

Merle Freye, Dennis-Kenji Kipker, Ezekiel Rindstone, Doreen Mwamlangala¹

Strengthening protection of personal data in the health sector: a comparative analysis of the Tanzanian and German eHealth system

Digitalisation is revolutionising medicine and rapidly spreading in the health sector. eHealth is gaining increasing importance in Tanzania as well as in Germany. This does not only concern awareness of patient rights and more transparency, but also essential questions of data protection and the technical-organisational security of data processing. In an attempt to

deal with this process the German legislator has just published the draft Patient Data Protection Act (PDSG-E) in April 2020.² The following observations will highlight the technical challenges associated with the digitalisation of healthcare on the example of electronic health records (EHR), medical telematics and in the broadest sense eHealth, in a comparison of German and Tanzanian law, and discuss the regulatory requirements derived from this by the legislator.

1 eHealth – a worldwide phenomenon that knows neither boundaries nor rules

EHR are hailed as the key to increasing the quality of care, but as exciting and beneficial as EHR sound, they also raise a number of technical and legal issues: While EHR promise the security of protected digital access, in theory requiring fewer structural or physical protective measures than paper records, the networking of patient data within the framework of a telematics infrastructure (TI) involves considerable problems and risks, which are difficult to control. This does not only require the legislator to establish high protective standards at an abstract level, the legal requirements must also be consistently implemented by medical practitioners and operators of the TI. The example of the German EHR and the related TI shows that this may entail grave data protection and data security problems despite years of careful planning. At the end of 2019, German IT security experts found that the technical components for the application and safeguarding of the EHR and the TI suffered from serious technical problems and, even worse, that their availability was not (sufficiently) restricted and thus access to



Merle Freye

Research Assistant and PhD Student at the Institute for Information, Health and Medical Law (IGMR), University of Bremen

E-Mail: mfreye@uni-bremen.de



Dr. Dennis-Kenji Kipker

Scientific Director of the IGMR at the University of Bremen. Member of the Board of the European Academy for Freedom of Information and Data Protection (EAID) in Berlin. Legal Advisor at VDE e.V. in Frankfurt (Main), CERT@VDE. Managing Director of

Certavo GmbH – international compliance management.
E-Mail: dennis.kipker@certavo.de



Dr. Rindstone B. Ezekiel

Dean, Faculty of Law, The Open University of Tanzania

E-Mail: rindstone.ezekiel@out.ac.tz



Dr. Doreen F. Mwamlangala

Lecturer, The Open University of Tanzania

E-Mail: doreen.mwamlangala@out.ac.tz

¹ The authors would like to thank the Alexander von Humboldt Foundation for its support in making this paper possible. See the end of this article for details.

² Available at: <https://www.bundesgesundheitsministerium.de/pdsg.html> (last accessed April 6, 2020).

the secure network was theoretically open to anyone.³ Similarly, the use of eHealth in Tanzania is double-edged as well. On the one hand, the adoption of eHealth services responds to the constraints of the physicians per capita rate, which currently stands at 0.02 per 1,000 people.⁴ eHealth has been adopted with the view of addressing the problems of limited health infrastructure such as shortage of X-ray, MRI, CT-Scan and ultrasound, which have made health service delivery more difficult especially in rural areas. By March 2018, Tanzania managed to integrate digital health services in 1303 health centers through the Digital Health Investment Recommendations Roadmap programme.⁵ On the other hand, experiences from Zanzibar, a semi-autonomous part of Tanzania, show that patients' health information is shared from lower to referral hospitals online through emails or WhatsApp messages.⁶ These include X-ray, medical and laboratory reports, etc, which leads to data protection and security questions.

eHealth bridges the gap and improves health service delivery within those constraints. Nevertheless, the absence of an adequate legal and regulatory framework for the protection of personal records fuels data protection and data security problems in Tanzania as well as in Germany.⁷

2 Data protection framework conditions and challenges

2.1 General law

Data protection in healthcare is an important component of confidence-building between patients and service providers and thus an essential requirement for a functioning healthcare system. This is above all due to the special characteristics of health data, which require particular protection. Health data contain highly personal information about the patient concerned and are thus associated with an enormous potential for discrimination. Mostly, they also have a multipolar function since medical care involves a large number of service providers and thus to a considerable extent third parties in the processing of the data.⁸ It is therefore hardly surprising that eHealth and in particular EHR have to be considered in the light of the particular sensitivity of health data and require extensive data protection. The actual implementation of this is faced with yet unresolved problems and, what is more, still in its infancy.

The starting point for the data protection framework regarding eHealth and in particular the EHR in Tanzania and Germany is the principle of medical confidentiality. The latter means that

personal and medical information given to a health care provider will not be disclosed to others unless the individual has given specific consent for such release.

In Germany, medical confidentiality is regulated by professional law (§ 9 Professional Code for Physicians (MBO-Ä)) and criminal law by § 203 Criminal Code (StGB). Due to the right to refuse to give evidence, medical confidentiality is guaranteed in criminal procedural law as well, § 53 (1) No. 3 Criminal Procedure Code (StPO). Equally, in Tanzania § 41 of the Medical, Dental and Allied Health Professionals Act, 2017, the Code of Ethics and Professional Conduct for Medical and Dental Practitioners 2005, § 64 of the Human DNA Regulation Act 2009 and §§ 16 and 17 of the HIV and AIDS (Prevention and Control) Act 2008 contain provisions that regulate medical confidentiality. Moreover, in Tanzania medical confidentiality is safeguarded by the general principle of duty of care on the part of health practitioners, a breach of which may attract a claim based on the tort of negligence in the area of breach of duty of care.⁹ It is noteworthy that the regulations of data protection law and the principles of medical confidentiality are very similar as regards their protective purpose and general design, and the diverging views are therefore only of relevance in a very limited number of cases.

The second cornerstone of any eHealth system is data protection law. The basic principle of data privacy law is not the freedom of the processing of personal data, but its prohibition. In Tanzania, data privacy law has its basis in the Constitution since Tanzania has not ratified the African Union Convention on Cyber Security and Personal Data Protection 2014, the only binding international treaty on data protection outside Europe. According to Article 16 of the Tanzanian Constitution, an individual has a right to privacy of his own 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 authorises the processing or data processing is provided by a law or data is processed in relation to 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 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 in relation to the purpose of collection. Nevertheless, the pending draft Personal Data Protection Bill does not sufficiently provide for the processing of health data, which is the concern of eHealth applications.

Since 2016, Germany is bound by the General Data Protection Regulation (GDPR). According to Art. 6 (1) GDPR, the processing of data and also the further processing of data already collected are generally prohibited, unless the data subject has effectively consented to the processing (Art. 6 (1) lit. a GDPR) or one of the other legal bases provided for by Art. 6 (1) lit. b-f GDPR applies. With regard to the processing of health data, which eHealth applications are mainly concerned with, the principle of prohibition is again expressly laid down in Art. 9 (1) GDPR. However, Art. 9 (2) GDPR provides for numerous legitimations for data processing – in particular in the health sector (Art. 9 (2) lit. h, i GDPR).

3 See Maus, "Hinweise auf mögliche Verwundbarkeiten der Medizin-Telematik", c't 17.01.2020, available at: <https://www.heise.de/ct/artikel/Hinweise-auf-moegliche-Verwundbarkeiten-der-Medizin-Telematik-4635791.html> (last accessed March 18, 2020).

4 The World Bank, "Physicians (per 1.000 people) – Tanzania", available at: <https://data.worldbank.org/indicator/SH.MED.PHYS.ZS?locations=TZ&display=graph--%3E> (last accessed March 31, 2020).

5 ICT & Telecom, "Germany grants Tanzania €8 mln to improve ICT use in the health insurance system", *ecofinagency.com* 22.10.2019, available at: <https://www.ecofinagency.com/telecom/2210-40594-germany-grants-tanzania-8mln-to-improve-ict-use-in-the-health-insurance-system> (last accessed March 30, 2020).

6 Deliberations at a workshop on "Strengthening protection of personal data in the health sector: a comparative analysis of the Tanzanian and German eHealth system" held on 09.08.2019 at the Open University of Tanzania, Zanzibar Regional Centre.

7 Msumi, DuD 2018, 373.

8 Weichert, in: Kühling/Buchner (eds.), DSGVO/BDSG (2nd edition 2018), Art. 9 marginal no. 38.

9 See e.g. High Court of Tanzania, Theodelina Alphaxad a Minor S/T Next Friend Vs the Medical Officer I/C, Nkinga Hospital, 1992, TLR 235.

2.2 Specific eHealth law

As mentioned in 2.1 above, there are some specific laws in Tanzania that provide for privacy in health-related issues. These include the HIV and AIDS (Prevention and Control) Act 2008 and the Human DNA Regulation Act 2009. The HIV Act generally provides in section 16 that medical specialists may not breach medical confidentiality or disclose information about persons' HIV or AIDS status unless in case of applicable exception. This provision is reinforced by section 17 which states that all health practitioners, workers, employers, recruitment agencies, insurance companies, data recorders, sign language interpreters, legal guardians and other custodians of any medical records, files, data or test results shall observe confidentiality in the handling of all medical information and documents, particularly the identity and status of persons living with HIV and AIDS. Correspondingly, the Human DNA Regulation Act 2009 regulates the disclosure of personal information relating to human DNA in section 52 to 65. The existing legal and regulatory framework imposes obligations upon medical practitioners which are very general. These include obligations of obtaining consent of patients and non-disclosure of medical records. However, these requirements are not adequate in ensuring the protection of health records in eHealth settings.

In Germany, eHealth is first of all regulated by social data protection law, which includes the regulations on the electronic health card (EHC) and on the electronic health record (EHR). While the current EHC is designed as proof of insurance and only stores few data (§ 291 (2) SGB V), the future EHR will be a collection of patient health information in a digital format, which can be shared across different healthcare settings.

On 1 January 2004, the Health Care Modernization Act introduced the EHC as a so-called "Lighthouse Project"¹⁰ and since then, § 291a SGB V has been amended several times. The EHC was intended to help to reduce unnecessary double prescriptions, prevent undesirable interactions between medications and make treatment data more easily available in emergencies.¹¹ Other objectives included a nationwide IT infrastructure and the promotion of communication in healthcare and general confidence in eHealth systems.¹² There are precise rules for how the access to the patients data has to be arranged¹³, which data storage on EHC is to be obligatory¹⁴ and which voluntary¹⁵. Although § 291a SGB V has succeeded in guaranteeing a high data security und protection level in connection with maximum transparency for the patient, the full potential¹⁶ of the EHC has not yet been tapped due to lack of technical feasibility.

The EHR as one of the possible applications is based on § 291a (3) Sent. 1 No. 4 SGB V and is to be made available to all members of statutory health insurance with effect from 1 January 2021. The EHR will be a central storage point for all relevant health information such as patient's illnesses, diagnoses or medication. Information is only made accessible to a specific group of people (§ 291a (4) SGB V). Additionally, the use of EHR is voluntary and

data is to be deleted on the patient's demand (§ 291a (6) SGB V). It may be assumed that the general principles of purpose limitation, data minimisation and storage limitation, availability, correctness, integrity and confidentiality (cf. Art. 5 GDPR) must also be observed in the context of the EHR.¹⁷ This also applies to the compliance with information duties (Art. 13, 14 GDPR) and the implementation of the rights of data subjects, e.g. information (Art. 15 GDPR) or deletion (Art. 17 GDPR), as well as privacy by design and privacy by default (Art. 25 GDPR).

In order to pave the way for EHR and to address the deficient implementation of EHC, the legislator has recently planned numerous changes for SGB V which can be found in the draft Patient Data Protection Act: Whereas the stored data¹⁸ on EHC is the same, there is a new chapter 11 dealing with TI and EHR (§§ 341 ff. SGB V PDSG-E). The access to data of EHR¹⁹ as well as the information obligations²⁰ are regulated in more detail. Patient sovereignty is safeguarded by the principle of consent and the right to erasure²¹. Additionally, the right to data portability²² and a clause that identifies the controller of EHR are completely new²³. The PDSG-E and its attempt to answer data protection questions are to be welcomed in principle. Nevertheless, it is just a first – and overdue – step on the way to EHR. Not all clauses are convincing²⁴ and many aspects need more detailed regulation²⁵ without becoming overly complicated.

2.3 Fundamental questions that have to be addressed in any eHealth regulation

Although the introduction of the EHR is to be welcomed in principle, the digitalisation of healthcare does not only result in increasing complexity of regulation, as has been criticised for some time, but also raises entirely new legal questions: some aspects have not yet been regulated or conclusively determined and regulations that have already been established are subject to some criticism. For example, there is no explicit regulation laid down in SGB V to determine who is to be responsible for data processing (Art. 4 No. 7 GDPR) in the context of the EHR.²⁶ In addition to the insured member, the healthcare provider and the service provider, an EHR provider commissioned by the health insurance fund can enter the circle of those potentially responsible. The situation in Germany is much or more the same as in Tanzania where a legal regulation as to who is to be responsible for data processing is lacking. Having noticed this gap, the German legislator has defined the controller of data processing in § 307 SGB V PDSG-E. To summarize, each section that provides services for the TI of EHR is responsible for the processing in its sphere (§ 307 (1-4) SGB V PDSG-E) and the gematik is subsidiarily responsible in case no controller can be identified

10 Angela Merkel, cited by Hilmar Schmudt, "Alles auf eine Karte", Der Spiegel 12.05.2018, No. 20, p. 102.

11 Bales/v. Schwanenflügel, NJW 2012, 2475.

12 Sachs, MPR 2018, 24, 26.

13 § 291a (4, 5, 5a) SGB V.

14 § 291 (2) Sent. 1 SGB V.

15 § 291 (2) Sent. 2 SGB V.

16 E.g. Electronic prescription, storage of data on EHC.

17 Similar Arning/Born, in: Forgó/Helfrich/Schneider (eds.), Betrieblicher Datenschutz (3rd edition 2019), sec. X, ch. 2 marginal no. 8 ff.

18 For obligatorily stored data see § 291a (2) PDSG-E, for voluntarily stored data see § 291a (3) PDSG-E, and for emergency data see § 358 (3) PDSG-E.

19 §§ 339, 352 ff. SGB V PDSG-E.

20 §§ 343, 314 SGB V PDSG-E.

21 § 344 (3) SGB V PDSG-E.

22 §§ 347-350 SGB V PDSG-E.

23 § 307 SGB V PDSG-E.

24 See 2.3 with regard to § 307 SGB V PDSG-E.

25 The German legislator has announced a more detailed management of access to EHR by the 1st of January 2022, draft Patient Data Protection Act, 2020, p. 95.

26 Schütz/Schmitz/Ippach, RDV 2019, 224, 230 f.; Arning/Born, in: Forgó/Helfrich/Schneider (eds.), Betrieblicher Datenschutz (3rd edition 2019), sec. X, ch. 2 marginal no. 21 ff.

(§ 307 (5) SGB V PDSG-E). Consequently, the legislator calls § 307 SGB V PDSG-E a regulation „without gaps“.²⁷ But since the gematik's field of activity comes close to determining the purposes and means of the processing of data (Art. 4 No. 7 GDPR),²⁸ it is questionable whether § 307 SGB V PDSG-E is an appropriate regulatory approach. In addition, the explicit negation of a processing under the authority of the controller (Art. 28 GDPR) – regardless of the actual contract design – seems to be a hasty decision that only serves to privilege the gematik. Unfortunately, the PDSG-E does not comment on Art. 26 GDPR (joint controllers). Ultimately, the role of controller of data processing in the EHR still raises questions in Tanzania as well as in Germany. An issue that has been frequently discussed is the admissibility of consent as a legal basis for data processing in the context of social data protection. This has been rejected in a Decision of the Federal Social Court (BSG) with regard to data processing of external accounting centres.²⁹ According to Art. 9 (2) a) GDPR member states are allowed to restrict the admissibility of consent in the context of health data. Nevertheless, it is not clear if the case law of BSG represents such a restriction. One of the main reasons of the decision was that social data protection law did not refer to consent as a legal basis for data processing. This argumentation of the BSG is not applicable to consent in the context of EHR since social data protection law explicitly refers to consent as a legal basis for health data processing. Despite this, an exclusion of consent can only convince when informational self-determination is not guaranteed due to the circumstances of the individual case, for example if the voluntariness of consent is restricted and a dependency relationship exists. Such a relationship of dependency between patient and recipient of consent cannot be assumed in the context of the EHR in general, but only in individual cases. Therefore, the case law of the BSG should not be applied too restrictively. In fact, the focus is on guaranteeing the requirements of consent which are stated in Art. 4 and 7 GDPR.

In Tanzania, the admissibility of consent for personal data protection remains obscure. The Draft Personal Data Protection Bill 2014 lacks a clear definition of what is consent in as far as processing of eHealth personal data is concerned. Thus, in the context of electronic sharing of digital medical records and test results, there is the obvious challenge of various stages of processing of file transfer and personal data processing and sharing in the course of medical data processing through multiple electronic file transfers.

It has to be considered that a national EHR infrastructure requires not only a specific legal framework, but also broad social acceptance and a basic understanding of its benefits. According to a survey, three quarters of German people would use EHR³⁰ provided that appropriate data protection and data security were ensured.³¹ A legal framework that guarantees appropriate data protection and security is thus not only an end in itself but could gain the essential trust. Despite the challenges of infrastructure and legal framework, there is a generally willingness of health care workers and patients to rely on eHealth service in Tanzania. Surveys have shown that only 16.9% of the Tanzanians fear the changes associated with the adoption of ICT healthcare ser-

vice delivery.³² There seem to be predominantly positive feelings about eHealth in Tanzanian and German society which is a perfect breeding ground for any eHealth system.

The implementation of eHealth goes along with the establishment of an accurate TI, which is not only time-consuming but also expensive. In Germany, the implementation of the EHC was accompanied by very high costs,³³ and it will be the same for the EHR. The records are being conceptualised for 15 years by gematik, a company that is expected to pave the way for EHR. But since health insurances already provide their members with EHR through health applications and smartphones are widely spread, one should not underestimate the technical potential of health insurances. In Tanzania, the health insurance industry is following the German example of embracing Information and Communications Technology (ICT) within the National Health Insurance Fund (NHIF), with the financial support of the German government.³⁴ Storing documents and records is crucial for the National Health Insurance Fund (NHIF), and will not only enhance the access of accurate and reliable statistics,³⁵ but also improve delivery of health service. The Tanzanian health insurance industry will surely participate in the establishment of TI although the whole extent is not yet foreseeable.

This overview gives the impression that the difficulties involved in the legal enforcement of personal data protection in eHealth are comparable in Germany and Tanzania, although they reach different dimensions. Firstly, the body of regulations is exceptionally complex, divergent, uncoordinated, and at different levels of legislative framework and enforcement in the two countries. A large number of data protection issues remain unsolved, e.g. the identification of the responsible person and the role of consent. Second, the establishment of a broad social acceptance is necessary but not impossible, and, thirdly, the time and cost components of building the TI have to be taken into account.

3 TI and data security

In Germany, the regulation of TI and data security in the health sector is based on different areas of law – there is no codified regulation; instead, the legal requirements always depend on the individual case. Some important requirements for TI protection can be found in the sectoral social data protection provisions of SGB V. Once again, there is no specific provision on data security, the legal requirements are widely dispersed and the applicable provisions depend on the respective context of the processing of personal data in the TI: where the data security of EHC use is concerned, the respective requirements are for example laid down in § 291 (2a) and § 291a (3) Sent. 2 SGB V.

32 Busagala/Kawono, "Underlying Challenges of E-Health Adoption in Tanzania", The International Journal of Information and Communication Technology Research, Vol. 3, No. 1, January 2013, pp. 34–41, p. 38.

33 See Bundesrechnungshof, Bericht an den Haushaltsausschuss des Deutschen Bundestages über die Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur 18.01.2019, available at: <https://www.bundesrechnungshof.de/de/veroeffentlichungen/produkte/beratungsberichte/langfassungen/langfassungen-2019/2019-bericht-einfuehrung-der-elektronischen-gesundheitskarte-und-der-telematikinfrastruktur-pdf> (last accessed March 18, 2020).

34 ICT & Telecom, "Germany grants Tanzania €8mln to improve ICT use in the health insurance system", ecofinagency.com 22.10.2019, available at: <https://www.ecofinagency.com/telecom/2210-40594-germany-grants-tanzania-8mln-to-improve-ict-use-in-the-health-insurance-system> (last accessed March 30, 2020).

35 Ibid.

27 Draft Patient Data Protection Act, 2020, p. 4.

28 The gematik is the approving agency for all service providers (§ 324, 325, 327 SGB V PDSG-E), takes measures for danger prevention (§ 329 PDSG-E) and develops guidelines for data processing (§ 313 (4) SGB V PDSG-E).

29 BSG v. 10.12.2008, Az.: B 6 KA 37/07 R.

30 Bitkom, Digital Health, 2019, p. 6.

31 Bitkom, Digital Health, 2019, p. 8.

If the health infrastructure is operated through networked TI components, challenges will arise not only for the secure processing of patient data, but also for the functioning of healthcare facilities. Thus, an insecure TI might not only result in unauthorised access to personal data, but also enable serious attacks on the entire technical infrastructure of medical practices and hospitals, e.g. through viruses and trojans.³⁶ Since health facilities are generally classed as so-called “critical infrastructures” in Germany, the legal requirements for their TI security are very strict.

With the protective strategy provided by the IT Security Act, the legislator has adopted a proactive approach, i.e. risks to the information technology infrastructure are to be identified and eliminated before a damage can occur. This objective is to be achieved by a comprehensive exchange of information relevant for IT security, on the one hand, and adequate protective measures adopted by the operators of critical infrastructures, also based on the newly acquired knowledge, on the other. The IT Security Act introduced the so-called “obligation to report” specifically for the exchange of information. The operators of critical infrastructure are thus obliged to report significant disruptions of availability, integrity, authenticity and confidentiality – relating to the classic objectives of IT protection – immediately to the Federal Office for Information Security (BSI), if the disruptions could lead or have led to a failure or impairment of the functioning of the critical infrastructure. The BSI uses this information to provide a report on the state of IT security in Germany and further ensures that information about potential threats is made available to other facilities that may be affected to enable them to take suitable protective measures prior to the occurrence of the actual risk. This strategy does not only ensure the protection of the individual critical infrastructure, but also serves to prevent coordinated attacks targeted at a number of facilities through the networked flow of information.

The draft Patient Data Protection Act envisages comprehensive changes of the existing law on health and social data. Not only the paragraphs 291 ff. SGB V mentioned at the beginning of this section are to be amended. At the core of the reform efforts on health-related data protection is the creation of two new and independent chapters within the SGB V. The new chapter 11 is intended to make the secure telematics infrastructure future-proof: This includes technical protective measures, requirements for the approval of providers, components and services, regulations on monitoring the functionality and security of the telematics infrastructure, cooperation with the BSI, authentication requirements, detailed regulations on the use of the electronic patient file, the secure transmission of medical prescriptions, telemedicine and requirements on interfaces in IT systems in the health care system. The draft for chapter 12 concerns the so-called “interoperability directory”, which contains, among other things, technical and semantic standards, profiles and guidelines for information technology systems in the health care sector. The interoperability directory is intended to promote the interoperability between

healthcare information technology systems, and it is planned to consult experts of different subject areas for its creation.

For the case of Tanzania, the Cyber Crimes Act 2015 applies if data abuse or violation is directed against a computer system, device, data or person located in Tanzania. Under the Act, operators and service providers are prohibited from monitoring activities or data being transmitted in their systems. However, it may be argued that the existing ecosystem of health data systems in Tanzania is crowded and fragmented.³⁷ In terms of policy, the National ICT Policy 2016 envisages the effective use of ICT for economic development. Equally, the Tanzanian National eHealth Strategy 2012–2018 among its broad areas of concern includes a vision to make eHealth a secure, high quality, efficient and sustainable health system through the use of ICT in delivery of health services.³⁸ The strategic objectives include addressing how data in the health system are collected and managed through ICT. Also, the National eHealth Strategy addresses how eHealth information is shared through the use of ICT as it tries to put in place eHealth standards, rules and protocols for information exchange and protection.³⁹ Today, Tanzania is faced with a problem of lack of harmonisation of eHealth data collection policies at the Ministry of Health, the e-Government Agency (eGA) and National Statistics Bureau (NSB). There is no centralized data control for both the Tanzania Mainland and Tanzania Zanzibar resulting in a lack of adequate critical ICT Infrastructure to guarantee security and legal protection of patient data.

4 Conclusion

The Tanzanian and German eHealth systems offer a promising future of improved health service delivery to a large number of patients. However, questions of data protection and the technical-organisational security of data processing have raised a lot of concerns from commentators as well as members of the public, affecting confidence and trust in the systems. The regulations that have so far been put in place in Tanzania and Germany have already demonstrated practical challenges. Of equal importance are issues of patient rights, transparency and accountability of health service providers. It is too early to predict the development of regulations and the corresponding practice as most of the systems in Tanzania and Germany are still at an infant stage.

This paper was made possible by the support of the Alexander von Humboldt Foundation. It is an outcome of the project „Strengthening protection of personal data in the health sector: a comparative analysis of the Tanzanian and German eHealth System“, a project within the Re-search Group Linkage Programme. The funding of this Research Group Linkage is provided in its entirety by the Federal Foreign Office.

³⁶ Maus, “Hinweise auf mögliche Verwundbarkeiten der Medizin-Telematik”, c’t 17.01.2020, available at: <https://www.heise.de/ct/artikel/Hinweise-auf-moegliche-Verwundbarkeiten-der-Medizin-Telematik-4635791.html> (last accessed March 18, 2020).

³⁷ Path, Data Use Partnership: The Journey to Better Data for Better Health in Tanzania, 2017–2023, pp. 179–180.

³⁸ Ministry of health and social welfare, Tanzanian National eHealth Strategy 2012–2018, Draft 2013, p. 10.

³⁹ Ibid, p. 11.