Mobile for Development mHealth

mHealth Regulation Impact Assessment: Africa

March 2015

This report was written by Beverley Townsend, ehealthlaw.co.za

Table of Contents

> **“[Africa] is too large to describe. It is a veritable ocean, a separate planet, a varied, immensely rich cosmos. Only with the greatest simplification, for the sake of convenience, can we say ‘Africa’. In reality, except as a geographical appellation, Africa does not exist.”**
>
> *Ryszard Kapuściński*

Introduction and scope of research

There have been considerable research efforts in recent years to create a common repository of reusable eHealth (or mHealth) system designs, documents, tools and codes focusing primarily on the standards related to the technical interoperability of healthcare systems. This has allowed health information systems currently in operation to function as a viable whole. Despite this, little has been done to create a common cohesive repository of international mHealth best practice, regulatory or ethical guidelines, protocols and/or legislation which could be useful in the legal regulation of mHealth in developing regions.

mHealth has largely been developed without the benefit of any specific formal law tailored directly at its practice. As such, it has become necessary to examine the existing laws that regulate the healthcare industry, and in particular those which find application within an mHealth environment. The key question to be determined is whether existing regulation is sufficient and if any additional specific mHealth regulation is in fact even necessary.

This review entailed a 20-week on-going process of data collection involving academics, from the fields of law, health and sociology, national and local non-governmental organisations, and governmental agencies including ministries of health, healthcare practitioners and lawyers.

Only seven of the ten countries, Ghana, Kenya, Nigeria, Rwanda, Tanzania, Uganda and Zambia, provided a complete data set within the allotted time frame, with data either not available or a non-response recorded for various themes in the remaining countries. Secondary data was obtained from global sources and a literature review of documents easily accessible in print or on the web. Relevant explanatory comments were documented, as were the exact legal provisions for indicators relating to the legal regulations and exact quotes from strategies and policies.

African countries investigated

This was an exploratory analysis of the data pertaining to the 10 countries targeted by the GSMA mobile nutrition (mNutrition) initiative, which is a part of the GSMA’s Pan-African mHealth Initiative. mNutrition aims to support the scale-up of mHealth in nutrition and maternal and child health, in support of the Millennium Development Goals 4, 5 and 6. mNutrition is closely aligned to the UN’s Every Woman Every Child Initiative, Scaling-Up Nutrition (SUN) and the Global Nutrition for Growth Compact.

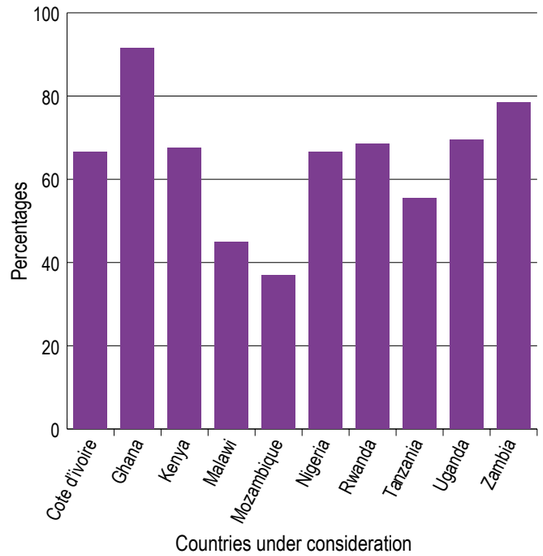
The target countries are Côte d’Ivoire, Ghana, Kenya, Malawi, Mozambique, Nigeria, Rwanda, Tanzania, Uganda and Zambia.

Executive summary

This report provides a high-level compilation of the mHealth legal and regulatory landscapes in ten African countries. This report has been compiled by carrying out a cross-jurisdictional review of the regulatory instruments (including statutes, policies and guidelines) that govern mHealth and related e-transactional interests. The objective of this report is to provide the mHealth community with, where possible, an overview of legal provisions contained within the existing legal frameworks that may have a direct impact on mHealth initiatives.

This high-level compilation of landscapes is summarised in a regulatory provisional ranking for the ten countries under review, on page 6. The ranking was created using provisional indicators based on the data available at the time of collection, and, as such, is to be interpreted as a snap-shot of that particular point in time. The ranking is created by placing a weighting on 14 themes under consideration, all explored in further detail throughout this report.

This graph presents the results of the ranking. A more detailed graph can be found on page 6.



This report also outlines a baseline of the mHealth legal and regulatory environment found within the ten selected African countries. It focuses on various, broad, albeit not exhaustive, themes that may be relevant in the mHealth discourse around appropriate regulatory review and revision. It attempts to consolidate mHealth legislation and policy data on a country level which is not readily available. The consolidated tables for each of the ten countries are contained in the appendix of this report.

Some important findings about mHealth adoption and regulation were unearthed across the ten target countries:

- Regulation should be proactive and enabling
- Avoid a so-called ‘one-size-fits-all’ approach
- Include both global and local approaches in solution-finding
- Engage with all national stakeholders
- Embrace private sector mHealth initiatives and cooperation between the public and private sectors
- Consider the changing nature of the socio-cultural environment
- Provide guidelines that address the quality and content of health information
- Safeguard the users’ rights to be the owners of their information and ensure adequate data security, data protection and privacy laws are in place
- Ensure adequate standards for the transference and exchange of data
- Encourage and find appropriate alternative and more pragmatic methods of performing activities in a virtual environment, so that they have the same effect as those carried out using traditional methods, including addressing issues of an evidential nature

The implications of not having the necessary clear legal safeguards in place in the countries may have an adverse impact of the development of mHealth initiatives in the region. The potential to realise the benefits of mHealth and the need to institutionalise mHealth after adoption is a collaborative journey that all stakeholders need to embark on.

It is therefore recommended that African countries review the gaps found in their legal regimes and begin instituting appropriate measures to address them. Only once these challenges have been suitably addressed by policy makers, and sustainable African-centric solutions found for the effective roll-out of robust mHealth initiatives, can the much-needed scale be attained to address the continent’s dire need for affordable and accessible preventative and primary healthcare.

Why fortify legal protection in mHealth?

By its very nature, healthcare and the practice of medicine is a highly regulated industry. Although the reasoning for this is sound, to protect public health and safety, it can have the unfortunate effect of delaying innovation. For rapidly changing environments, such as those driven by technology, the advancement frequently either creates a regulatory void - which increases risk for providers and users alike - or the application of inappropriate regulations from earlier technologies.

For African countries to align themselves with other key players globally, and embrace modern means of communication and information technology, certain legal issues and challenges cannot be ignored. Strengthening regulations relevant to mHealth will promote mHealth development by increasing regulatory clarity and legal certainty for mHealth users and suppliers.

Regulatory provisional indicator/ranking for countries under review

The graph below is a summary of findings for the 10 countries under review. The scores/ratings contained in the graph are provisional indicators based on the data available at the time of collection. While a zero score was allocated where the data was unavailable or uncertain, that does not necessary accurately reflect the position within the country. Moreover, as laws, policies and regulations are in a constant state of evolution, this graph is to be interpreted as a snapshot of the data available at the time of compilation.

weighting		Cote d'Ivoire	Ghana	Kenya	Malawi	Mozambique	Nigeria	Rwanda	Tanzania	Uganda	Zambia
10%	E-health Strategy/Roadmap/Policy	10	10	10	10	10	10	10	10	10	10
5%	Implementation	2.5	2.5	2.5	0	0	0	5	2.5	2.5	5
5%	e-consulting, e-diagnosing, e-advising, e-prescribing, edispensing	0	2	3	0	0	0	0	0	0	2
2%	Governance and policy mechanisms in place at a national, regional and/or local level to ensure implementation, support and monitoring of the e-health strategy	0	2	2	0	0	0	2	2	0	0
10%	E-transactions and e-signature legislation	10	10	10	5	0	10	10	5	10	10
5%	Consumer Protection	5	5	5	2.5	3	5	2.5	4	4	5
5%	e-health regulatory body	0	5	2.5	0	0	2	5	5	5	0
10%	e-Legislation	10	10	10	5	0	10	10	5	10	10
3%	Restrictions on sensitive data	0	3	0	0	0	0	0	1.5	0	1.5
5%	Data protection legislation provides for minimum standards of collected fairly and lawfully; • used only for the specified purpose for which it was originally collected; • adequate, relevant and not excessive to purpose; • accurate and up to date; • accessible to the subject; • kept secure; and • destroyed after its purpose is completed.	4	5	5	2.5	4	2.5	4	3	3	5
5%	e-health or telemedicine codes of practice/guidelines in place	0	2	2.5	0	0	2	0	0	0	0
10%	Limitation of Service Provider Liability	0	10	0	5	0	10	10	0	10	10
5%	Restrictions on offshore data transfers	5	5	0	5	0	0	0	2.5	0	0
20%	Applicable data protection legislation	20	20	15	10	20	15	10	15	15	20
100%		66.5	91.5	67.5	45	37	66.5	68.5	55.5	69.5	78.5

Identified barriers facing mHealth development

Barriers identified specifically by the respondents in the various African countries include:

- Lack of explicit enabling mHealth policies and legal frameworks
- Lack of mHealth awareness amongst policy makers
- The absence of explicit data protection law
- Lack of mHealth / ICT / data protection regulatory bodies

Themes under consideration

Although by no means exhaustive the particular legal/ ethical themes under consideration in the questionnaire and interviews included:

- **The existence of an mHealth roadmap/strategy**
- **The constitutional protection and rights to healthcare and privacy**
- **Medical-legal and ethical concerns in the practice of mHealth**
- **Privacy and data protection**
- **Cyber legislation and e-transaction law**
- **mHealth application and device regulation**
- **Content control and ISPs liability**
- **Consumer protection (online)**

A comprehensive health plan or roadmap for the adoption of mHealth and its regulation

The level of governmental commitment and readiness to embrace the adoption of mHealth guidelines at a national and regional level impacts directly and facilitates mHealth integration and implementation in the healthcare system of the country.

Findings:

The data collected showed that generally a sound base of mHealth strategies and policies exist within Africa. Of the responding African countries surveyed almost all had an eHealth (mHealth) strategy in place. Most strategies or policies had been adopted within the last ten years with the intention of setting out a road map for mHealth development in the country. However, the strategies generally could be described as only 'partially implemented', with it being acknowledged that any mHealth roll-out plan requires time, commitment and resources to fulfil.

The commitment to the process of mHealth development and implementation in these countries is moderate to high. Despite this, the reality is that few countries have addressed mHealth regulation in any meaningful way. Most national mHealth strategies build on broader ICT and health visions of the countries and regions. Moreover, the policies are generally deficient in addressing ethical issues around patient/user care and liability, for instance, e-diagnosing, e-consultations or e-prescribing via mobile applications and devices and more specifically when this is done across geographical borders. Practical guidelines on its integration and implementation at national and regional levels were also lacking. African countries under review by and large acknowledge that the regulatory environment should act as an enabler for the effective delivery of mHealth strategies and related activities, although there is little clarity on how this is to be implemented.

Formal recognition of the right to health

The question to be determined was whether a country's Constitution, Bill of Rights or other human rights instruments recognised the fundamental right to healthcare for its people.

Findings:

All ten countries had some form of recognition of the right to health or healthcare.

Examples:

These rights to health provisions are mostly well established and range from a mere mention, as found in the Constitution of the Ivory Coast in Article 7 which provides '[e]very human being has the right to the development and to the full realisation of his personality in the material, intellectual and spiritual dimensions. The State assures to all citizens equal access to health, to education, to culture, to information, to professional formation and to employment' to the more detailed, as found in the Constitution of the Federal Republic of Nigeria of 1999, which provides for the right to health in section 17. Section 17(3) c provides '[t]he State shall direct its policy towards ensuring that there are adequate medical and health facilities for all persons'.

Although there is, for example, no express provision in the Constitution of the United Republic of Tanzania, 1977, on the right to healthcare, Article 9(i) obliges the state authorities and all its agencies to direct their policies and programmes towards ensuring the use of national resources for development of the people and particularly geared towards the eradication of poverty and disease. Moreover, Article 30(2) (b) calls for enactment of laws to ensure public health.

Most of the right to health provisions placed a positive obligation or duty on the state to progressively adopt or implement health policies. The Rwandan Constitution, for instance, provides in Article 41 that '[a]ll citizens have the right and duties relating to health. The State has the duty of mobilising the population for activities aimed at promoting good health and to assist in the implementation of these activities.' While the Malawian Constitution states in Section 13(c) under the Principles of National Policy that 'the State undertakes to actively promote the welfare and development of the people of Malawi by progressively adopting and implementing policies and legislation aimed at providing adequate healthcare, commensurate with the health needs of Malawian society and international standards of healthcare'.

To give effect and provide substance to the formal recognition of the right to health, as contained in the various constitutions, bills of rights or human rights instruments, requires a legal response in the form of legislation, regulations, guidelines, ethical codes of conduct and protocols.

This is of importance as a clear commitment to healthcare rights is fundamental to healthcare adoption and delivery within the country. The language used in these instruments generally indicates a high level of importance and commitment attributed to the safeguarding of healthcare service quality and accessibility.

eHealth (mHealth) legislation in Africa

Findings:

The regulatory and legislative frameworks differ from country to country, and between the various African regions, often with seemingly large disparities. Presently, the general view of the mHealth regulatory and legislative landscape in Africa is that it is either non-existent, or that it comprises an increasingly complex, albeit fragmented, national regulatory system of policies, influenced by a dense web of international law instruments regulating healthcare privacy and human rights issues. mHealth policy provisions are often 'embedded' or incorporated into larger health, e-government or e-commerce policies or strategies. It is for this reason that certain provisions are not always immediately apparent. Irrespective of their size, wealth or health system, the African countries investigated were united in their experience of certain, common mHealth challenges.

Africa cannot be seen as a homogenous mass. Differing expectations and independent priorities between African countries lead to unclear and divergent policy expectations, processes and executions. Significantly, the management of issues around privacy and data protection are pivotal indicators in the maturity of a country's mHealth regulatory environment. However, the fact that an mHealth strategy or 'road map' has been adopted is in no way indicative of the actual legislative advancement or healthcare delivery reality within the country.

Practical considerations/recommendations:

- The need to regulate sufficiently so that acceptable standards are maintained without hampering innovation and serving a large consumer market.
- The need for simple legislation with sound, practical principles built on the existing mHealth regulatory environment.
- A 'one-size-fits all' approach is not necessary appropriate - as Africa requires unique solutions to Africa's problem.
- The culture and custom of the region and community are significant considerations.

Medical-legal and ethical concerns: telemedicine, e-advising, e-consultation, e-prescribing and e-dispensing

Telemedicine, eHealth and mHealth rely on the use of technology as complementary to physical face-to-face interactions, without compromising healthcare standards, quality and delivery or adding unnecessary cost. Although recognising that there is not one definitive definition, the WHO has described telemedicine as '[t]he delivery of health services, where distance is a critical factor, by all healthcare professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health providers, all in the interests of advancing the health of individuals and their communities'.[1] Although no universally accepted definition of eHealth exists, it is generally considered a broader term encompassing all tele-health activities[2] and is described by the WHO as lying at the intersection of 'medical information, public health and business'[3]. To this end, the WHO has advocated the use of reduced cost information technology as a means of improving the quality of service delivery especially for primary healthcare.[4]

Although studies on telemedicine in Africa in particular have to a large extent centred on the 'technological feasibility, specialist clinical interest, implementation costs and estimated cost savings'[5], there is a clear and obvious socio-economic benefit to users/patients: that of better quality care, greater participation, cost effectiveness and increased accessibility[6].

However, in the adoption of telemedicine and more particularly eHealth and mHealth, issues around liability, licensure (including cross-border licensure), jurisdiction, quality and continuity of care, data security, confidentiality, consent, authentication and remuneration all need to be considered.

Certainly, clinical practice standards should apply regardless of whether technology is introduced into the healthcare process or not. The interaction between healthcare practitioner and patient, while using a technological platform as a means of healthcare delivery, should not diminish the obligation on the healthcare practitioner to meet certain clinical standards or the right to autonomous decision-making of the patient. Similarly, any shortcomings inherent in the use of technological platforms should not be a mitigating factor in the failure to achieve these standards.

eHealth and mHealth may alter the traditional healthcare experience for the user/patient. Access to the healthcare system is not necessarily through a primary care practitioner and a user/patient does not always progress through the healthcare system in a linear fashion. Examination, diagnosis, treatment and follow-up care involving the physical presence and personal interaction of the primary practitioner does not necessarily follow the traditional predefined course. This departure from traditional thinking may be concerning, as the ultimate responsibility for the user/patient's care is not always clearly defined. Thus, the conventional, traditional approach to the patient doctor relationship does not always necessarily sit comfortably with the advancement of mHealth. Certain legal regimes, for instance, require the establishment of a doctor-patient relationship before treatment commences, except in cases of emergency where a patient is unconscious. Likewise, certain legal regimes require a physical examination of the patient.

Example:

In Ghana, for example, Article 30 of the 1992 Constitution stipulates that '[a] person who by reason of sickness or any other cause is unable to give his consent shall not be deprived by any other person of medical treatment... by reason only of religious or other beliefs'. To ensure adequate standards of quality and to provide more fully for the protection of patients' interests, certain countries have developed charters such as that implemented by the Ghana Health Service in 2002. The Patients' Charter of Ghana, for example, sets out the nature of the relationships between patients and providers. Additionally, it addresses the requirement for greater preventative health promotion and simple curative strategies for its people.

Although it is unclear what the standard of care imposed on health practitioners providing mHealth services should be, it is understood that the standard of care in a particular jurisdiction should be the same as it is for other similar healthcare procedures in that jurisdiction[7].

Findings:

Although telemedicine is often well established and encouraged, legalities around econsulting, e-prescribing and e-dispensing remain unclear at this stage. The laws in

[1] *World Health Organization 'Telemedicine Opportunities and developments in Member States' Report on the second global survey on eHealth Global Observatory for eHealth series – Volume 2 (2010) at 9. Moreover, the definition of telemedicine adopted by National Health Information System of South Africa (NHIS/SA) is as follows: '[t]he practice of medical care using interactive audio, visual and data communications; this includes medical care delivery, consultation, diagnosis and treatment, as well as education and the transfer of medical data'.*
[2] *A Le Roux 'Telemedicine: A South African legal perspective' (2008) (1) TSAR 99 at 100.* [3] *World Health Organization WHA58.28 e-health Geneva: WHO 2005.*
[4] *Ibid.* [5] *PA Jennett et al "The socio-economic impact of telehealth: a systematic review" 2003 Journal of Telemedicine and Telecare 311-312 and Le Roux (note 2) at 102.* [6] *Ibid at 102*
[7] *D Svantesson 'Legal liability for Internet based cross-border provision of medical advice, information and products' (2003) 9th Greek Australian Legal and Medicine Conference Rhodes Greece.*

the African countries reviewed are either silent or undecided on exactly what is permitted in this regard. A call for the development of discipline-specific guidelines and policies for the practice of mHealth covering clinical, operational, technical and legal and ethical concerns is required.

Data messages, e-contracts, e-transactions and e-signatures

Cote d'Ivoire	• Unknown
Ghana	• Yes, not fully developed in all sectors
Kenya	• Yes
Malawi	• In draft
Mozambique	• Unknown
Nigeria	• Yes
Rwanda	• Yes
Tanzania	• In draft
Uganda	• Yes
Zambia	• Yes

An obvious characteristic of mHealth initiatives is that they are carried out at a distance where the provider and the user are for the most part in different environments. With regard to mHealth this contractual relationship may be conducted partially or wholly electronically in an online environment.

While concerns may not arise in traditional paper-based contractual arrangements or when consultations or services are provided face-to-face, issues pertaining to the validity and enforceability of electronic transactions, contracting online and providing consent electronically as well as the admissibility of documents become problematic. Jurisprudence in this area has not yet been developed and clear, unambiguous guidelines are sought[8].

Examples:

Certain African counties, Uganda most notably, have been in the process of formulating elegislation since 2003 with a national taskforce led by the Uganda Law Reform Commission set up to undertake this exercise. E-laws were enacted in 2011 with the Ugandan Electronic Transactions Act 8 of 2011, the Computer Misuse Act of 2011 and the Electronic Signatures Act of 2011 providing the backbone of the e-legislative framework. Rwanda also enacted a law governing electronic messages, electronic signatures, electronic transactions, data protection and cyber security in May 2010 - Law no.18/2010, as has Zambia in the Electronic Communications and Transactions Act 21 of 2009.

Consent, informed consent, e-consent and dynamic consent

It is generally accepted that healthcare professionals should respect the decision-making capacities of autonomous users/patients[9]. The trend for people to take greater responsibility for their health, increased information seeking and involvement in decision-making, the need for self-determination and autonomy, coupled with a willingness to challenge the power that doctors' exercise over them, has fundamentally changed the doctor-patient relationship in western society[10].

Findings:

The doctrine of consent is entrenched in most African common law, case law and legislation, in which effect is given to the protection of an individual's right to physical integrity and selfdetermination. Consent management is thus vital for mHealth providers. Certain legal regimes require 'written' consent before treatment can be received (Tanzania, for instance) whether such consent may be electronically obtained is unclear.

Recommendations:

A case for dynamic consent may be made which combines both technical and policy flexibility, as traditional consent models may no longer be viable. Despite the formality for consent to be 'in writing', it is expected that e-legislation may provide some relief to mHealth practitioners where data messages are recognised as the functional equivalence of writing and as having the same legal value as a message written on paper[11]. Once again greater legal certainty is sought.

The monitoring and regulation of mHealth applications and devices

mHealth development and initiatives cover an entire spectrum, from the very basic to the most comprehensive. These follow something of a risk continuum from the seemingly benign to the highly risky and potentially life threatening. The degree of regulatory influence and involvement will of necessity correspond and find application as the risk profile of the mHealth activity increases.

Recommendations:

- Ensure the right balance, between risk and innovation when reviewing mHealth applications. The intended use and medical functionality or purpose should be borne in mind.
- Aim to promote innovation, protect user/patient safety and avoid regulatory duplication.
- Application software and hardware developers need clarity to support the continued development of their mHealth products. Likewise, greater regulatory clarity for users is required - users need to know the regulatory status of an mHealth solution. Also the level of scrutiny applied to the application or device and/or studies conducted in this regard should be clarified.
- No substantial new regulations for products and applications that pose a low risk to patient safety. Differentiation should be made between disease / diagnostic and wellness / preventative healthcare applications and devices.
- Existing regulatory framework should be 'more nimble and flexible' to respond to a rapidly expanding mHealth sector.
- Regulatory authorities (like the US FDA equivalent) within each African country to be tasked to provide guidance and tailored decisions.

Internet service providers and the limitation of their liability

Cote d'Ivoire	• Unknown
Ghana	• Yes
Kenya	• No
Malawi	• Unknown
Mozambique	• Unknown
Nigeria	• Yes
Rwanda	• Yes
Tanzania	• No
Uganda	• Yes
Zambia	• Yes

Findings:

Legislation which limits the liability of recognised service providers under certain circumstances is lacking in almost half of the African countries investigated.

Examples:

Nigeria is an example of an African country that accommodates this in paragraph 11 of the Nigerian Communications Commission Guidelines for the provision of Internet services (2007) published pursuant to section 70(2) of the Nigerian Communications Act of 2003. In terms of this provision a service provider can escape liability as content intermediaries under certain circumstances. Paragraph 12 of the NCC guidelines provides 'ISPs must have in place a procedure for receiving and promptly responding to content related complaints, including any notice to withdraw or disable access to identified content issued by the Commission or other legal authority,' that is, 'takedown notices'[12]

Uganda also has specific limitations of intermediary/service provider liability provisions or 'safe harbour provisions'. Under section 29 of the Electronic Transactions Act of 2011 a service provider is not subject to civil or criminal liability in respect of third party material that is in the form of electronic records to which he merely provides access, acts as a conduit or merely links or refers to material. The Act provides for a notice and take-down procedure to be put in place. Zambia also has similar provisions in Part X of its Electronic Communications and Transactions Act 21 of 2009.

Legislation intended to consolidate provisions providing protection and the limitation of Internet intermediary liability under certain conditions should be welcomed. This should limit the liability of service providers who have little control over the content on their sites but who act merely as innocent disseminators of content. It is suggested that their position should be considered analogous to that of distributors or vendors.

[8] The UNICITRAL Model Law on E-Commerce adopts the principles of non-discrimination, technological neutrality and functional equivalence. The principle of non-discrimination provides that any document would not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form. The principle of technological neutrality enforces provisions that are neutral with regard to the technology used and functional equivalence establishes criteria under which electronic documents may be considered equivalent to paper-based documents. The UNCITRAL Model Law on E-Commerce has been largely influential in the drafting of the provisions of many of the e-legislation found in Africa.

[9] Respect for patient privacy and confidentiality is well recognised in contemporary professional medical ethics. See in this regard JC Moskop, CA Marco, GL Larkin, JM Geiderman and AR Derse 'From Hippocrates to HIPAA: privacy and confidentiality in emergency medicine--Part I: conceptual, moral, and legal foundations' (2005) 45 (1) Annals of Emergency Medicine 53-59. See also M Siegler 'Confidentiality in medicine- a decrepit concept.' (1982) 307 (24) New England J Medicine 1518–1521; also TL Beauchamp & JF Childress Principles of Biomedical Ethics 6 ed (2008).

[10] GT Bosslet 'Commentary: The Good, the Bad, and the Ugly of Social Media' (2011) 18 Academic Emergency Medicine 1221 at 1222 and GT Bosslet AM Torke SE Hickman CL Terry PR Helft 'The patient-doctor relationship and online social networks: results of a national survey' (2011) 26 J Gen Intern Med 1168 at 1172.

[11] Dynamic consent: a patient interface for twenty-first century research networks, European Journal of Human Genetics, May 2014.

[12] such as that found for instance in the South African Electronic Communications and Transactions Act No. 25 of 2002.

What are the practical implications for Internet Service Providers / Intermediaries where this legislation is in place?

The service provider may escape liability in the following circumstances:

- must be defined as a service provider in terms of the Act,
- must operate as a 'mere conduit', that is the service provider does not initiate the transmission, select the addressee, modify the transmitted data contents and performs the function in an automatic, technical manner without selection of the data; or
- provides for 'caching' data, that is, to make transmissions more efficient; or
- provides 'hosting' services, that is, the storage of data; or
- provides referring or linking users to a web page.
- does not have actual knowledge, or is unaware, that the material is of an infringing nature, and is not aware of facts or circumstances from which the infringing nature of the material or activity is apparent, and
- upon receipt by the service provider or its designated agent of a take-down notice, acts expeditiously to remove or block access to the material.

As it is, the 'owner' of the website who controls the contents on its website and as such provides a forum for the content, they will generally not be able to rely on the protection of the legislation.

Content control and accuracy

Strikingly, little or no regulatory control over content or its accuracy was found. Voluntary compliance and/ or self-regulation by content providers appears to be prevalent.

Concern as to the quality, reliability and accuracy of information available online and the credibility of the persons providing such information is an issue. Inaccurate, misleading and dangerous information has the potential to cause harm with those users lacking evaluating skills at even higher risk.

- As the Internet is largely unregulated, it is incumbent upon the website owner or content provider to voluntarily self-regulate in matters of content accuracy and quality with limited or no policing by the authorities.
- Education of users is paramount as research has indicated that those who more frequently use social media services are not only better able to discriminate between useful and non-useful information, but can do so more efficiently and are for the most part, satisfied with the information sought[13].
- Trust in the reliability of the application, service or product should be established and maintained.

Privacy and data protection

Is privacy a concern for online users?

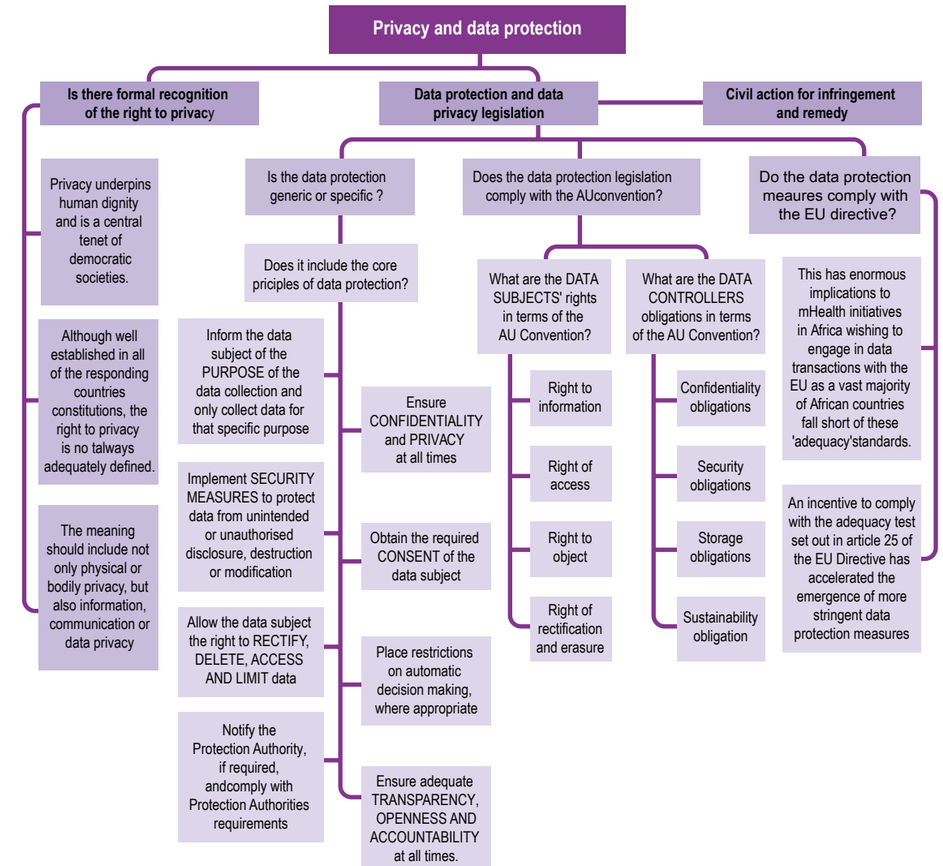
If proper systems of privacy and data protection in mHealth are not initiated, users and patients may be reluctant to use the mHealth application. This is especially true where adverse situations may arise following a diagnosis, such as stigma or social exclusion resulting from an HIV/AIDS or STDs finding. An example of this is where SMS messages are sent to users providing them with test results, specific treatment advice, or medication or appointment reminders. The safeguarding of this content is imperative, particularly in communities where mobile phones are shared amongst family members who may inadvertently intercept these messages.

The enforcement of registration of all SIM cards, a necessity requirement in most of Africa, plays a role in user/patient identification and results in a user never being truly anonymous. The protection and safety of their data is therefore of more importance.

Findings and Recommendations:

Data security is imperative in any mHealth initiative. The solution is to base protection measures in legal frameworks that are understood, trusted and enforced.

- When compared to the Western implementation of privacy regimes, many African countries have not adopted sufficiently comprehensive data protection legislation. Additionally, privacy and data protection, where enacted, is not specific to the healthcare sector but rather part of general privacy and data protection legislative regimes.
- While Mauritius, Morocco, South Africa, Ghana and Tunisia have developed comprehensive data protection laws, others are in the process of drafting and finalising such laws.
- The general regulation of privacy and data protection spans many disciplines so it would be unlikely and unexpected to be found exclusively in mHealth-specific regulatory policy. Generally, it was found that there are no provisions expressly addressing privacy in mHealth, rather the law on privacy as it applies to mHealth has to be extrapolated from generic privacy and healthcare legislation.
- Where investment into mHealth has been considerable, the legal frameworks providing concomitant legal protection are being accelerated. However, this has been largely on a fragmented and reactionary basis. The potential of the regulations to act as a catalyst to facilitate mHealth initiatives is not being fully or sufficiently realised. While the law by and large has been lagging behind the growth of mHealth requirements, certain jurisdictions are uncertain of the impact it will have on their legal systems. A limited or almost non-existent body of jurisprudence has been built up over the past relating to issues surrounding mHealth and e-transactions. Very little literature is available dealing specifically with mHealth regulation in an African context.
- With regard to health and sensitive data most African countries under investigation have medical and healthcare legislation and medical ethical codes of practice which often also provide protection for confidential data and issues around the need for consent, the establishment of a patient-medical practitioner relationship and/or the need for a physical examination. In the establishment of trust, the requirement that health-related information be kept private is a central tenet of most doctor-patient relationships and commonly accepted as the basis of good ethical practice. More than ever, data handling and good, secure record-keeping should form part of this practice in light of the advancement in medical testing, genetic profiling and medical imaging, hugely increasing the volume and detail of digitally available health information.



[13] G Eysenbach and C Kohler 'How do consumers search for and appraise health information on the World Wide Web? Qualitative study using focus groups, usability tests, and in-depth interviews' (2002) 324 (7337) BMJ 575.

Findings:

Although certain constitutional rights are absolute, the right to privacy typically is not. Although recognised in various forms, the majority of responding countries have some degree of constitutional privacy right in place.

Privacy levels vary across nations, cultures and historical time periods and are dependent on a complex array of factors[14], including cultural, religious and philosophical factors. Although interpreted in different ways, privacy is a universal process inherent in all cultures and societies, with even those having ostensibly minimum privacy requirements, desiring at least some degree of privacy[15].

Cote d'Ivoire	• Yes
Ghana	• Yes
Kenya	• Yes, Bill expected to be tabled 2014
Malawi	• Draft Bill
Mozambique	• Yes
Nigeria	• Yes, Bill to extend protection
Rwanda	• Partial, no comprehensive regime exists
Tanzania	• Yes limited, specific protection in Bill
Uganda	• Yes, Bill
Zambia	• Yes, Bill

The uneasy juxtaposition of rapidly advancing information technology and the inherent conservatism of the law around informational privacy has understandably exacerbated concerns and sensitivities around potential privacy intrusions.

- Cultural variations to the concept and meaning of 'privacy' differ between the regions although a common ground based on a western notion of 'privacy' may be established. Regardless of this, before applying 'modern' or 'universal' standards to 'privacy' one should be cognisant of sensitive to the cultural norms, customary values and historical context within the divergent groupings.
- Many African countries have a 'hybrid' or 'mixed' legal system formed by the interweaving of a number of distinct legal traditions. Indigenous, or African customary law, finds application in many African legal systems.
- Personal or health data, although factually or contextually accurate, may be of such a sensitive and/or personal nature that it may cause potential harm and embarrassment if disclosed to a third-party without the individual's knowledge and/or consent.
- Despite data protection legislation being enacted or being in the process of enactment, not all data protection legislation is comparable. While considerable international Human Rights instruments, comprehensive data protection literature and authoritative sets of data protection principles are available to which countries can refer, regrettably certain data protection measures may be described as narrow and inadequate versions of the full range of data protection principles ideally required. Nevertheless, attempts at addressing the issues are positive and encouraging and may be an indicator of what is to come.

Data protection instruments in Africa

Findings:

100% of countries surveyed were members of the African Union and 100% were members of their respective regional economic communities. The recently adopted AU Convention on Cyber Security and Personal Data Protection is to be welcomed. In line with this Convention, African countries are obligated to take immediate steps to adopt data protection laws and fortify their constitutional provisions in this regard.

Although once lagging behind the world in the development of data protection law, Africa has of late transformed its data privacy regimes. Although modest progress has been made thus far, the expectation is that the pace of legislative enactment will continue accelerating in Africa largely due to the requirement stipulated in the European Directive. This provides that the transfer of personal data to third countries, that is, non-European Union member states (which would include African countries) can only occur where such country can guarantee an 'adequate' level of data protection.

To comply with the adequacy test set out in article 25 of the EU Directive, and because of the recent increase in ICT development on the continent, Africa has witnessed the emergence of data protection measures with various countries providing for constitutional protected rights of privacy and/or legislative protection. To date a total of 17 countries in Africa have privacy laws that regulate the collection and use of personal data. These laws have either been recently enacted or amended in Cape Verde, Burkina Faso, Gabon, Mauritius, Tunisia, Morocco, Seychelles, Uganda, Cote D'Ivoire, South Africa, Mali and Ghana. Other African countries, such as Kenya and Nigeria, are expecting new data protection laws to be enacted in the course of 2014.

14 LA Bygrave 'Privacy and Data Protection in an International Perspective' (2010) Stockholm Institute for Scandinavian Law at 174.
15 Altman 'Privacy regulation: Culturally universal or culturally specific?' (1977) 33 (3) Journal of Social Issues at 66.

African Union

All ten countries under consideration are members of the African Union. The development of initiatives by the African Union and more particularly the African Union Convention on Cyber Security and Personal Data Protection adopted at the 23rd Ordinary Session of the Assembly of the Union, in Malabo on the 27th June 2014, is an attempt to address certain cyber law issues. The AU Convention seeks to harmonise African cyber legislations and substantively elevates the rhetoric of 'protection of personal privacy' to that of an international level. Moreover, it seeks to establish a legal framework for cyber security and personal data protection in the context of e-commerce and e-transactions

Findings and recommendations:

- While international and regional frameworks establish the themes, intent and functionality, in most countries national legislation is required to give substance to the principles protected.
- Although model laws do not have binding effect, the member states are called upon to align themselves with the provisions thereof. The model provisions are a means to assist in, but not to substitute, the meticulous process of drafting national law.
- Although it is likely that any new legislation will mirror the provisions of international law, the adoption of data protection legislation should not be merely that of 'cutting and pasting' EU or regional model laws. While it should build on and adopt what is available and appropriate it should nonetheless reflect the nuanced customary and community needs of the people it is to serve and represent.
- Extensive consultation and engagement is required from all stakeholders before such laws should be adopted.
- Standardised and harmonised definitions and processes, including narrower definitions for different data types, are required. 'Sensitive, health or personal data' may need to be treated appropriately.

Data exchange and cross-border data transfer

To prevent the creation of 'data havens' it is necessary for different countries to provide an **equivalent level of data protection** so that information can be passed between them without restriction. 'Data havens' are described as countries with no or little data protection laws to which personal data can be transferred, for the purpose of circumventing the national laws of the country of origin of the data.

Findings:

The general rule prevalent across most investigated legal regimes is that personal data should only be transferred to recipients if an adequate level of protection is ensured in the country of the recipient and the data transferred is solely to allow tasks covered by the competence of the controller to be carried out. Also as a general rule, consent of the data subject is necessary.

The increase and advancement in, for example, cloud computing places increasing pressure on regulatory systems for cross-border data flows, making it important that such systems bring about a desirable level of compliance. Cloud computing is an example of cross-border data flow, as personal information is hosted and 'transferred' to a foreign jurisdiction or site.

Of particular importance is article 25 of the 1995 EU Directive on data protection which regulates the collection, processing and transfer of personal data within the EU while enabling the free flow of data. **This directive is seen as a significant driver of an emerging global data protection regime.** The EU Directive provides that the transfer of personal data to third countries, that is, non-European Union member states (which would include African countries) can only occur where such a country can guarantee an 'adequate' level of data protection. Thus, countries that wish to engage in data transactions and exchanges with EU member states are required to provide an 'adequate' level of data protection.

Recommendations:

By standardising and harmonising data protection laws across countries, the free and safe flow of data across national boundaries may be enabled.

Case study

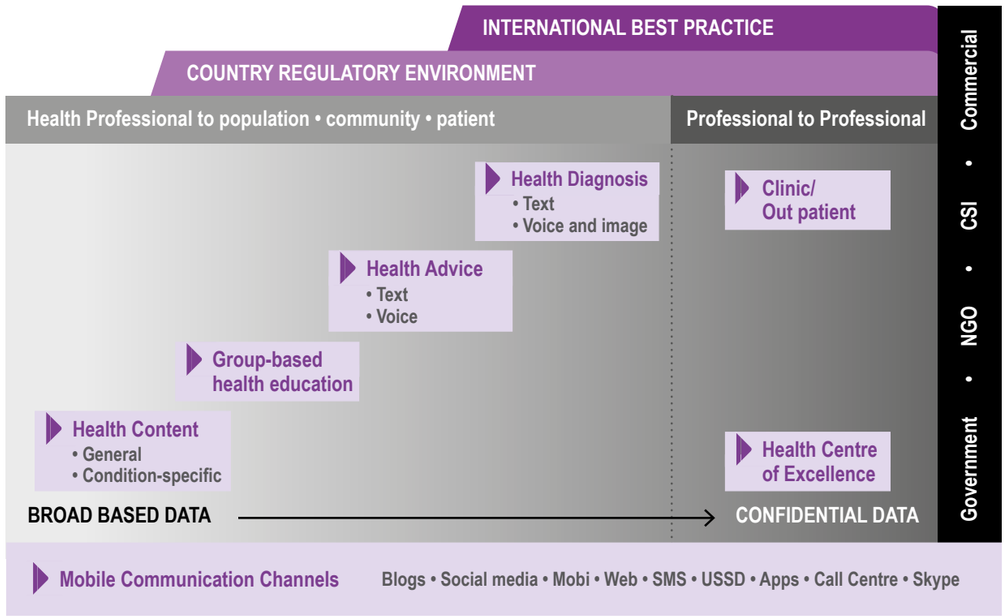
In June 2012, the GSMA mHealth programme launched the Pan-African mHealth Initiative (PAMI). PAMI is closely aligned to the UN's Every Woman Every Child Initiative, Scaling-Up Nutrition (SUN) and the Global Nutrition for Growth Compact. After an initial focus on South Africa, in September 2013 PAMI expanded to mHealth services targeting nutrition and maternal and child health in Côte d'Ivoire, Ghana, Kenya, Malawi, Mozambique, Nigeria, Rwanda, Tanzania, Uganda and Zambia.

The mHealth initiative was to provide basic health tips or messages aimed at providing information regarding a specific medical condition or wellness concerns. These tips, while for the most part generic in nature, may still require data from the user to be provided and stored/used as appropriate. These are targeted, timely and actionable health information messages delivered to consumers through SMS, IVR, audio and video which aim to increase knowledge, provide reminders and affect behaviour.

Regulatory issues relevant to a mHealth initiative such as this:

- **Privacy and data protection – especially data security, confidentially and data transfer/exchange**
- **E-legislation: validity of data messages**
- **Content control and validity**
- **Consent management**
- **Consumer protection provisions – including opt-in/ opt-out**
- **Monitoring and regulation of mHealth device and software applications**

Regulatory impact assessment: risk vs regulation



It is essential that regulatory bodies within the African regions and individual African countries work together with mHealth providers to provide regulatory measures that are appropriate and proportional to the inherent risks and to the management thereof. Instead of analysing the numerous examples of mHealth services and the associated regulatory impact of each per African territory, a holistic "for Africa" Regulatory Impact Assessment Model has been created. This model aims to practically demonstrate different types of mHealth services that are possible in relation to increasing levels of care and health professional involvement in their delivery versus data usage and collection, as the complexity of the care given increases.

mHealth services to users /consumers

Health Content

- **General**
- **Condition-specific**

Access by a user to health content for educational purposes is possibly the most common and basic form of mHealth and takes the form of a one-off search for health information or opting-in to receive ongoing health information or tips, by selected health conditions or topics. Common categories found include education on pregnancy and infant care, education on malaria, HIV and nutrition support and/or guidelines.

Using a mobile device to search for health content via Google, for instance, is generally free to the user, apart from associated mobile data costs, but where daily information or tips are served to a user's mobile device, subscription costs or premium SMS costs were found to apply.

This is a one-way push of health content with no or minimal data being collected, apart from perhaps the user's mobile number, and where applicable a reference date which could be a birthing due date or a child's birth date. No interaction with a health professional exists and users can, or should be allowed to, opt-out from receiving the information at any time.

Group-based health education

One level above the basic healthcare information delivery, so-called group-based health education, involves a health professional providing remote education and guidance on a specific health topic at a pre-determined time and date to a group of individuals simultaneously. Information shared is not confidential and can be seen/heard by all participants. Examples found include electronic group, blog or chat discussions on sexual health, birth control, hygiene and basic first aid.

The level of care increases with the introduction of a healthcare professional and the possibility exists for increased data gathering and storage. It was found that this type of service was generally provided as a free educational initiative to users or participants.

Health Advice

- **Text**
- **Voice**

The providing of one-to-one remote mHealth advice by qualified health professionals (either nurse or doctor) moves significantly up the healthcare service levels value chain, with significant sharing of personal information and data. Advice on this level ranges from simple text-based questions and answers to talking to a healthcare professional.

Few examples of this level of mHealth delivery could be found in the territories under observation. Apart from the regulatory issues involved with this level of care, additional delivery implications include payment methodologies for the health advice given and whether ongoing subscription type services or fee-for service models are initiated.

Health Diagnosis

- **Voice**
- **Voice and image**

The most complex form of mHealth occurs where a remote user interfaces with a registered doctor by mobile phone, voice call or imaged-based Skype-type call, for health advice, consultation and potential symptom diagnosis, resulting in specific treatment advice with or without a medication prescription. The level of care given is at the top end of the scale with substantial data sharing, gathering and storage.

Whilst no examples of this level of mHealth care were found in the study, it is included for the purposes of completion. As the full spectrum of mHealth services become available so too does the requirement for greater regulatory involvement become more apparent.

mHealth services from one healthcare professional to another

This form of mHealth occurs where a health professional seeks remote advice, opinion and/or diagnosis from a more senior professional in another location, that is, traditional telemedicine. For instance, nurses/healthcare practitioners

in a clinic to a doctor in another centralised location, interpretation of x-rays/scans and the interpretation of pathology results. To the extent that these disciplines can leverage the existing health legislation/guidelines in place is good, however adjustments to the existing law may be required as there may be the need to address issues not legislated for.

Recommendations:

Risks and obligations vary on a continuum that involves multiple factors, including the degree of power or autonomy of the user/patient, the trust accorded the service/product, and the necessity and benefit to society. Some of these risks may be mitigated by regulation but a balance between over-regulation and too little regulation should be carefully considered.

General key findings and practical mHealth regulatory recommendations

- **Ensure that regulation is proactive, enabling and contextually appropriate.**
- **Establish a careful definition of the concept of mHealth, eHealth, telemedicine and what it means to 'practice' medicine**
- **Avoid a so-called 'one-size-fits-all' approach**
- **Incorporate both global and local approaches in solution-finding**
- **Engage in greater collaboration with international and regional agencies**
- **Encourage engagement with all national stakeholders**
- **Embrace private sector mHealth initiatives and cooperation between the public and private sectors**
- **Facilitate the granting of licenses to practice mHealth, if required, for e-diagnosis, e-prescribing or telemedicine, and appropriate guidelines and/or codes of conduct**
- **Consider the changing nature of the socio-cultural environment and the historical context**
- **Establish and transform regulatory bodies – including a telecommunications regulator, a data protection regulator and a cyber-crime prevention regulator**
- **Provide guidelines that address the quality and content of health information**
- **Clarify the responsibilities and limitations of the liability of ISPs**
- **Provide guidance and/or regulate medical device technology and medical software applications**
- **Safeguard users' rights to be the owners of their information and ensure that adequate data security, data protection and privacy laws are in place**
- **Ensure adequate standards for the transfer and exchange of data**
- **Encourage and find appropriate alternative and more pragmatic methods of performing activities in a virtual environment, so that they have the same effect as those carried out using traditional methods, including addressing issues of an evidential nature**

Conclusion

The study and literature reviewed unearthed some important findings about mHealth adoption and regulation in the ten target African countries. The implications of not having the necessary clear legal safeguards in place in the countries may have an adverse impact of the development of mHealth initiatives in the region. The potential to realise the benefits of mHealth and the need to institutionalise mHealth after adoption is a collaborative journey that all stakeholders need to embark on.

It is therefore recommended that African countries review the gaps found in their legal regimes and begin instituting appropriate measures to address them.

Only once these challenges have been suitably addressed by policy makers, and sustainable African-centric solutions found for the effective roll-out of robust mHealth initiatives, can the much needed scale be attained to address the continent's dire need for affordable and accessible preventative and primary healthcare.

Limitations of the review

Although this review may be a guide or overview of the existing legal position within the ten target countries, it is important to state that it is exploratory in nature, and aimed at presenting the beginnings of a picture of the regulatory situation in the area of mHealth. The study was limited in size and not a definitive solution to mHealth regulation but merely a means of highlighting points of discussion that require closer consideration and further research. Additionally, the legal provisions within the countries were those found, and provided to the author, at the time the research was conducted and, are of course, subject to amendment and change.

Abbreviations and terminology

AU – African Union
EU – European Union
IVR – Interactive Voice Response
ISP – Internet Service Provider
NCC – Nigerian Communications Commission
PAMI – Pan-African mHealth Initiative
SMS – Short Message Service
STD – Sexually Transmitted Disease

Appendix

Consolidated reports for countries under review, in alphabetical order.

COTE D'IVOIRE

m-Health road map/strategy

National eHealth (mHealth) strategy, policy or framework in place	Yes
Year adopted	2011
Implementation	Partially
Regulatory body that deals specifically with eHealth (mHealth) issues/initiatives	Unclear

Existing legal framework

Recognition and protection of an individuals right to healthcare	Yes
Recognition and protection of an individuals right to privacy	Yes
Indigenous law/traditional or customary law plays a role in the legal system	Yes
Member of	ECOWAS (Economic Community of West African States)
Member of the African Union	Yes
Policies or laws that regulate medical research	Yes

Privacy and Data Protection

Specific data protection legislation in place **Law No. 2013-450 on Protection of Personal Data (Cote D'Ivoire Law), enacted in August 2013.**	Yes
Data protection legislation provides for minimum standards of collected fairly and lawfully; • used only for the specified purpose for which it was originally collected; • adequate, relevant and not excessive to purpose; • accurate and up to date; • accessible to the subject; • kept secure; and • destroyed after its purpose is completed.	Yes/Limited
Privacy legislation covers public and/or private sectors or both	Both
Are cross border data exchanges restricted?	
- between the country and other African countries	Yes/unclear
- between the country and the EU	Yes/unclear
Country's data protection mechanisms compliant with the EU directive on data exchange	Unclear

Online Protection and e-regulation

e-Legislation **Ordinance N°2012-293 of March 21 2012 relating to Telecommunications and Information and Communication Technologies** **The Committee on Economic and Financial Affairs of the National Assembly of the Côte d'Ivoire has adopted the Bill on Electronic Transactions presented by the Minister of Post and Information Technology and Communication, Bruno Nabagné Kone.** **This law is designed to provide legal standards for the management of electronic transactions in Côte d'Ivoire, in line with international conventions ratified by Côte d'Ivoire, including legal instruments of ECOWAS, the African Union and the International Union Telecommunications.**	Yes
Regulation of online content	No government restrictions on access to the Internet. Voluntary compliance by content providers and government control.
Validity of electronic documents	Yes/Unclear
Validity of contracts concluded online	Yes/Unclear
Validity of e-signatures	Yes/Unclear

Licensure and registration of medical practioners

Requirement that medical practitioners are registered	Yes
Governing body that controls registration **National Council of the Order of Physicians**	Yes
Requirement for the licensing or accreditation of medical practitioners who practice eHealth	Yes
Medical practitioners can do the following online:	
- provide advice online	Unclear
- diagnose online (e-consultations)	Unclear
- prescribe medicine online (e-prescribing)	Unclear
- dispense medicine online (e-dispensing of medicine)	Unclear
Requirement for the licensing or accreditation of online e- health applications	Unclear

Content control and liability of service providers

Provisions in place that protect service providers under certain conditions	None/unsure

Medical device regulations

Medical device technology regulations	Yes

Consumer protection

Law that governs consumer protection **Ordinance N°2012-293 of March 21 2012 relating to Telecommunications and Information and Communication Technologies Art 66 provides direct marketing requirements.**	Yes

Regulatory bodies

telecommunications regulatory body **ARTCI - Autorite de regulation des telecommunications/tic de Cote d'Ivoire**	Yes
regulatory body that oversees data protection	Yes

m-Health road map/strategy

National eHealth (mHealth) strategy, policy or framework in place	Yes
Year adopted	2010
eHealth (mHealth) policy "embedded" in a larger e-government policy or as a part of a broader health or teleHealth policy	Stand-alone policy
Implementation	Partially
Regulatory body that deals specifically with eHealth (mHealth) issues/initiatives	Yes
Name of regulatory body GHANA HEALTH SERVICE	
Role of government in eHealth development	Guided market
Governance and policy mechanisms in place at a national, regional and/or local level to ensure implementation, support and monitoring of the strategy	Yes
EHealth (mHealth) codes of practice or guidelines in place	Unclear
Any failed or stalled attempts to develop an eHealth policy and legislation	No
Policies or law defining liability and re-imbursement for eHealth (mHealth) services	Yes

Existing legal framework

Recognition and protection of an individuals right to healthcare	Yes
Recognition and protection of an individuals right to privacy	Yes
Recognition and protection of the right of individuals to access information held by the government/state	Yes
Indigenous law/traditional or customary law plays a role in the legal system	Yes
Member of	ECOWAS (Economic Community of West African States)
Member of the African Union	Yes
Policies or laws that regulate medical research	Yes

Online Protection and e-regulation

Monitoring and/or control of information and content over an electronic medium by service providers?	Yes
Consumer protection legislation in place that protects users in an online environment	Yes
Regulation of online content	Yes
Validity of electronic documents	Yes
Validity of contracts concluded online	Yes
Validity of e-signatures	Yes
Policies exist to promote e-commerce and services provision (e.g. e-signatures) in all sectors	e-Ghana - not fully developed
Policies for quality criteria, information management and sale of medicines and regulated health products online?	No

Privacy and Data Protection

Specific data protection legislation in place.	Yes
Legislation in place that governs how health information is stored and accessed across geographical and health-sector boundaries?	Yes
Data protection legislation covers private and/or public sectors	Both
Regulation addresses individuals' choice to 'opt in' or 'opt out' of the collection of their personal health information?	Yes
Regulations that control 'direct marketing'	Yes
Are cross border data exchanges restricted?	
- between the country and other African countries	Yes/unclear
- between the country and the EU	Yes/unclear
Country's data protection mechanisms compliant with the EU directive on data exchange	Unclear
Policies for equity of access to information including for gender and other sociocultural groups	Yes
Requirement in the law to protect personal or 'sensitive' data	Yes
Provisions governing 'research data'	Yes

Licensure and registration of medical practitioners

Requirement that medical practitioners are registered	Yes
Governing body that controls registration	Yes
Requirement for the licensing or accreditation of medical practitioners who practice eHealth	Yes/Not specific
'Informed consent'/consent required in an eHealth consultation	Yes
Can consent be obtained electronically	Yes
Establishment of a patient-doctor relationship before a patient can be treated	No
Clearly defined medical jurisdiction for medical practitioners	Yes
Medical practitioners can do the following online:	
- provide advice online	Yes
- diagnose online (e-consultations)	Yes/No clear guidelines
- prescribe medicine online (e-prescribing)	Yes/No clear guidelines
- dispense medicine online (e-dispensing of medicine)	Yes/No clear guidelines
Requirement for the licensing or accreditation of online e- health applications	Yes
eHealth (mHealth) or telemedicine guidelines/codes of practice in place	Yes

Content control and liability of service providers

Provisions in place that protect service providers under certain conditions	Unsure
Law protecting service providers in respect of material transmitted or posted on their service where they are notified about infringing material or where they are under an obligation by contract, licence or law to remove, block or deny access to specified material	Unsure
Law provides a mechanism whereby content can be removed at the instance of notification by a user	Yes

Medical device regulations

Medical device technology regulations	Yes
eHealth (mHealth) suppliers need accreditation	Yes/unclear

Consumer protection

Law that governs consumer protection	Yes
Consumer protection laws require that certain information regarding the service or product be made available to the user	Yes
Law requires that a consumer be offered an opportunity to withdraw from the transaction	Yes
Law requires a person offering services electronically to use a secure and technologically accepted payment system?	Yes

Regulatory bodies

eHealth (mHealth) regulatory body NITA	Yes
telecommunications regulatory body NATIONAL COMMUNICATION AUTHORITY	Yes
regulatory body that oversees data protection NATIONAL COMMUNICATION AUTHORITY	Yes
Cyber crime prevention regulatory authority NATIONAL COMMUNICATION AUTHORITY	Yes

m-Health road map/strategy

National eHealth (mHealth) strategy, policy or framework in place		Yes
Year adopted		2011
eHealth (mHealth) policy "embedded" in a larger e-government policy or as a part of a broader health or teleHealth policy		Stand-alone policy
Implementation		Partially
eHealth legislation	Although healthcare legislation and the regulation of health providers is entrenched in Kenya's statutes (Public Health Act, Pharmacy and Poisons Act amongst others), the Health Bill of 2014 provides in Part 18 specific eHealth and e-legislation. ' The Cabinet Secretary, in consultation with the Director General for Health shall ensure the enactment of legislation that provides for among other things: - Functional Domains; … - Administration of Health Information Banks including interoperability framework, data interchange and security; - Collection and use of personal health information; - Management of disclosure of personal health information; - Protection of privacy; … - Business continuity, Emergency and disaster preparedness; .... - Health service delivery through MHealth, E-learning, Tele-Medicine; - e-Waste disposal; and ... - Medical Tourism'	
Governance and policy mechanisms in place at a national, regional and/or local level to ensure implementation, support and monitoring of the strategy		Yes / Draft
THE HEALTH BILL OF 2014	Undergoing internal review and stakeholder consultation	
Any failed or stalled attempts to develop an eHealth policy and legislation		No/Unclear

Existing legal framework

Recognition and protection of an individuals right to healthcare	Yes
Recognition and protection of an individuals right to privacy	Yes
Indigenous law/traditional or customary law plays a role in the legal system	Yes
Indigenous law/traditional or customary law plays a role in the legal system	Yes
Member of	EAC (East African Community)
Member of the African Union	Yes
Policies or laws that regulate medical research	Yes

Privacy and Data Protection

Specific data protection legislation in place. **The DATA PROTECTION BILL OF 2013 (expected to be tabled at the end of May 2014). Specific data protection provisions including e-commerce contained in Kenya Information and Communication Act (KICA) as read with the Kenya Information and Communication (Consumer Protection) Regulations. Also provided for in the 2014 Health Bill.**	Yes/Draft
Privacy legislation covers public and/or private sectors or both	Both
Are cross border data exchanges restricted?	
- between the country and other African countries	
- between the country and the EU'	
Country's data protection mechanisms compliant with the EU directive on data exchange	Unclear
Data protection legislation provides for minimum standards of collected fairly and lawfully; • used only for the specified purpose for which it was originally collected; • adequate, relevant and not excessive to purpose; • accurate and up to date; • accessible to the subject; • kept secure; and • destroyed after its purpose is completed.	Draft
Remedy available for breach of privacy (for instance in delict / tort)	Yes

Licensure and registration of medical practitioners

Requirement that medical practitioners are registered	Yes
Governing body that controls registration Healthcare practitioners are bound by their healthcare regulatory bodies, for example, the Kenya Medical Practitioners and Dentists Board and related health Acts concerning ICT in healthcare.	Yes
Medical practitioners can do the following online **Although telemedicine is well established, legalities around e-consulting, e-prescribing and e-dispensing remain unclear at this stage**.	
- provide advice online	Unclear
- diagnose online (e-consultations).	Unclear
- prescribe medicine online (e-prescribing)	Unclear
- dispense medicine online (e-dispensing of medicine)	Unclear
Requirement for the licensing or accreditation of online e- health applications	Unclear

Content control and liability of service providers

Provisions in place that protect service providers under certain conditions	No / limited

Online Protection and e-regulation

Regulation of online content	Yes, voluntary compliance by content providers and government control
Validity of electronic documents Kenya Information and Communication Act (KICA), Chapter 411A of the Laws of Kenya, which was passed in January 2009. Kenya Communications (Electronic Transactions) Regulations were passed in 2010.	Yes
Validity of contracts concluded online	Yes
Validity of e-signatures	Yes
Policies exist to promote e-commerce and services provision (e.g. e-signatures) in all sectors	Yes

Medical device regulations

eHealth (mHealth) suppliers need accreditation	Draft HEALTH BILL to provide - Part 7—Regulation of Health Products and Technologies 43—Establishment of single Regulatory body for Health Products and Technologies Part 8—Procurement, of Health Products and Technologies

Consumer protection

Law that governs consumer protection **Kenya enacted a Consumer Protection Act in 2012. Additionally, Kenya Information and Communication (Consumer Protection) Regulations read with the KICA. The Act also provides for agreements and transactions entered into over the Internet.**	Yes

Regulatory bodies

telecommunications regulatory body COMMUNICATIONS AUTHORITY OF KENYA	Yes

m-Health Regulatory Impact Assesment in Africa — MALAWI

m-Health road map/strategy

National eHealth (mHealth) strategy, policy or framework in place	Yes
Year adopted	

Existing legal framework

Recognition and protection of an individuals right to healthcare	Yes
Recognition and protection of an individuals right to privacy	Yes
Member of	SADC (Southern African Development Community)
Member of the African Union	Yes

Privacy and Data Protection

Specific data protection legislation in place. **The drafting of electronic legislation the Electronic Transactions and Management Bill of 2013 contains data protection provisions.The legislation will also guide in maintaining a secure space where data could be stored, shared and legally and securely transferred. The Bill offers 'data protection' with specific provisions in order to regulate online collection of personal information regarding users and imposing systematic information on the purposes of the data processing and the rights of the data subject.**	Draft
Data protection legislation provides for minimum standards of collected fairly and lawfully; • used only for the specified purpose for which it was originally collected; • adequate, relevant and not excessive to purpose; • accurate and up to date; • accessible to the subject; • kept secure; and • destroyed after its purpose is completed.	Draft
Country's data protection mechanisms compliant with the EU directive on data exchange	Unclear
Remedy available for breach of privacy in common/civil law (for instance in delict / tort)	Yes

Consumer protection

Law that governs consumer protection **The Bill regulates online purchase of goods and services under the section 'Consumer protection with respect to e-commerce'. It provides that online purchase of services or goods require the adoption of specific provisions in addition to traditional consumer rules. Moreover, it places specific obligations on professionals regarding the display of information as well as online advertising.**	

Online Protection and e-regulation

Validity of electronic documents **Electronic Transactions and Management Bill of 2013. The Bill includes the legal recognition of electronic messages, proceedings applicable to the conclusion of electronic contracts, consumer protection with respect to e-commerce and Encryption. The Bill also deals with issues of cybercrime, data protection, domain names and e-Government.** **The Bill provides for 'proceedings applicable to the conclusion of electronic contracts' - where it is specifies and clarifies rules regulating the conclusion of contracts in order to ensure security with respect to electronic transactions.**	Draft
Validity of contracts concluded online	Draft
Validity of e-signatures	Draft

Licensure and registration of medical practitioners

Requirement that medical practitioners are registered	Yes
Governing body that controls registration	Yes
Medical practitioners can do the following online	
- provide advice online	Unclear
- diagnose online (e-consultations).	Unclear
- prescribe medicine online (e-prescribing)	Unclear
- dispense medicine online (e-dispensing of medicine)	Unclear
Requirement for the licensing or accreditation of online e- health applications	Unclear

Content control and liability of service providers

Content control Yes **The Censorship and Control of Entertainment Act prohibits the printing, publishing, manufacturing of any publication … which is 'undesirable'. 'Undesirable' is that which is obscene or indecent, offensive to religious convictions or feelings, contrary to the interests of public safety.**	Yes
Provisions in place that protect service providers under certain conditions **The proposed legislation also seeks 'legal responsibility of various actors' with respect to the Internet. It observes that as it is the case regarding television, radio, or written press, the freedom of speech should be limited by certain principles of public order. The Bill defines precisely the responsibility of technical service providers and editors of online contents. The Bill's chapter three of Part III, which has the headline 'Online user's protection and liability of intermediaries and content editors', defines who the editors are in Section 23. The draft Bill describes operators as intermediary, who are any legal or physical person or any entity that provides electronic communications services consisting of the provision of access to communication networks, as well as storing or transmission of information through communication networks.**	Draft

Regulatory bodies

telecommunications regulatory body COMMUNICATIONS AUTHORITY OF KENYA	Yes

MOZAMBIQUE

The health system in Mozambique has traditionally been controlled by ministerial decrees by the Ministry of Health with input from the medical profession.

In the 1970s to the 1990s, a focus on primary healthcare was sought and public sector regulation has recently moved towards hospital-based urban services. The private sector is largely regulated by quality, profession and price legislation.

m-Health road map/strategy

National eHealth (mHealth) strategy, policy or framework in place	Yes
Year adopted	2011
eHealth (mHealth) policy "embedded" in a larger e-government policy or as a part of a broader health or teleHealth policy	Stand-alone policy
Implementation	Partially
Any failed or stalled attempts to develop an eHealth policy and legislation	Unclear

Existing legal framework

Recognition and protection of an individuals right to healthcare	Yes
Recognition and protection of an individuals right to privacy **Article 68 of the Constitution of Mozambique provides' [t]he home and the correspondence or other forms of private communictaion shall be inviolable, except in cases specifically provided for by law'.** **Article 71 provides for ' Use of Computerised Data** **1. The use of computerised means for recording and processing individually identifiable data in respect of political, philosophical or ideological beliefs, of religious faith, party or trade union affiliation or private lives, shall be prohibited.** **2. The law shall regulate the protection of personal data kept on computerised records, the conditions of access to data banks, and the creation and use of such data banks and information stored on computerised media by public authorities and private entities.** **3. Access to data bases or to computerised archives, files and records for obtaining information on the personal data of third parties, as well as the transfer of personal data from one computerised file to another that belongs to a distinct service or institution, shall be prohibited except in cases provided for by law or by judicial decision.** **4. All persons shall be entitled to have access to collected data that relates to them and to have such data rectified.'**	Yes
Indigenous law/traditional or customary law plays a role in the legal system **The official recognition of legal pluralism has been specifically provided for in the Constitution of Mozambique of 2004 where in article 3 it is provided '[t]he The Republic of Mozambique is a State governed by the rule of law, based on pluralism of expression and democratic political organisation and on the respect for and guarantee of fundamental human rights and freedoms.' And again in article 4 entitled 'Legal Pluralism' it provides, '[t]he State recognises the different normative and dispute resolution systems that coexist in Mozambican society, insofar as they are not contrary to the fundamental principles and values of the Constitution.'**	
Member of	SADC (Southern African Development Community)
Member of the African Union	Yes

Privacy and Data Protection

Specific data protection legislation in place. **The Civil Code (Administrative Ordinance no. 22869 of 1967 provides that everyone shall keep private any information concerning another's private life. This broad provision provides privacy protection which may also find application in electronic data.**	Yes
Privacy legislation covers public and/or private sectors or both	Both
Data protection legislation provides for minimum standards of collected fairly and lawfully; • used only for the specified purpose for which it was originally collected; • adequate, relevant and not excessive to purpose; • accurate and up to date; • accessible to the subject; • kept secure; and • destroyed after its purpose is completed	Yes/limited
- between the country and other African countries	Unclear
- between the country and the EU	Unclear
Country's data protection mechanisms compliant with the EU directive on data exchange	Unclear
Remedy available for breach of privacy in common/civil law (for instance in delict / tort)	Yes

Online Protection and e-regulation

Regulation of online content **Limited approach taken to ensure quality of health related content online.** **The Mozambican government is proposing a bill (April 2014) that will criminalise text messages, emails and other types of online posts that are considered "insulting" or that "jeopardize the security of the state". It is unclear whether this has been passed.**	Limited
Validity of electronic documents **Electronic Transactions Act :**	*Yes/unsure*
Validity of contracts concluded online	Unclear
Validity of e-signatures	Unclear

Licensure and registration of medical practitioners

Requirement that medical practitioners are registered	Yes
Governing body that controls registration	Yes
Can consent be obtained electronically	Unclear
Medical practitioners can do the following online	
- provide advice online	Unclear
- diagnose online (e-consultations).	Unclear
- prescribe medicine online (e-prescribing)	Unclear
- dispense medicine online (e-dispensing of medicine)	Unclear
Requirement for the licensing or accreditation of online e- health applications	Unclear

Content control and liability of service providers

Provisions in place that protect service providers under certain conditions	No/unclear

Consumer protection

Law that governs consumer protection	Limited

Regulatory bodies

telecommunications regulatory body **Instituto Nacional das Communicacoes de Mozambique (INCM)**	Yes

NIGERIA

m-Health road map/strategy

National eHealth (mHealth) strategy, policy or framework in place	Nigeria does not have an explicit eHealth policy however, the National Strategy Health Development Plan Framework (2009 - 2015) states 'Use of information technology on HIS will be strenghtened, and decentralised software-based systems for data collection and analysis will be promoted public-private partnerships in the management of data warehouses will be established as well as mechanisms to enhance the wide use of eHealth data, such as through electronic management Intelligence Information System, websites, patient information systems, etc'. (paragraph 2.5.5.8 at p. 40)
Regulatory body that deals specifically with eHealth (mHealth) issues/initiatives	No – Although Nigeria does not have a regulatory body that deals specifically with eHealth initiatives/issues, section 6 (c) of the National Information Technology Development Agency (NITDA) of 2007 grants the NITDA powers to 'develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper based methods in government, commerce, education, and the public and private sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information'. The NITDAis empowered to set regulatory standards and guidelines for eHealth initiatives.
Role of government in eHealth development	None - currently the role of government or market actors in the development of eHealth has not been explicitly defined by any policy or legal framework
Governance and policy mechanisms in place at a national, regional and/or local level to ensure implementation, support and monitoring of the strategy	No
Any failed or stalled attempts to develop an eHealth policy and legislation	Yes. In December 2011 a national conference on ICT Health was organised by the government which led to a decision to develop a policy and strategy for implementating eHealth in Nigeria. There is presently no information on the subsequent developments that followed the national conference in December 2011.
Policies or law defining liability and re-imbursement for eHealth (mHealth) services	None / unknown

Privacy and Data Protection

Specific data protection legislation in place	No
Legislation in place that governs how health information is stored and accessed across geographical and health-sector boundaries?	No
Regulation addresses individuals' choice to 'opt in' or 'opt out' of the collection of their personal health information?	No
Regulations that control 'direct marketing	No
Are cross border data exchanges restricted?	
- between the country and other African countries	No
- between the country and the EU	No
Country's data protection mechanisms compliant with the EU directive on data exchange	No
Policies for equity of access to information including for gender and other sociocultural groups	No
Enforcement and sanctions mechanisms built into the law	No
Requirement in law to protect personal or 'sensitive' data	No

Existing legal framework

Recognition and protection of an individuals right to healthcare	Yes
Recognition and protection of an individuals right to privacy	Yes
Recognition and protection of the right of individuals to access information held by the government/state	Yes
Indigenous law/traditional or customary law plays a role in the legal system	Yes
Member of	ECOWAS (Economic Community of West African States)*
Member of the African Union	Yes
Policies or laws that regulate medical research NATIONAL CODE FOR HEALTH RESEARCH ETHICS IN NIGERIA (2007)	Yes

Licensure and registration of medical practitioners

Requirement that medical practitioners are registered	Yes
Governing body that controls registration THE NIGERIAN MEDICAL AND DENTAL COUNCIL	Yes
Requirement for the licensing or accreditation of medical practitioners who practice eHealth	No additional requirements
'Informed consent'/consent required in an eHealth consultation	No
Can consent be obtained electronically NIGERIAN EVIDENCE ACT 2011	Yes
Establishment of a patient-doctor relationship before a patient can be treated	Yes, unless emergency
Clearly defined medical jurisdiction for medical practitioners	No
Medical practitioners can do the following online:	
- provide advice online	Yes/limited
- diagnose online (e-consultations)	No
- prescribe medicine online (e-prescribing)	Yes/limited
- dispense medicine online (e-dispensing of medicine)	No/unclear
Requirement for the licensing or accreditation of online e- health applications	No
eHealth (mHealth) or telemedicine guidelines/codes of practice in place	No

Content control and liability of service providers

Provisions in place that protect service providers under certain conditions NIGERIAN COMMUNICATIONS COMMISSION GUIDELINES FOR THE PROVISION OF INTERNET SERVICES (2007) ESTABLISHED UNDER S 70(2) OF THE NIGERIAN COMMUNICATIONS ACT 2003	Yes
Law protecting service providers in respect of material transmitted or posted on their service where they are notified about infringing material or where they are under an obligation by contract, licence or law to remove, block or deny access to specified material	Yes
In the case of infringing material, is a service provider only liable where…	e has actual knowledge that the material is infringing or is notified about the infringement (a notice to take down) and does not remove the material or link to the material within a reasonable time.
Law provides a mechanism whereby content can be removed at the instance of notification by a user, 'take down notices'.	Yes

Online Protection and e-legislation

Monitoring and/or control of information and content over an electronic medium by service providers?	No
Consumer protection legislation in place that protects users in an online environment.	No
Regulation of online content	No
Validity of electronic documents	Yes
Validity of contracts concluded online	Yes
Validity of e-signatures	Yes
Policies exist to promote e-commerce and services provision (e.g. e-signatures) in all sectors NATIONAL BROADBAND PLAN (2013 – 2018) NATIONAL INFORMATION COMMUNICATION TECHNOLOGY POLICY (2012) REPORT OF THE VISION 2020 NATIONAL TECHNICAL WORKING GROUP ON ICT (2009) NATIONAL POLICY FOR INFORMATION TECHNOLOGY (2010)	Yes
Policies for quality criteria, information management and sale of medicines and regulated health products online	Yes
NATIONAL AGENCY FOR FOOD AND DRUG ADMINISTRATION AND CONTROL ACT	

Medical device regulations

Medical device technology regulations SRANDARDS ORGANIZATION OF NIGERIA ACT CONSUMER PROTECTION (PRODUCTS AND SERVICES MONTORING AND REGISTRATION) REGULATIONS 2005.	Yes
Regulations control medical device technology	Both hardware and software
eHealth (mHealth) suppliers need accreditation	Only in as far as other similar non eHealth providers do

Consumer protection

Law that governs consumer protection	Yes
Consumer protection laws require that certain information regarding the service or product be made available to the user	Yes
Law applies to goods, services and transactions conducted…	Over an electronic medium (i.e. e-transaction) and conventional methods of transacting
Law requires that a consumer be offered an opportunity to withdraw from the transaction	No
Law requires a person offering services electronically to use a secure and technologically accepted payment system?	No

Regulatory bodies

eHealth (mHealth) regulatory body	No
telecommunications regulatory body	Yes
regulatory body that oversees data protection	None/unsure

m-Health Regulatory Impact Assesment in Africa — RWANDA

m-Health road map/strategy

National eHealth (mHealth) strategy, policy or framework in place	Yes
Year adopted	2014
eHealth (mHealth) policy "embedded" in a larger e-government policy or as a part of a broader health or teleHealth policy	Stand-alone policy
Implementation	Fully
Regulatory body that deals specifically with eHealth (mHealth) issues/initiatives	Yes
Name of regulatory body **eHealth Unit in the Ministry of Health**	
Role of government in eHealth development	Fully regulated
Governance and policy mechanisms in place at a national, regional and/or local level to ensure implementation, support and monitoring of the strategy	Yes, still in development
EHealth (mHealth) codes of practice or guidelines in place	No / unsure
Any failed or stalled attempts to develop an eHealth policy and legislation	None

Existing legal framework

Recognition and protection of an individuals right to healthcare	Yes
Recognition and protection of an individuals right to privacy	Yes
Member of	EAC (East African Community)
Member of the African Union	Yes
Rwanda has historically had a civil law system, it has begun to move towards a common law system to align itself with the harmonisation requirements after admission into the East African Community and the Commonwealth.	
Policies or laws that regulate medical research	Yes

Privacy and Data Protection

Specific data protection legislation in place Partial reference made in Chapter XVI of the Telecommunications Law. No comprehensive regime exists.	Yes
Data protection legislation provides for minimum standards of collected fairly and lawfully; • used only for the specified purpose for which it was originally collected; • adequate, relevant and not excessive to purpose; • accurate and up to date; • accessible to the subject; • kept secure; and • destroyed after its purpose is completed.	Yes / limited
Country's data protection mechanisms compliant with the EU directive on data exchange	Unclear

Online Protection and e-legislation

Monitoring and/or control of information and content over an electronic medium by service providers?	Yes
Validity of electronic documents **Enactment of a law governing electronic messages, electronic signatures, electronic transactions, data protection and cyber security in May 2010 - Law no.18/2010.**	Yes
Validity of contracts concluded online	Yes
Validity of e-signatures	Yes

Licensure and registration of medical practitioners

Requirement that medical practitioners are registered	Yes
Governing body that controls registration	Yes
Requirement for the licensing or accreditation of medical practitioners who practice eHealth	Yes
Medical practitioners can do the following online:	
- provide advice online	Unclear
- diagnose online (e-consultations)	Unclear
- prescribe medicine online (e-prescribing)	Unclear
- dispense medicine online (e-dispensing of medicine)	Unclear
Requirement for the licensing or accreditation of online e- health applications	Unclear

Content control and liability of service providers

Provisions in place that protect service providers under certain conditions **Law no.18/2010, Chapter III, provides immunity from liability for service providers and intermediaries for third-party content where conditions are meet.**	Yes

Consumer protection

Law that governs consumer protection	Yes

Regulatory bodies

telecommunications regulatory body	Yes

m-Health road map/strategy

National eHealth (mHealth) strategy, policy or framework in place	Yes
Year adopted	2012
eHealth (mHealth) policy "embedded" in a larger e-government policy or as a part of a broader health or teleHealth policy	Stand-alone policy
Implementation	Partially
Regulatory body that deals specifically with eHealth (mHealth) issues/initiatives	Yes
Role of government in eHealth development	Guided market
Governance and policy mechanisms in place at a national, regional and/or local level to ensure implementation, support and monitoring of the strategy	Yes
EHealth (mHealth) codes of practice or guidelines in place	
Any failed or stalled attempts to develop an eHealth policy and legislation	No
Policies or law defining liability and re-imbursement for eHealth (mHealth) services	No / uncertain

Existing legal framework

Recognition and protection of an individuals right to healthcare	Yes
Recognition and protection of an individuals right to privacy	Yes
Indigenous law/traditional or customary law plays a role in the legal system	Yes
Member of: EAC (East African Community) SADC (Southern African Development Community)	
Member of the African Union	Yes
Policies or laws that regulate medical research	Yes

Online Protection and e-legislation

Monitoring and/or control of information and content over an electronic medium by service providers?	No
Consumer protection legislation in place that protects users in an online environment	Limited
Regulation of online content	No
Validity of electronic documents DRAFT ELECTRONIC TRANSACTIONS BILL 2014	Draft
Validity of contracts concluded online	Yes
Validity of e-signatures	Draft
Policies exist to promote e-commerce and services provision (e.g. e-signatures) in all sectors ICT POLICY 2003, E-GOVERNMENT STRATEGY	Yes
Policies for quality criteria, information management and sale of medicines and regulated health products online?	No

Privacy and Data Protection

Specific data protection legislation in place DRAFT DATA PROTECTION BILL 2014 HIV&AIDS (Prevention and Control) Act of 2008 provides at a high level for the disclosure (without patient consent) records related to HIV/AIDS	Draft
Legislation in place that governs how health information is stored and accessed across geographical and health-sector boundaries?	No
Regulation addresses individuals' choice to 'opt in' or 'opt out' of the collection of their personal health information?	No
Remedy available for breach of privacy (for instance in delict / tort)	Yes
Regulations that control 'direct marketing'	Yes
Are cross border data exchanges restricted?	
- between the country and other African countries	No
- between the country and the EU	No
Country's data protection mechanisms compliant with the EU directive on data exchange	No
Policies for equity of access to information including for gender and other sociocultural groups	No
Enforcement and sanctions mechanisms built into the law	No
Requirement in the law to protect personal or 'sensitive' data	No
Provisions governing 'research data'	Yes

Licensure and registration of medical practitioners

Requirement that medical practitioners are registered Established the GUIDING PRINCIPLES ON MEDICAL ETHICS AND HUMAN RIGHTS INTANZANIA (CODE OF ETHICS OF MEDICAL PROFESSION IN TANZANIA)	Yes
Governing body that controls registration TANZANIA MEDICAL COUNCIL	Yes
Requirement for the licensing or accreditation of medical practitioners who practice eHealth	Not specific
'Informed consent'/consent required in an eHealth consultation	Yes
Can consent be obtained electronically	Unclear
Establishment of a patient-doctor relationship before a patient can be treated	Yes
Clearly defined medical jurisdiction for medical practitioners	No
Medical practitioners can do the following online:	
- provide advice online	No clear guidelines
- diagnose online (e-consultations)	No clear guidelines
- prescribe medicine online (e-prescribing)	No clear guidelines
- dispense medicine online (e-dispensing of medicine)	No clear guidelines
Requirement for the licensing or accreditation of online e- health applications	Yes
eHealth (mHealth) or telemedicine guidelines/codes of practice in place	No

Content control and liability of service providers

Provisions in place that protect service providers under certain conditions	No
Law protecting service providers in respect of material transmitted or posted on their service where they are notified about infringing material or where they are under an obligation by contract, licence or law to remove, block or deny access to specified material	No
Law provides a mechanism whereby content can be removed at the instance of notification by a user	No

Medical device regulations

Medical device technology regulations	No
eHealth (mHealth) suppliers need accreditation	No

Consumer protection

Law that governs consumer protection		Yes
Consumer protection laws require that certain information regarding the service or product be made available to the user		Yes
Law applies to goods, services and transactions conducted…	over an electronic medium (i.e. e-transaction) and to conventional methods of transacting	
Law requires that a consumer be offered an opportunity to withdraw from the transaction		Yes
Law requires a person offering services electronically to use a secure and technologically accepted payment system?		No

Regulatory bodies

eHealth (mHealth) regulatory body	Yes
telecommunications regulatory body	Yes
regulatory body that oversees data protection	No

m-Health road map/strategy

National eHealth (mHealth) strategy, policy or framework in place	Yes
Year adopted	2012/2013
eHealth (mHealth) policy "embedded" in a larger e-government policy or as a part of a broader health or teleHealth policy	Stand-alone policy
Implementation	Partially
Regulatory body that deals specifically with eHealth (mHealth) issues/initiatives	Yes
Governance and policy mechanisms in place at a national, regional and/or local level to ensure implementation, support and monitoring of the strategy	Yes
Any failed or stalled attempts to develop an eHealth policy and legislatio	None known
Medical codes of conduct	Yes

Existing legal framework

Recognition and protection of an individuals right to healthcare	Yes
Recognition and protection of an individuals right to privacy	Yes
Recognition and protection of the right of individuals to access information held by the government/state	Yes
Member of	EAC (East African Community
Member of the African Union	Yes
Policies or laws that regulate medical research **National Guidelines for Research Involving Humans as Research Participants (2007) with regard to research participants and the collection of research data.**	Yes

Licensure and registration of medical practitioners

Requirement that medical practitioners are registered	Yes
Governing body that controls registration **Uganda Medical and Dental Practitioners Council**	Yes
Can consent be obtained electronically	Unclear but likely as e-contracts val
Medical practitioners can do the following online:	
- provide advice online	Unclear
- diagnose online (e-consultations)	Unclear
- prescribe medicine online (e-prescribing)	Unclear
- dispense medicine online (e-dispensing of medicine)	Unclear
Requirement for the licensing or accreditation of online e- health applications **No stand alone laws that apply to eHealth or health data.**	Unclear

Privacy and Data Protection

Specific data protection legislation in place **Uganda opened a public consultation, on 15 November 2014, regarding a draft Data Protection and Privacy Bill 2014. If passed by the Ugandan Parliament, the Bill would become Uganda's first piece of legislation which focuses exclusively on privacy and data protection.**	Limited/Bill
Data protection legislation provides for minimum standards of collected fairly and lawfully; • used only for the specified purpose for which it was originally collected; • adequate, relevant and not excessive to purpose; • accurate and up to date; • accessible to the subject; • kept secure; and • destroyed after its purpose is completed.	Limited/ inadequate
Country's data protection mechanisms compliant with the EU directive on data exchange	Unclear
Constitutional recognition and protection of an individuals right to privacy **Article 27 of the Constitution of Uganda contains '[r]ight to privacy of person, home and other property' and 41 containing the '[r]ight of access to information' of the Constitution of the Republic of Uganda, 1995 and the Uganda Communications Act of 2000. The Ugandan Human Rights Commission (UHRC) is tasked to monitor and advance human rights in Uganda. Additionally, it deals with the delimitation of conflicting rights, a matter which is not left to the courts. Uganda does not have a Data Protection Authority. Consequently, the UHRC is the only body dealing with complaints and violations arising out of the abuse of rights relating to privacy.**	Yes

Online Protection and e-legislation

e-Legislation **Process of formulating cyberlaws in Uganda was initiated in 2003 - a national taskforce led by the Uganda Law Reform Commission was set up to undertake the exercise. However laws not enacted until 2011.** **Ugandan Electronic Transactions Act 8 or 2011, the Computer Misuse Act of 2011 and the Electronic Signatures Act of 2011 provide the backbone of the e-legislative framework.**	Yes
Regulation of online content **Generally, the existing law does not provide for monitoring and controlling the information transmitted over an electronic medium. Voluntary compliance and some government assurance.**	Limited
Validity of electronic documents **Functional equivalence to e-transactions and communications ito Electronic Transactions Act 8 or 2011.**	Yes
Validity of contracts concluded online	Yes
Validity of e-signatures **E-signatures recognized ito Electronic Signatures Act of 2011.**	Yes
Policies exist to promote e-commerce and services provision (e.g. e-signatures) in all sectors	Yes

Content control and liability of service providers

Provisions in place that protect service providers under certain conditions **Uganda has specific limitations of intermediary/service provider liability provisions or 'safe harbour provisions'. Under section 29 of the Electronic Transactions Act of 2011 a service provider is not subject to civil or criminal liability in respect of third party material which is in the form of electronic records to which he merely provides access, acts as a conduit or merely links or refers to.**	Yes
Law protecting service providers in respect of material transmitted or posted on their service where they are notified about infringing material or where they are under an obligation by contract, licence or law to remove, block or deny access to specified material	Yes
Law provides a mechanism whereby content can be removed at the instance of notification by a user **Notice and take down procedures provided for ito of the 2011 Act.**	No

Medical device regulations

Medical device technology regulations	Yes

Consumer protection

Law that governs consumer protection **No general consumer protection law. However, sections 24 to 28 of the Electronic Transactions Act offer a degree of protection to consumers involved in e-transactions. It also requires that an opportunity should be provided to withdraw from the electronic transaction before it is concluded and requires a person offering services electronically to use a secure and technologically accepted payment system. Section 28 makes it unlawful for an electronic medium to contain a provision that purports to exclude the rights of consumers as provided for under the Act.**	Limited

Regulatory bodies

telecommunications regulatory body UGANDAN COMMUNICATION COMMISSION	Yes
regulatory body that oversees data protection	No / unknown

m-Health Regulatory Impact Assesment in Africa — ZAMBIA

m-Health road map/strategy

National eHealth (mHealth) strategy, policy or framework in place	Yes
Year adopted	2013
eHealth (mHealth) policy "embedded" in a larger e-government policy or as a part of a broader health or teleHealth policy NATIONAL HEALTH STRATEGIC PLAN	Embedded
Implementation	Partially
Regulatory body that deals specifically with eHealth (mHealth) issues/initiatives	No
Governance and policy mechanisms in place at a national, regional and/or local level to ensure implementation, support and monitoring of the strategy	No
Role of government in eHealth development	Free Market
EHealth (mHealth) codes of practice or guidelines in place	Uncertain
Any failed or stalled attempts to develop an eHealth policy and legislation	No

Existing legal framework

Recognition and protection of an individuals right to healthcare	Yes
Recognition and protection of an individuals right to privacy	Yes
Recognition and protection of an individuals right to access information held by the state	Yes
Indigenous law/traditional or customary law plays a role in the legal system	Yes
Member of	SADC (Southern African Development Community)
Member of the African Union	Yes
Policies or laws that regulate medical research	Yes
MEDICAL RESEARCH IS GUIDED BY THE ETHICS COMMITTEE OF THE UNIVERSITY OF ZAMBIA	

Content control and liability of service providers

Provisions in place that protect service providers under certain conditions THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 21 OF 2009 PART X	Yes
Law protecting service providers in respect of material transmitted or posted on their service where they are notified about infringing material or where they are under an obligation by contract, licence or law to remove, block or deny access to specified material	Yes
In the case of infringing material, is a service provider only liable where…	he has actual knowledge that the material is infringing or is notified about the infringement (a notice to take down) and does not remove the material or link to the material within a reasonable time.
Law provides a mechanism whereby content can be removed at the instance of notification by a user	Yes

Privacy and Data Protection

General Constitutional protection	Yes
Specific data protection legislation in place THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 21 OF 2009 PART VII AND DATA PROTECTION BILL.	Yes/Draft
Remedy available for breach of privacy (for instance in delict / tort)	Yes
Privacy legislation covers public and/or private sectors or both	Both
Regulation addresses individuals' choice to 'opt in' or 'opt out' of the collection of their personal health information?'	Uncertain/No
Notice and/or consent requirement built into privacy law	Yes
Data protection legislation provides for minimum standards of collected fairly and lawfully; • used only for the specified purpose for which it was originally collected; • adequate, relevant and not excessive to purpose; • accurate and up to date; • accessible to the subject; • kept secure; and • destroyed after its purpose is completed.	Yes
Data Protection Authority (DPA) or Privacy Commissioner provided for in regulations	No
Regulations that control 'direct marketing'	No
Are cross border data exchanges restricted?	No but Draft – ito the Data Protection Bill restrictions are placed on personal data sent outside Zambia - 'adequate level' of protection is needed as to how data will be treated.
Country's data protection mechanisms compliant with the EU directive on data exchange	No
Policies for equity of access to information including for gender and other sociocultural groups'	Yes
Enforcement and sanctions mechanisms built into the law	Yes
Requirement in the law to protect personal or 'sensitive' data	Yes
Provisions governing 'research data'	Yes

Online Protection and e-legislation

Monitoring and/or control of information and content over an electronic medium by service providers?	No and voluntary compliance
Consumer protection legislation in place that protects users in an online environment	No but information to be provided by the online supplier of goods or services ito section 35(1)
Validity of electronic documents THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 21 OF 2009	Yes
Validity of contracts concluded online THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 21 OF 2009	Yes/Uncertain
Validity of e-signatures THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 21 OF 2009	Yes/Uncertain
Policies exist to promote e-commerce and services provision (e.g. e-signatures) in all sectors	Yes/Uncertain

Licensure and registration of medical practitioners

Requirement that medical practitioners are registered	Yes
Governing body that controls registration HEALTH PROFESSIONALS COUNCIL OF ZAMBIA	Yes
Requirement for the licensing or accreditation of medical practitioners	Yes
Requirement for the licensing or accreditation of medical practitioners who practice eHealth	No
'Informed consent'/consent required in an eHealth consultation	Implied
Can consent be obtained electronically	Unclear
Doctor-patient relationship need to be established	Yes
Clearly defined medical jurisdiction for medical practitioners	No
Medical practitioners can do the following online NO LEGISLATION IN PLACE REGULATING THIS:	
- provide advice online	Unclear
- diagnose online (e-consultations)	Unclear
- prescribe medicine online (e-prescribing)	Unclear
- dispense medicine online (e-dispensing of medicine)	Unclear
Requirement for the licensing or accreditation of online e- health applications	No
EHealth/telemedicine guidelines/codes of practice in place	No

Medical device regulations

Medical device technology regulations ZAMBIA BUREAU OF STANDARDS	Yes
eHealth (mHealth) suppliers need accreditation	No/ Unclear / eHealth suppliers need specific accreditation only in as far as other similar non eHealth providers do
Regulations control medical device technology	Both hardware and software

Consumer protection

Law that governs consumer protection THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 21 OF 2009 PART VI	Yes
Consumer protection laws require that certain information regarding the service or product be made available to the user	Yes
Law applies to goods, services and transactions conducted…	over an electronic medium (i.e. e-transaction) and to conventional methods of transacting
Law requires that a consumer be offered an opportunity to withdraw from the transaction	Yes
Law requires a person offering services electronically to use a secure and technologically accepted payment system?	Yes

Regulatory bodies

eHealth (mHealth) regulatory body	No
Regulatory body that oversees data protection ZAMBIA INFORMATION AND COMMUNICATIONS AUTHORITY (ZICTA)	Yes
Cyber crime prevention regulatory body ZAMBIA INFORMATION AND COMMUNICATIONS AUTHORITY (ZICTA)	Yes

Telecommunications regulatory body ZAMBIA INFORMATION AND COMMUNICATIONS AUTHORITY (ZICTA)	Yes

Barriers Identified AS CONCEPTS ARE UNCLEAR UNCERTAINTY EXISTS AND SUSPICION OVER CERAIN ASPECTS OF MHEALTH FOR INSTANCE, E-PRESCRIPTIONS	Yes

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at www.gsma.com.
Follow the GSMA on Twitter: @GSMA.

About GSMA Mobile for Development - Serving the underserved through mobile

GSMA Mobile for Development brings together our mobile operator members, the wider mobile industry and the development community to drive commercial mobile services for underserved people in emerging markets. We identify opportunities for social, economic impact and stimulate the development of scalable, life-enhancing mobile services.

For regular updates follow us on Twitter @GSMAm4d

About GSMA Mobile for Development mHealth

The GSMA Mobile for Development mHealth programme brings together the mobile industry and health stakeholders to improve health outcomes in emerging markets, with initial focus on Millennium Development Goals 4, 5 and 6 across Africa. The programme convenes key stakeholders using many forums including working groups and workshops, as well as providing resources and support to identify partnership opportunities to bring mHealth solutions to scale.

For more information on the GSMA's Mobile for Development mHealth programme - mhealth@gsma.com
http://www.gsma.com/mobilefordevelopment/programmes/mhealth

This document is an output from a project funded by UK aid from the Department for International Development (DFID) for the benefit of developing countries. The views expressed are not necessarily those of DFID.