DPO
PRIVACY CENTRE
EAST AFRICA

Handling Health Data in Uganda

Legal Obligations, Consent and Patient Rights

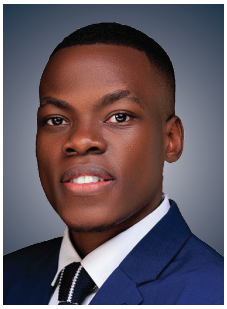
June, 2026

Contributors:

Kemigisha Liticia

Mugambe Andrew

Namugera Joel Peter



Kityo Martin

Introduction

The rapid digitisation of healthcare systems in Uganda has significantly improved access, efficiency and management of health data. Despite these developments, there have been emerging concerns about risks to the privacy and confidentiality of sensitive patient data.

This article examines the legal framework governing the processing patient data in Uganda, explores the key legal obligations of key stakeholders, patient rights and highlights regional enforcement developments. It also proposes recommendations for improving the protection of patients' personal data in Uganda.

Legal Framework for Processing Patient Data in Uganda

The right to privacy is a fundamental human right guaranteed under **Article 27(2)** of the **Constitution of the Republic of Uganda, 1995 as amended.** This constitutional protection is operationalised by the **Data Protection and Privacy Act, Cap. 97 ("Act")** and the **Data Protection and Privacy Regulations, 2021 ("Regulations")** ensuring that personal health information is protected from unlawful access, disclosure or misuse.

Recognising the sensitivity of health information, the Ministry of Health (MoH) also issued sector-specific guidelines, the **Uganda Health Data Protection, Privacy and Confidentiality Guidelines ("Guidelines")** in 2023 to standardise the management, exchange and use of personal health information across the Ugandan health sector. These guidelines build on broader national legislation to ensure that both public and private health actors safeguard sensitive patient data.

Accordingly, the protection of patient data is both a statutory obligation and an ethical imperative.

a. What is covered?

The Act defines personal data to mean information about a person from which the person can be identified. It includes information relating to nationality, age or marital status of the person; the educational level or occupation of the person and identity data.[1]

The Guidelines expand the scope of personal data in the health sector to include information about an individual for the provision of health services, information about

1. Data Protection and Privacy Act, Cap. 97, Section 2

eligibility for healthcare concerning the individual, number or particular symbol assigned to an individual to uniquely identify the individual for health purposes and information derived from the testing or examination of a body part or bodily substance.[2]

Health-related information such as medical history, diagnostic information, biometric data, genetic data and information relating to a person's physical or mental health falls within the scope of personal data under the Act. It is further classified as special personal data given its sensitive nature thus subject to a higher level of protection and stricter processing obligations.[3]

b. Who is Covered?

The Act defines key players in the data processing cycle to include (a) a data collector, who collects personal data, (b) a data controller, who determines the purposes for and manner in which personal data is processed and (c) a data subject, the person whose data is being collected.[4]

Healthcare providers, health insurers, researchers and academic institutions, digital health platforms and mobile health service providers act as data controllers and collectors and the patients as data subjects.

The data protection framework imposes a mandatory registration obligation with the Personal Data Protection Office (PDPO) for data controllers and collectors before they process one's personal data.[5] The failure to register is an offence which on conviction is punishable with a fine not exceeding Ugx 120,000/- (six currency points) or imprisonment for not more than three (3) months or both.[6] When this offence is committed by an entity, its deemed committed by every officer who knowingly and wilfully authorised the contravention. Much as the sentence for the offence of non-registration seems significantly low, it has a significant high reputational impact. The Act has been tested in practice and enforcement is also steadily rising. The Magistrate Court at Makindye recently convicted three (3) mobile money agents for the offence of illegally obtaining and sharing personal data. They were also not registered as required by the Act and thus fined with a possibility of imprisonment in case they default.[7]

2. Uganda Health Data Protection, Privacy and Confidentiality Guidelines, Definition of Terms.
3. Data Protection and Privacy Act, Cap. 97, Section 9.
4. Data Protection and Privacy Act, Cap. 97, Section 2
5. Data Protection and Privacy Act, Cap. 97, Section 29; Data Protection and Privacy Regulations, 2021, Regulation 15.
6. Data Protection and Privacy Regulations, 2021, Regulation 15(1) and (3).
7. B. Tumusiime, "Court fines mobile money agents over data breach, Daily Monitor" (5th May 2026) <https://www.monitor.co.ug/uganda/news/national/court-fines-mobile-money-agents-over-data-breach-5447526>

c. Data Protection Principles

The **Act** sets out principles that ought to be followed when processing personal data.[8] In the context of the health sector, these principles mandate that health facilities shall be accountable of health data collected or processed. Health data obtained through patient diagnosis, treatment, billing among others should be processed lawfully, fairly and in a transparent manner. Additionally, only personal data that is relevant and necessary should be collected. Healthcare providers must also ensure quality of patient data collected and processed by taking care to record correct names of patients, note accurate test results and not mix up patient details.

Importantly, health data must be retained for the period authorised by law and data security must be observed. The Guidelines establish a minimum retention period of five (5) years,[9] however, the actual retention period, beyond the five years should be determined according to the nature of the data and the purpose of processing. For instance, a hospital may not need to retain records relating to a walk-in patient's inquiry about its services beyond the period necessary for administrative purposes. However, patient medical records, diagnostic results and treatment histories may require longer retention periods to facilitate ongoing care.

d. Lawful Bases for Processing

The data protection framework also sets out lawful bases under which personal data must be collected. These are the justifications for processing data and they must be identified before data is collected.

The first and key lawful basis is “Consent” and it must be obtained from the data subject before processing their personal data as stated in **Section 7** of the Act. Consent must be freely given without coercion or undue influence, specific, informed whereby the patient understands what they are agreeing to and it must be expressed clearly orally or in writing. It’s worth noting that patients have a right to withdraw consent at any time.

While consent is key, there are other lawful alternative bases which can be relied on to process patients’ personal data. For instance, where processing of the patients’ personal data is necessary for medical purposes.[10] Sometimes patients may not be able to consent if they are minors, unconscious or incapacitated, yet they need medical attention urgently. In such situations, the Guidelines provide that consent must be sought from the Nominee, who is the person the patient nominates to

8. The Data Protection and Privacy Act Cap 97, Section 3.
9. Uganda Health Data Protection, Privacy and Confidentiality Guidelines, Guideline 5.
10. Data Protection and Privacy Act, Cap. 97, Section 79(2)(d); See also Mental Health Act, Cap. 308, Section 21.

provide consent on their behalf in case they are unable to.[11] Where a patient did not elect a nominee prior to their incapacitation, then consent can be sought from an adult member of the patient's family.[12] Similarly, the **HIV And AIDS Prevention And Control Act, Cap. 126** allows a parent, guardian, next of kin or agent of the patient to give consent for HIV testing, in case a patient is unable to.[13]

The Act also provides for other lawful bases such as compliance with legal obligations, public health interests, national security and performance of a contract to which the data subject is a party which can be relied on by healthcare providers to process patients' health information without necessarily obtaining consent.

e. Patient Rights

The **Act** under **Part V** empowers patients as data subjects with legally enforceable rights over their personal health information. These include the right to access personal information such as their medical records, right to rectification of inaccurate and outdated data, right to erasure where data is no longer necessary or was unlawfully processed, right to prevent processing of personal data especially where it is not necessary for treatment or legal compliance and the right to redress where patients' rights are violated hence lodging complaints with the PDPO. It's important to note that not all rights are absolute meaning requests based on these rights may be declined with reason and the Act and Regulations stipulate timelines within which a response must be provided.

Recent Data Protection Developments

Recently on 15th April 2026, the Ministry of Health issued a directive to all health facilities in Uganda due to recent institutional functionality and performance audits that identified significant gaps in the protection, confidentiality and lawful processing of patient information. All health facilities in Uganda, as data controllers, are required to designate a **Data Protection Officer (DPO), register with Personal Data Protection Office (PDPO),** implement adequate security measures and maintain proper records of all data processing activities. Compliance with these requirements is not optional and forms an integral part of the Ministry's Digital Health Transformation Agenda. Non-compliance may attract penalties as stipulated in the Act and Regulations

In Kenya, the data protection regulator, the **Office of the Data Protection Commissioner (ODPC)** has taken a firm enforcement stance against health facilities,

11. Uganda Health Data Protection, Privacy and Confidentiality Guidelines, Guideline 10.4
12. Uganda Health Data Protection, Privacy and Confidentiality Guidelines, Guideline 10.4(d).
13. HIV And AIDS Prevention And Control Act, Cap. 126, Section 10.

a position we anticipate the PDPO will similarly adopt. The ODPC ordered The Nairobi Hospital to pay KES 500,000 (approximately UGX 14,567,795.29) for processing personal data without consent. The facility was faulted for recording and using a patient's image in an advertisement without authorisation.[14] The ODPC found St. Luke's Orthopaedic and Trauma Hospital, Eldoret liable for unlawfully disclosing a patient's sensitive personal data ordering it to compensate the patient KES 525,000 (approximately UGX 15,300,000).[15] In 2022, following a compliant by data subject that a member of the hospital's staff had inappropriately contacted them, ODPC issued Aga Khan University Hospital with an enforcement notice and directed the hospital to outline specific measures it would take to mitigate or eliminate the breach, and to establish structures for compliance which would be implemented in 30 days.[16] Additionally, ODPC has issued specific health sector guidelines which are enforceable.

14. "Kenya: ODPC orders The Nairobi Hospital to pay KES 500,000 for processing data without consent", Onetrust Data Guidance (26th January, 2026) < https://www.dataguidance.com/news/kenya-odpc-orders-nairobi-hospital-pay-kes-500000 >
15. "Data Commissioner Orders Hospital to Pay Sh525,000 for Mishandling Patient's Medical Data", Capital News (16th April, 2026) < https://www.capitalfm.co.ke/news/2026/04/data-commissioner-orders-hospital-to-pay-sh525000-for-mishandling-patients-medical-data/>
16. S. Tejpar, "Office of the Data Protection Commissioner Imposes its First Fine under the Kenya Data Protection Act", ALN Kenya (31st December, 2022) < https://aln.africa/insight/data-protection-commissioner-imposes-fine/>

Challenges and Recommendations

Despite the existing framework, there are critical concerns about the protection of sensitive patient data.

Weak enforcement and Limited Sanctions: The capacity of the PDPO needs to be strengthened, potentially through granting it greater independence. Furthermore, the deterrent effect of penalties must be enhanced and the PDPO should be empowered to offer monetary compensation to victims.

Limited Awareness of data protection obligations: Health workers often lack sufficient awareness of their data protection obligations, meaning patient data is at risk. The Ministry of Health, should, in collaboration with the PDPO, provide technical guidance, regular training and support to all health facilities to facilitate compliance. Facilities should utilise these resources to strengthen their data governance frameworks.

Inadequate digital infrastructure: Some health facilities lack enough digital infrastructure especially in rural areas due to inadequate funding and resource constraints. The Ministry of Health, in collaboration with the PDPO should provide support and introduce programs so as to have a meaningful impact on the average Ugandan.

Evolving Technology: The rapid technology advancements continually outpace regulatory responses. For example, risks associated with mobile health technologies and cross-border data flows. This calls for development of forward-looking laws that anticipate future trends and ensure the legal framework remains robust and adaptable. Further, the growing use of artificial intelligence, wearable devices, mobile health applications, electronic medical records and telemedicine platforms have introduced new privacy and ethical concerns. Current legislation does not comprehensively address automated decision-making, algorithmic bias, profiling or the use of patient data for AI training and predictive healthcare technologies.

Uganda should consider developing specific regulations or guidelines governing emerging health technologies to ensure transparency, accountability, fairness and lawful processing of health data in digital healthcare ecosystems.

Poor Data Sharing Governance and Interoperability Risks: The increasing use of interconnected health systems such as the Integrated Health Management Information System (IHMIS), use of digital laboratories and telemedicine services has created challenges relating to uncontrolled data sharing between institutions. In many instances, there are no clear data-sharing agreements defining access rights, responsibilities, retention periods or accountability in the event of a breach. This creates risks of unauthorised disclosures and inconsistent handling of patient information. There is therefore a need for sector-specific interoperability standards and legally compliant data-sharing frameworks to regulate the exchange of health information among healthcare providers, insurers, laboratories, researchers, and government agencies.

Cybersecurity Threats and Rising Health Data Breaches: Healthcare institutions are increasingly becoming targets for cyberattacks, ransomware incidents, phishing schemes and unauthorised system intrusions due to the high value of medical information. Many health facilities lack robust cybersecurity systems, encryption mechanisms, intrusion detection tools, and incident response procedures. Healthcare providers should invest in stronger cybersecurity infrastructure, conduct regular vulnerability assessments, implement encryption and multi-factor authentication systems and establish clear breach response protocols in line with the Act and Regulations.

Conclusion

Uganda has established a constitutional and statutory foundation for protecting patient data, aligning with regional and global standards. The Ministry of Health in collaboration with the Personal Data Protection Office should effectively implement and enforce clear guidelines of protecting patient data. Ultimately, compliance with the Data Protection and Privacy Act, Cap. 97 and the Data Protection and Privacy Regulations, 2021 is not only a mandatory legal requirement but also essential for safeguarding patient dignity, maintaining confidentiality, integrity and security. Health practitioners are advised to register their facilities with the Personal Data Protection Office, have mandatory data protection and privacy training for their staff and embed privacy practice and culture within every process and activity within their facilities and activities. With this, they will not only have ticked the regulatory requirements but also enhance patient trust.

DPO
PRIVACY CENTRE
EAST AFRICA

Interested in receiving similar publications direct to your inbox? Subscribe to our Substack

substack.com/@privacycentreea

Want to contribute an article or have an idea for collaboration?

privacycentreeastafrica@gmail.com