminal Appeal No. 173 of 2021, (unreported); available at https://www.dataguidance.com/notes/tanzania-data-protection-overview (Accessed on 02/11/2023)

3.2 Modern Protection Measures (Best Practices Adopted in Data Protection in E-Health)

Thus, for there to be a balance between the right to privacy, and the right to health access, several countries including the European Union, are adopting measures that promote equal enjoyment of the two rights; the following measures have been adopted;

3.2.1 Adoption of Prior and Post-Effective and Adequate Regulatory Schemes Domestically, Which Safeguard Personal Data

The Kingdom of Saudi Arabia serves as the best country having pre-regulatory schemes embarked to protect personal data, especially health data.[29] The Kingdom embarked on the following;

Integrated Regulatory Authorities responsible for overseeing the health sector (Saudi Food and Drugs Authority), and their national authority overseeing information technology (The Communication and Information Technology Commission; the Saudi Data and Artificial Intelligence Authority; National Data Management Authority). All these four Authorities assist one another when it comes to issues of "personal data protection".

Established a regulatory requirement for all software, and all Artificial Intelligence (AI) to be used in the health sector to obtain prior approval from the Saudi Data and Artificial Intelligence Authority. In so doing the regulatory authority requires the software developer, or AI developer to submit technical specifications used in developing this software or AI, security measures available within the software itself, and also post measures that can be employed by a user of the software to continually monitor the software security once in operation, these are some of few things.

For all Medical devices such as telemedicine, wearables, robotics, Virtual assistance such as Alexa, Mobile Apps, and a list of them; needs to obtain prior-market approval from Saudi's Food and Drugs Authority. The Saudi Food and Drugs Authority has issued a guideline of what to do[30] by importers of the aforementioned things in Saudi Arabia before the same can be consumed in the Saudi Market.[31]

Whereas when it comes to post measures, the European Union through the case of **Schrems case**[32], which among other things, contains a detailed discussion of how a state can redress victimized data subjects against:

Standard forms contractual clauses, which are mostly used to abuse data privacy right and yet limits the liability of offenders.

Cross-border data transfer to third countries, which have laws shielding those countries in instances of an abuse of data privacy rights. The case urges regulatory authorities to look into looking onto different factors, not only an assurance from the state itself that it can safeguard the exported personal data, but the state authority shall satisfy itself regarding relevant provisions of the law applicable in the state where personal data are about to be exported.

---

[29] Suhaib Hammad, Data Protection Laws and Regulations, Saudi Arabia, (2023), available at https://iclg.com/practice-areas/data-protection-laws-and-regulations/saudi-arabia (accessed on 16/10/2023)

[30] Premarket Review Considerations criteria used by Saudi Food and Drugs Authority includes, Device Description and Specification, Including Variants and Accessories. Information to be provided by the Manufacturer. Design and Manufacturing Information. Essential Principles of Safety and Performance. Benefit-Risk Analysis and Risk Management. Product Verification and Validation. Post Market Surveillance Plan. Periodic Safety Update Report and Post Market Surveillance Report

[31] The Saudi Food and Drugs Authority, Guidance on Artificial Intelligence (AI)and Machine Learning (ML) technologies based Medical Devices, issued on November 29, 2022.

[32] Data Protection Commissioner v Facebook Ireland and Schrems, European Court of Justice (Grand Chamber), CASE C-311/18, ECLI:EU:C:2020:559, pg. 40-45

The case further urges lawmakers at the national level to enact provisions, which enable state Authorities such as "the Personal Data Protection Commission" to pursue claims against external infringement on data privacy on behalf of a data subject whose right has been infringed.

Yet, the case extends the room for redress by laying down another remedy for the data subject whose right to privacy was infringed by third countries, and the State Authority has negligently pursued his remedy for the violation, to sue such state authority under national laws and ask for redress from such national authority.

Last but not least, the case comments on the need to have an internal "data protection officer" within any institution, which is in law termed a "data controller". Something that "the Personal Data Protection Act" does not provide for as a minimum requirement.

Now, about the above-discussed criteria available in other jurisdictions, The Personal Data Protection Act falls short of addressing several important things so that it can adequately safeguard personal data not only in e-health but also in other sectors,

3.2.2 Adoption of Operational Safeguarding Measures

Health facilities and other stakeholders engaged in health provision (including but not limited to, public and private registered health facilities, e-health software programmers, e-health app developers, and e-health devices manufacturers) which are in law termed as data controllers and data processors are highly advised to;

1. conduct a risk assessment on e-health systems before adoption of the e-health system, and how to establish a better cyber security system in an established e-health software[33]
2. Seek clear consent from the data subject before the acquisition of data, and clearly, state to what extent the data acquired will be used, and shared.
3. Clearly state any risks or data breaches that may occur on the retrieved data.
4. Ensure that IT systems facilitate adherence to data subject requests (such as deletion of data).
5. Develop a communication strategy on any reasons for turning down data subject requests.
6. Develop a market Surveillance Plan for the installed health system.

Conclusion:

Generally, for there to be a balance between "data protection" and the right to health access, there is no hard and fast rule to adhere to, after a thorough study, what is advised is that, from each e-health context, stakeholders thereto are advised;Study the whole chain of data applicable in the particular context, and pinpoint all key players in the chain, Develop data protection compliance measures for each key player, Conduct a risk assessment on e-health systems before adoption of the e-health system, and how to establish a better cyber security system in an established e-health software Develop a market Surveillance Plan on the installed health system Deploy measures to monitor the installed e-health system, such as having in place a data protection officer.

[33] Recital 77 of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, which directs Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

Put into place internal redressing mechanisms on the claims of violation of privacy.

BIBLIOGRAPHY

Legal Instruments

1. The Code of Ethics and Professional Conduct for Medical and Dental Practitioners 2005
2. The Constitution of the United Republic of Tanzania of 1977[CAP 2 R.E.2002]
3. The Cybercrimes Act [Act No.14 of 2015]
4. The HIV and AIDS (Prevention and Control) Act [Act No 28 of 2008]
5. The Human DNA Regulation Act 2009
6. The Judicature and Application of Laws Act, [CAP 358 R.E 2019]
7. The Medical, Dental, and Allied Health Professionals Act [Act No 11 of 2017]
8. The Personal Data Protection Act [CAP 44 of 2022]
9. The REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

Policy & Guidelines:

1. The National Information and Communications Technology Policy, 2016
2. The Saudi Food and Drugs Authority, Guidance on Artificial Intelligence (AI)and Machine Learning (ML) technologies based Medical Devices, issued on November 29, 2022.

Books & Articles:

1. Abraham Y. et al, Administrative Law: Teaching Material, Ethiopia Justice and Legal System Research Institute Publisher (2009).
2. Tobias Schulte et al, The protection of personal data in health information systems – principles and processes for public health. Copenhagen, (2021).
3. Voigt P, von dem Bussche A. Rights of data subjects. In: The EU General Data Protection Regulation (GDPR). Cham: Springer; (2017)

Websites:

1. https://www.dataguidance.com/notes/tanzania-data-protection-overview
2. Suhaib Hammad, Data Protection Laws and Regulations, Saudi Arabia, (2023), available at https://iclg.com/practice-areas/data-protection-laws-and-regulations/saudi-arabia
3. Suhaib Hammad, Digital Health Laws and Regulations, Saudi Arabia, (2023), available at https://iclg.com/practice-areas/digital-health-laws-and-regulations/saudi-arabia

Bills & Case Laws:

1. Data Protection Commissioner v Facebook Ireland and Schrems, European Court of Justice (Grand Chamber), CASE C-311/18, ECLI:EU: C:2020:559
2. Deogras John Marando v Managing Director, Tanzania Beijing Huayuan Security Guard Service Co. Ltd, High Court of Tanzania, Civil Appeal No 110 of 2018 (unreported);
3. Francis Nyandindi v Republic, High Court of Tanzania (at Dar es Salaam), Criminal Appeal No. 173 of 2021, (unreported)
4. Jamii Media Company Ltd v. The Attorney General (2017) TLS LR 447;
5. Kisonga Ahmed Issa & Another Vs. Republic, Court of Appeal of Tanzania, Consolidated Criminal Appeal No. 17 of 2016 and 362 of 2017, Multichoice (T) Ltd v Alphonce Felix Simbu & two others, Comm. Appeal No. 01 of 2023, in the High Court of Tanzania (Commercial Division), at Arusha: available at https://tanzlii.org/akn/tz/judgment/tzhccomd/2023/344/eng@2023-10-1

6. Raymond Paul Kanegene and Bob Chacha Wangwe v The Attorney General, High Court of Tanzania, Consolidated Misc. Civil Cause No. 15 OF 2019 & No. 5 OF 2020;
7. The Data Protection and Privacy Model Bill (Final version)