CLOUD CHECKLIST FOR KENYA* - HEALTHCARE

Source	Compliance obligation	Microsoft commitments	Azure	Dynamics 365	Office 365
The Constitution of Kenya, 2010	Uphold every person's constitutional right to privacy which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed.	Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, availability, and integrity. Microsoft adheres to numerous internationally recognised standards addressing information security and privacy which can help the customer comply with its legal requirements. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements.	✓	✓	✓
Access to Information Act, 2016	Observe the right of every Kenyan: (a) to access information held by another person and which is required for the exercise or protection of any of their rights or fundamental freedoms; and (b) to access and amend their personal information held by any entity. A Kenyan citizen may request any public entity or private body to correct, update or annotate any personal information held by it relating to the requestor, which is out of date, inaccurate or incomplete, within a reasonable time, at the entity's own expense.	Microsoft acknowledges the customer as exclusive owner of its data. A customer accordingly has complete control over its data in the Microsoft cloud and is able to address any requests for access, correction, or destruction. In this way, Microsoft can help the customer comply with its legal requirements. In this way, Microsoft can help the customer comply with its legal requirements.	✓	✓	✓
Data Protection Bill, 2018[1] Under the Data Protection Bill, Microsoft will likely be considered a "data processor", and each customer the "data controller".	Notify a data subject of the actual collection of personal information, the purpose for which the information is being collected, the intended recipient of the information and the right to access and/or correct the collected personal information.	Microsoft acknowledges the customer as exclusive owner of their data. A customer accordingly has complete control over their data in the Microsoft cloud and is able to address any requests for access, correction, or destruction.. In this way, Microsoft can help the customer comply with its legal requirements.	✓	✓	✓
	Put in place appropriate, reasonable, technical and organisational measures to protect a data subject against the risk of loss, damage or destruction of or unauthorised access to personal information.	Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, availability, and integrity. Microsoft adheres to numerous internationally recognised standards addressing information security and privacy which can help the customer comply with its legal requirements. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements.	✓	✓	✓
	Only collect, store or use personal data: (a) using lawful means; and(b) using means that in the circumstances do not intrude to an unreasonable extent on the personal affairs of a data subject except in accordance with any written law.	Microsoft specifically undertakes and agrees with its customers to only process customer information and/or personal information under authority of its customer. Microsoft also contractually commits not to disclose customer information and/or personal information unless legally required to do so.	✓	✓	✓
	Where personal data is held, put in place such security safeguards as are reasonable in the circumstances to protect the data against:	Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality,	✓	✓	✓

[1] We have considered the Data Protection Bill, 2018, issued under Kenya Gazette Supplement No. 66 (Senate Bills No. 16) dated 30 May 2018 (available at http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2018/DataProtectionBill_2018.pdf). This version may be subject to future amendment.

Source	Compliance obligation	Microsoft commitments	Azure	Dynamics 365	Office 365
	(a) loss, damage or destruction; or (b) access, modification, negligent disclosure or use by an unauthorised person.	security, availability, and integrity. Microsoft adheres to numerous internationally recognised standards addressing information security and privacy which can help the customer comply with its legal requirements. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements.			
	Where information relating to a data subject is held by a third party, only release it to another person or put it to a different use with the consent of the data subject.	Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, availability, and integrity. Microsoft adheres to numerous internationally recognised standards addressing information security and privacy which can help the customer comply with its legal requirements. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements. Microsoft holds itself accountable to and is subject to laws of general application applicable to information technology service providers, including security breach notification law, and has binding agreements which, in its view, provide adequate protection.	✓	✓	✓
	Not to use personal data for commercial purposes without the consent of the person to whom it relates.	Microsoft acknowledges the customer as exclusive owner of its data. Microsoft specifically undertakes and agrees with its customers to only process customer information and/or personal information under authority of its customer. Microsoft also contractually commits not to disclose customer information and/or personal information unless legally required to do so.	✓	✓	✓
	Restrictions on the flow of personal data outside Kenya save in specified circumstances, such as where the third party is subject to a law or agreement that requires the putting in place of adequate measures for the protection of personal data; the data subject consents to the transfer; the transfer is necessary for the performance or conclusion of a contract between the agency and the third party; and the transfer is for the benefit of the data subject.	Microsoft holds itself accountable to and is subject to laws of general application applicable to information technology service providers and has binding agreements which, in its view, are likely to constitute adequate measures.	✓	✓	✓
	Ensure that data is processed: (a) without infringing the right to privacy of a data subject or any other person; (b) in a lawful manner; and (c) in a reasonable manner.	Microsoft specifically undertakes and agrees with its customers to only process personal information under authority of its customer. Microsoft also contractually commits not to disclose personal information unless legally compelled to do so.	✓	✓	✓
	Restricts processing of health information (special personal information) but permits processing with consent of the data subject or in other specified circumstances.	Microsoft acknowledges the customer as exclusive owner of their data. Microsoft specifically undertakes and agrees with their customers to only process customer information and/or personal information under authority of its customer. Microsoft also contractually commits not to disclose customer information and/or personal information unless legally required to do so.	✓	✓	✓
Computer Misuse and Cybercrimes Act, 2018	This creates new offences relating to the use of computer systems and may impose requirements, including those relating to critical infrastructures. In relation to information sharing in certain instances, it	Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, availability, and integrity. Microsoft adheres to numerous internationally recognised standards addressing information security and privacy which can help the	✓	✓	✓

Source	Compliance obligation	Microsoft commitments	Azure	Dynamics 365	Office 365
	limits sharing of health status information without consent of the data subject.	customer comply with its legal requirements. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements			
Health Act	Keep information concerning a person's health status, treatment or stay in a health facility confidential unless the person has given consent in writing or there is a court order or legislation requiring it.	Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, and availability. Microsoft adheres to numerous international standards addressing information security and privacy. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements responding to the said policies and regulations.	✓	✓	✓
HIV & AIDS Prevention and Control Act	For any information relating to a HIV Test, not include any information which directly or indirectly identifies the person to whom an HIV test relates. Disclosure should only be in accordance with the Act.	Microsoft contractually commits not to disclose customer information and/or personal information unless legally required to do so.	✓	✓	✓
National Intelligence Service Act	The right to privacy may be limited in respect of a person who is subject to investigation by the Service or suspected to have committed an offence, the privacy of a person's communications may be investigated, monitored or otherwise interfered with.	Microsoft contractually commits not to disclose customer information and/or personal information unless legally required to do so.	✓	✓	✓
Public Health Act	Not divulge any information relating to a person with a venereal disease or share photographs of persons confined in an asylum.	Microsoft contractually commits not to disclose customer information and/or personal information unless legally required to do so.	✓	✓	✓
Cancer Prevention and Control Act	Guarantee the right to privacy of the individual.	Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, and availability. Microsoft adheres to numerous international standards addressing information security and privacy. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements responding to the said policies and regulations.	✓	✓	✓
Public Officers Ethics Act	Government staff must take all reasonable steps to ensure that property entrusted to their care is adequately protected and not misused or misappropriated.	All information stored on the cloud belongs to the customer and Microsoft provides technical and operational measures to address confidentiality and security. Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, and availability. Microsoft adheres to numerous international standards addressing information security and privacy. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements responding to the said policies and regulations. Microsoft allows flexibility and can cater for a customer to select and implement its own compliance regime.	✓	✓	✓
Kenya National eHealth Policy 2016 – 2030	To ensure eHealth solutions are of good quality, guarantee confidentiality, privacy, security, and the integrity of health data, anonymize all health data for research purposes, ensure deployment	Microsoft holds itself accountable to and is subject to laws of general application applicable to information technology service providers, including security breach notification law, and has binding agreements which, in its view, provide adequate protection.	✓	✓	✓

Source	Compliance obligation	Microsoft commitments	Azure	Dynamics 365	Office 365
	of user-friendly eHealth platforms for ease of use to implement technology-driven interventions in clinical and public health. To ensure the sharing of information, knowledge and practice as well as guarantee secure transfer of health information between healthcare service providers. To realize full systems integration, data interchange and interoperability between both homogenous and heterogeneous systems in the health sector. To ensure that health services are electronically accessible to patients, consent is sought before transferring or sharing patient information electronically through platforms. To ensure the eHealth systems capture quality data at the point of care that may be used across heterogeneous platforms to secure privacy, confidentiality and integrity of patient health information.	While not a direct provider, we support provider/end-user compliance. Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, and availability. Microsoft adheres to numerous international standards addressing information security and privacy. Microsoft offers many widely-recognized certifications, third party attestations and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements responding to the said policies and regulations. Processing of data including anonymization is at the sole discretion of the customer. Microsoft provides anonymization capabilities adhering to the definitions in ISO.IEC 20889 and can assist the customer in achieving compliance.			
Health Information System Policy	All inpatient activities and outcomes be recorded by the Data controller in line with WHO ICD or a similar nomenclature authorized by the Health Information System Division. Customer to ensure that data collected is non-patient identifiable, save with approval of the Ministry of Health. Medical data should only be used for the purposes for which it was collected, and for additional purposes authorized by law, or consented to by the data subject. All the health and health related data and information shall belong to the Government of Kenya. Personal data as inpatient records are the property of the facility and are held in trust on behalf of the patients by the said data controller. The Health workers who have privileged access to patient's records shall be accountable to maintain the highest level of confidentiality and ensure that shared confidentiality is only practiced in the interest of the patient. Data controllers shall be responsible for safe storage and easy retrieval for all records under their care. Security mechanisms shall be ensured for health data and information (i.e. storage, improper possession, brokering, disclosure, dissemination, confidentiality and privacy. Health and health related data and information shall be hosted by HIS; Warehousing shall also be created and maintained for data and information at central level within the health sector.	While not a direct provider, we support provider/end-user compliance. Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, and availability. Microsoft adheres to numerous international standards addressing information security and privacy. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements responding to the said policies and regulations. Microsoft also contractually commits not to disclose customer information and/or personal information unless legally required to do so. Microsoft holds itself accountable to and is subject to laws of general application applicable to information technology service providers, including security breach notification law, and has binding agreements which, in its view, provide adequate protection.	✓	✓	✓
Government Enterprise Architecture -	All government Ministries, Counties and Agencies are expected to implement the use of these principles for ICT-based solutions; that the systems are trustworthy, transparent, leveraged, effective, aligned,	Microsoft supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, and availability. Microsoft adheres to numerous international standards addressing information security and privacy. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3,	✓	✓	✓

Source	Compliance obligation	Microsoft commitments	Azure	Dynamics 365	Office 365
General Guiding Principles	equitable, cohesive, managed and compliant. The solution should be interactive, interoperable, secure and easy to integrate.	contractual data processing terms, SLAs) that customers can use to address their own compliance requirements responding to the said policies and regulations. Additionally, Microsoft provides a dynamic set of online services that can assist customer with achieving the principles outlined.			
Health Sector Strategic Plan for Health Information Systems 2009-2014	Have a system (HIS) that is comprehensive and integrated that collects, collates, analyses, evaluates, stores and disseminates health and health related data and information for use by all. The information provided should be provided to the right user at the right time. Data collected and information generated must be handled with confidentiality and security that they deserve.	Microsoft acknowledges the customer as exclusive owner of its data. A customer accordingly has complete control over its data in the Microsoft cloud and is able to address any requests for access, correction, or destruction. While specific design and engineering principles fall to customers, Microsoft holds itself accountable to and is subject to laws of general application applicable to information technology service providers, including security breach notification law, and has binding agreements which, in its view, provide adequate protection. Microsoft also supports customer compliance by providing both strong contractual undertakings as well as technical and operational measures to address confidentiality, security, and availability. Microsoft adheres to numerous international standards addressing information security and privacy. Microsoft offers many widely-recognized certifications, third party attestations, and legal assurances (e.g. ISO27018, SOC2&3, contractual data processing terms, SLAs) that customers can use to address their own compliance requirements responding to the said policies and regulations. Additionally, Microsoft also contractually commits not to disclose customer information and/or personal information unless legally required to do so.	✓	✓	✓
Kenya Health Policy 2014-2030	Develop a functional, efficient, safe and sustainable health infrastructure based on the needs of the clients. Develop a system that is appropriate (accessible, affordable, feasible and culturally acceptable to the community)		✓	✓	✓
Health Sector ICT Standards and Guidelines- Ministry of Health June 2013	Adhere to the cloud computing guidelines; implement and maintain a security process, build and maintain a secure cloud infrastructure, ensure confidential data protection, implement strong access and identity management, establish application and environment provisioning, implement governance and audit management process, implement a vulnerability and intrusion management program and maintain environment testing and validation.		✓	✓	✓
Kenya National e-Health Strategy 2011-2017	To put in place measures to protect consumer confidentiality, to provide a basic system security and to protect against unlawful access or malicious damage to information. Every effort must be made to ensure that access is absolutely restricted to authorized persons.		✓	✓	✓
Kenya Standards and Guidelines on mHealth Systems April 2017	To conform to various non-functional requirements including security, confidentiality, integrity, availability and non-repudiation.		✓	✓	✓
Kenya Health Enterprise Architecture (KHEA)	To satisfy quality requirements levied upon the data for which the trustee is accountable, provide user confidence, be accountable and responsible for the accuracy and currency of the designated data element(s), protect data from unauthorized use and disclosure, put in place data security safeguards and ensure information at all levels, including generation, analysis and decision making, must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster or disclosure.		✓	✓	✓

Source	Compliance obligation	Microsoft commitments	Azure	Dynamics 365	Office 365
National Cancer Control Strategy 2017-2022	To link data collection to the Health Management Information System (HMIS) to ensure that accurate, timely, comprehensive and complete data is generated.		✓	✓	✓