DHRP
Digital Health & Rights Project

KELIN
Reclaiming Rights, Rebuilding Lives

KCAT
KENYA COMMUNITY ADVISORY TEAM

Know Your Digital Health Rights: A Practical Guide for Young People in Kenya[1]

What rights do I have when accessing health information and services using digital devices or online:

a) Privacy:

- Kenyan law protects your privacy when you access health information or services online or via digital devices.
- As per the Data Protection Act (2019), health records are classified as sensitive personal data, with strict requirements for informed consent, purpose limitation, data security, rights to access, correction and deletion, as well as breach notification. This means such health records must be handled carefully—people should give clear permission, data should only be used for the right reasons, kept secure, and individuals have the right to see, fix, or delete their information. If there is a data leak, it must be reported.

When accessing health information and services online or via digital devices, you are legally entitled to:

- **Right to Privacy**
- **Right to Health**
- **Right non-discrimination and dignity**
- **Access to information and participation**

[1]Acknowledgement: KELIN is grateful to Belice Odamna (consultant) and Wakesho Kililo (Kenya Community Advisory Team) for their support in developing this toolkit. Special appreciation to the KELIN project team led by Timothy Wafula (Senior Programme Manager), Simon Odiwuor (consultant) for their invaluable support towards the conclusion of this brief.

- Health care workers, providers, and professionals are legally required to maintain confidentiality when handling your health information.
- You are entitled to be informed about how your health data will be used, who can access it, and the measures in place to secure it.
- It is advisable to check the credentials and privacy policies of health service providers, use secure apps or connections, and keep records of your consents and communications.

b) Health:

- You have the right to the highest attainable standard of health. This includes timely access to reliable health information and safe digital health services. Online and mobile health platforms should be accessible, non-discriminatory, clinically reliable, and secure, allowing you to obtain advice, diagnosis, and care without unnecessary barriers or risks to your privacy and safety. Clinically reliable means the health information or service is accurate, safe, and based on real medical knowledge and standards—so you can trust it like advice from a qualified health professional.
- Laws such as the *Digital Health Act (2023)*, *Health Act*, and *Data Protection Act (2019)* protect you when using digital health services. These laws require service providers to:
  - Deliver safe, accurate, and high-quality care
  - Obtain your informed consent before collecting or using your data
  - Keep your personal health information private and secure

  Because of these protections, you have the right to:

  - Access reliable and trustworthy health information
  - Have your personal health data protected from misuse
  - Receive fair and equal access to telehealth services
  - Seek help or take action through regulators or the courts if your rights are violated.

c) Right non-discrimination and dignity:

- When accessing health information or services online, you have the right to be treated with dignity and without discrimination.
  - In Kenya, the Constitution (Article 27) and laws such as the Health Act and the HIV and AIDS Prevention and Control Act protect you from:
    - Harassment or unfair treatment
    - Disclosure of your health status without your consent
    - Denial of care or services
  - These protections apply regardless of your health status, sexual orientation, gender, or gender identity.
  - If you experience discrimination or unfair treatment, you have the right to report it and seek redress.
- Digital health providers and professionals must treat you with respect, protect your privacy, and provide services without discrimination.
- If you experience a violation—such as exposure of your information, harassment, or denial of care—you can take action:

- Document what happened: Keep evidence such as screenshots, names, dates, and any communication
- Report the incident to the appropriate authority, including:
  - Kenya Medical Practitioners and Dentists Council (KMPDC)
  - The Office of the Data Protection Commissioner (ODPC)
  - Seek legal redress through the courts if necessary
- Taking these steps can help protect your rights and prevent similar violations from happening to others.

d) Access to information and participation:

- You have the right to access public health information and take part in decisions about digital health tools and services.
- In Kenya, the Constitution (Article 35) guarantees your right to access information and requires public participation in governance (Article 10). The Access to Information Act (2016) allows you to request official health data from public bodies.
- This means you can:
  - Access government health guidelines, statistics, and policy documents
  - Request information from public institutions about digital health services
  - Participate in decision-making processes on telemedicine, eHealth policies, and digital health procurement
- You can engage through:
  - Ministry of Health consultations
  - Regulator calls for public comments
  - Public forums and stakeholder meetings
  - Parliamentary processes
- Being informed and participating helps ensure digital health systems are transparent, accountable, and responsive to your needs.
- If a public body refuses to give you information or excludes you from participating in decision-making, you have the right to take action. You can:
  - File a complaint under the Access to Information Act (2016)
  - Petition the relevant regulator or the Office of the Ombudsman (Commission on Administrative Justice)
  - Seek legal redress through the courts
  - These mechanisms help ensure transparency, accountability, and your inclusion in decisions that affect digital health services.

Digital Health Rights issues young people experience often

Issue	Example and Immediate Action
Apps collecting extra data without clear purpose	**Example:** A symptom-checker app asks for contacts, location and device identifiers though only symptom data is needed. **Action:** Ask for purpose; refuse or uninstall; report to the Office of the Data Protection Commissioner (ODPC)
Consent buried in long privacy policies	**Example:** A mental health chatbot auto enrols users for research or marketing via buried checkboxes. **Action:** Decline non-essential options; screenshot consent screens; withdraw consent and demand deletion if misused.
Sensitive health status leaked via insecure SMS or email	**Example:** Clinic sends HIV test results by plain SMS to a phone shared with family, exposing a young person's status. **Action:** Request secure delivery (in-person, encrypted app); ask provider to correct communication method; complain to health regulator and ODPC.

Parental/guardian disclosure without consent	**Example:** A clinic's online booking system automatically copies parents on appointment confirmations for sexual and reproductive health services. **Action:** Ask for confidential alternatives; cite professional confidentiality rules; escalate to regulator or seek legal advice if refused.
Anonymity breached in online support groups	**Example:** A closed youth support group leaks screenshots of members' posts to public social media. **Action:** Leave group, request takedown, demand deletion of posts, report platform abuse and ODPC for unlawful processing.
Targeted advertising from apps revealing	**Example:** After using a reproductive health app, the user gets targeted ads about specific treatments visible to others using the same device. **Action:** Opt out of ad profiling, clear app data, change privacy settings, complain to the app provider and ODPC.
Weak security on telemedicine platforms	**Example:** A telehealth service uses unencrypted video calls or shared practitioner accounts, risking interceptions and misattribution. **Action:** Ask about encryption and login controls; refuse sensitive consultations until secure; report breaches.
Misuse of youth data for commercial profiling	**Example:** A startup aggregates young users' sexual health queries and sells insights to insurers or advertisers. **Action:** Demand data access/portability, withdraw consent, file complaint with ODPC and consider civil action.
Cyberbullying or harassment after seeking help online	**Example:** A young person posts about HIV and is doxed and harassed by other users on a platform. **Action:** Preserve evidence (screenshots), report to platform, police (cybercrime) and seek regular support including counselling.
Denial of digital services due to identity or orientation	**Example:** A teleclinic refuses to register an LGBTQ+ youth or disables their account after profile changes. **Action:** Record denial, request written reasons, complain to relevant health regulator and the National Gender and Equality Commission or courts.

Some practical knowledge young people must have before using digital health apps:

- Ask what data is being collected and why before using a health-related app or a service
- Refuse or withdraw consent if you discover your data is used for other purposes
- Ask providers to explain how they secure your records
- Demand anonymity where possible (use pseudonyms in groups, private modes)
- Ask for correction or deletion if data is wrong or not needed.

Practical safety tips (for phones, apps, groups

- Use strong passwords and two-factor authentication where applicable
- Turn off autofill or contact-sync on dating/health and related apps
- Use app privacy settings; check what data an app asks for before you accept
- Avoid sharing devices. If you must, log out of health apps and delete history
- Use secure networks (avoid public Wi-Fi for sensitive searches)
- If threatened with blackmail, stop contact, screenshot evidence, and report
- Vet WhatsApp/Facebook groups before joining, ensure there are clear descriptions and trusted admins.

Short practical steps after any incident:

- Preserve evidence (screenshots, timestamps, messages).
- Ask providers to correct, delete or stop processing your data in writing.
- Lodge complaints with the Office of the Data Protection Commissioner, the relevant professional regulator (e.g., Kenya Medical Practitioners and Dentists Council (KMPDC), the Office of the Ombudsman, or the police for criminal breaches.
- Seek youth-friendly legal or counselling support from NGOs, adolescent health services and pro bono lawyers.

Procedures and Venues for Seeking Redress in Cases of Digital Health Rights Violations

Immediate Actions

	Preserve all evidence, including screenshots, messages, links, dates and names. This information will be important for any follow-up actions or complaints.
	Secure your accounts by changing passwords, enabling two-factor authentication (2FA), and removing any suspicious devices connected to your accounts.
	Report the incident to the relevant platform (such as WhatsApp, Facebook, TikTok, or X etc) using the in-app reporting tools provided.
POLICE	If you or someone else is in immediate danger, **contact the police without delay.**

Quasi-Judicial and Regulatory Complaint Routes

a) Office of the Data Protection Commissioner (ODPC):

- The ODPC is the independent regulatory authority established under the Kenya Data Protection Act, 2019 to oversee and enforce data protection and privacy rights. It plays a key role in safeguarding personal data, including sensitive health information accessed through digital platforms.
- Complaint handling and investigations: You can file a complaint with the ODPC if you believe your personal health data has been misused, accessed unlawfully, shared without consent, or inadequately protected. The ODPC has the power to investigate such complaints against data controllers or processors (e.g., hospitals, insurers, digital health platforms).
- Enforcement and corrective action: If a violation is confirmed, the ODPC can issue enforcement notices, requiring the organization to take specific corrective measures—such as stopping unlawful processing, improving security safeguards, or deleting improperly obtained data.
- Penalties and fines: The ODPC can impose administrative fines and penalties on organizations that fail to comply with the law, especially in cases of serious breaches involving sensitive data like health records.
- Data breach response: In the event of a data breach, the ODPC ensures that affected individuals are notified and that the responsible entity takes steps to mitigate harm and prevent recurrence.
- Guidance and compliance support: The ODPC also provides guidance to organizations on proper data handling practices, ensuring that digital health service providers comply with legal standards for privacy, security, and consent.
- You should contact or lodge a complaint with the ODPC if:
  - Your health data is leaked or exposed online
  - Your information is shared with third parties without your consent
  - A hospital, app, or insurer refuses to give you access to your data
  - Your data is being used for purposes you did not agree to

b) Communications Authority of Kenya (CA): Handles complaints regarding telecom and service providers, such as SIM registration and network data issues. Use this route if your telecom operator has misused your SIM or data, or if there has been unlawful access via your telco.

c) Commission on Administrative Justice (Office of the Ombudsman/CAJ): The Commission on Administrative Justice (CAJ) is a constitutional body mandated to address maladministration, abuse of power, and unfair treatment by public institutions in Kenya. It ensures that government services—including public healthcare—are delivered in a lawful, fair, and accountable manner.

- Handling complaints against public institutions: You can report issues to the CAJ if a public health facility (e.g., government hospital or clinic) acts unfairly, negligently, or unlawfully in handling your health information or providing services.
- Investigation of maladministration: The CAJ investigates cases such as wrongful disclosure of personal health data, delays in service, denial of access to medical records, discrimination, or poor administrative practices in public healthcare settings.
- You should file a complaint with the CAJ if:
  - A public clinic or hospital wrongfully discloses your health information

- You experience unfair treatment, discrimination, or denial of services
- There is delay, negligence, or abuse of authority in handling your case
- A public institution fails to follow proper procedures regarding your health data.

d) Kenya National Commission on Human Rights (KNCHR):

- The Kenya National Commission on Human Rights (KNCHR) is a constitutional body mandated to promote and protect human rights in Kenya, including rights related to privacy, dignity, health, and access to information.
- Protection of fundamental rights and freedoms: KNCHR addresses violations of basic rights such as the right to privacy (including protection of personal health data), the right to health, and human dignity, especially in both physical and digital healthcare settings.
- Investigations of human rights violations: You can report cases where your rights are violated, such as unauthorized disclosure of sensitive health information, denial of healthcare, inhumane treatment, or digital surveillance without consent. KNCHR has the authority to investigate such complaints.
- Redress and referrals: KNCHR can recommend remedies, facilitate dispute resolution, and refer cases to other bodies (such as courts or the ODPC) for further legal action where necessary.
- Monitoring and reporting: The Commission monitors government and institutional compliance with human rights standards and publishes reports to promote accountability in sectors including healthcare and digital services.
- You should approach KNCHR if:
  - Your right to privacy or dignity is violated through misuse of your health data
  - You are denied access to healthcare services unfairly
  - You experience inhumane, degrading, or discriminatory treatment in a health setting
  - There are broader or systemic human rights concerns involving digital health systems

e) National Gender and Equality Commission (NGEC)

- The National Gender and Equality Commission (NGEC) is a constitutional body in Kenya mandated to promote gender equality, equity, and freedom from discrimination for all persons, including vulnerable and marginalized groups.
- Addressing discrimination and inequality: NGEC handles complaints related to discrimination in access to health services or misuse of personal data based on gender, age, disability, ethnicity, or other protected characteristics.
- Protection of vulnerable groups: The Commission specifically safeguards the rights of groups such as women, children, persons with disabilities, the elderly, and marginalized communities, ensuring they are not excluded or unfairly treated in digital or physical health services.
- Investigations and redress: NGEC can investigate cases where individuals are denied healthcare, stigmatized, or have their health information mishandled in a discriminatory manner. It can recommend corrective actions and refer matters to relevant authorities for enforcement.
- Policy oversight and advocacy: The Commission monitors government policies and practices to ensure they comply with constitutional principles of equality and non-discrimination, including in digital health systems.
- You should approach NGEC if:
  - You are denied digital or physical health services due to gender, disability, age, or other status
  - Your health information is used in a way that leads to stigma or discrimination
  - A health program or digital platform is exclusionary or inequitable

f) Platform Complaint Escalation:

- This refers to the process of raising and resolving complaints directly within the digital platform or service (such as a health app, telemedicine service, hospital portal, or insurance system) before escalating to external regulators.
- Internal complaint mechanisms: Most digital health platforms are required to have customer support channels, complaint forms, or help desks where users can report issues related to their personal data or service experience.
- First level of resolution: You should typically start here if you notice issues such as incorrect health records, unauthorized access to your account, data inaccuracies, or privacy concerns. The platform is expected to respond, investigate, and resolve the issue within a reasonable time.
- Data protection obligations: Under the Data Protection Act, the platform (as a data controller or processor) must handle your complaint seriously, ensure data security, and take corrective action where necessary.
- Documentation and evidence: When escalating a complaint internally, it is important to keep records (e.g., emails, screenshots, complaint reference numbers). This can support further escalation if the issue is not resolved.
- Escalation to regulators: If the platform fails to act, delays unreasonably, or provides an unsatisfactory response, you can escalate the matter to bodies like the ODPC, CAJ, or KNCHR, depending on the nature of the issue.
- When to use this route:
  - When you experience a problem directly within a digital health platform
  - When your data is incorrect, inaccessible, or potentially compromised
  - As a first step before reporting to external authorities

g) Health Facility Complaint Mechanism/ County Health Offices:

- These are formal complaint and feedback channels within health facilities and county health systems that allow patients to report concerns about healthcare services, including issues related to privacy, data handling, and quality of care.
- Facility-level complaint systems: Most hospitals and clinics (public and private) have complaint desks, suggestion boxes, patient relations offices, or designated officers where you can raise concerns. These mechanisms are often the first point of contact for resolving issues.
- County health oversight: County Health Departments (through County Executive Committee Members for Health or County Directors of Health) oversee public health facilities and can handle escalated complaints involving multiple facilities, systemic issues, or unresolved cases.
- You can report:
  - Breach of confidentiality (e.g., staff sharing your health information without consent)
  - Poor handling of digital health records
  - Denial of access to your medical records
  - Negligence, mistreatment, or delays in care
  - Poor service delivery or administrative failures
- If the issue involves data protection violations or human rights concerns, the matter may be referred to bodies like the ODPC, CAJ, or KNCHR for further action.
- When to use this route:
  - When the issue arises within a specific health facility or county health service
  - When you want a quick, local resolution before escalating externally
  - When dealing with service delivery or staff conduct issues, including misuse of your health data

Criminal Reporting (Where Abuse is an Offence)

- **Directorate of Criminal Investigations (DCI)** – Cybercrime Unit: Report cases such as hacking, doxxing, non-consensual sharing of intimate images, blackmail, or online threats, which are offences under the Computer Misuse and Cybercrimes Act (see below section on technology facilitated abuse for further information on this).
- File a police statement and request referral to the cybercrime unit for further investigation.

Courts (Judicial Redress)

- Petition the High Court for constitutional violations, such as breaches of Articles 31, 43, or 27 of the Constitution.
- File a civil suit for damages related to data breaches, privacy invasion, defamation, or emotional harm suffered.
- Pursue criminal prosecution via the Director of Public Prosecutions (DPP) – through the report to the police if cybercrime or other criminal conduct is established.

Note: Reporting to regulators such as the Data Commissioner or KNCHR first can strengthen your claims in court.

How to Prepare a Complaint (Short Checklist)

	Clearly state what happened, including dates, places, apps, and messages involved.
	Gather evidence such as screenshots, saved files, and the names of any witnesses.
	Identify who is responsible – whether it is an app, health facility, person, or telecom operator.If you or someone else is in immediate danger.
	Describe the harm caused, whether emotional, physical, financial, or discriminatory.
	Specify the outcome you are seeking, such as removal of content, data deletion, an apology, compensation, or criminal action.

Support Organisations and Community Help

- Reach out to local health rights or human rights NGOs, such as KELIN, for support and guidance.
- Connect with community-based peer groups, such as WhatsApp peer support groups. Ensure you vet administrators and use private channels for confidentiality.
- Seek assistance from legal aid clinics and pro bono lawyers if you need to file court petitions or claim compensation.
- Utilise youth and key population-friendly health services and request confidential services and digital safety advice if needed.

How does the law in Kenya protect digital health rights?

Law/Policy	Sections / Articles	Protections offered
The Constitution of Kenya, 2010	Article 27 of the Constitution guarantees that every individual is entitled to **equality before the law and freedom from discrimination.** This protection is particularly significant for young people engaging with digital health services. It mandates that all online health platforms, including telehealth services, health apps, government eHealth programmes and health providers, deliver information and care without unfair distinction based on age, sex, conscience, belief, health status, disability, ethnicity or socioeconomic status.	In practice, this means **digital health solutions must be designed and operated to ensure equal access for all users.** This includes providing reasonable accommodations, such as accessible interfaces and language options, and employing non-discriminatory algorithms and practices. It is essential that these platforms and providers do not stigmatise, expose, or deny care to young users based on any protected characteristic. Article 27 also ensures that young people have access to remedies if they experience discrimination or exclusion in digital health settings. This includes the right to lodge complaints with regulators such as the National Gender and Equality Commission, professional bodies, the Office of the Data Protection Commissioner, or to pursue legal action through the courts. These mechanisms empower young users to seek redress in cases of discriminatory treatment, exclusion, or harmful profiling within digital health services.
The Constitution of Kenya, 2010	Article 28 of the Constitution guarantees every individual the **right to human dignity.** For young people accessing digital health services, this right means they must be treated with respect and value in all online interactions. Their digital health information should never be used in a manner that demeans, humiliates or stigmatises them.	Upholding dignity requires strict confidentiality and the use of informed consent. Special care must be taken when handling intimate or sexual reproductive health data, and degrading communications or public exposure should be always avoided. This applies across platforms, including apps, teleconsultations, support groups and digital data releases. Digital health platforms and providers must design their services to preserve privacy and cultural sensitivity. They are obliged to deliver care in a non judgmental manner and ensure effective redress is available if dignity is violated. This includes providing avenues for complaints to regulators, professional bodies, the Office of the Ombudsman or the courts.

The Constitution of Kenya, 2010	Article 31 of the Constitution of Kenya guarantees every individual the **right to privacy**. This right covers several aspects, ensuring that no person, home or possessions can be searched without authorisation, and that personal communications and information are safeguarded from infringement or disclosure	**Implications for Young People Using Digital Health Services** For adolescents and young people accessing digital health services, Article 31 provides constitutional protection for their online health data, messages, teleconsultations and device-stored records. This means that such information is protected from unauthorised access, interception, disclosure or forced exposure. **Legal Protections and Professional Duties** The constitutional right to privacy underpins legal frameworks such as the Data Protection Act 2019 and the Health Act, as well as professional confidentiality obligations. These laws and duties require informed consent, secure handling of health data, purpose limitation and lawful bases for processing sensitive information. **Remedies for Breaches of Privacy** Should privacy be breached, individuals are entitled to remedies including complaints to regulators, civil claims and constitutional petitions. These avenues offer recourse when personal health information is exposed or mishandled. **Extra Risks for Adolescents and Safeguards** Adolescents may face additional risks such as family exposure, stigma or coercion. Article 31 reinforces their entitlement to confidential digital healthcare, enforces limits on unlawful parental or third-party access, and imposes obligations on both providers and the State to implement safeguards and proportional rights respecting policies within digital health systems.
The Constitution of Kenya, 2010	Article 35 of the Constitution of Kenya, 2010, guarantees every individual the **right to access information** held by the State or by any other person. This provision places a duty upon public bodies to publish and make key information available and accessible to the public	**Implications for Young People's Digital Health Rights** For young people, Article 35 significantly strengthens digital health rights. It ensures that they can acquire official guidance on health matters, access relevant policies, review health statistics, and examine procurement and approval records for eHealth tools. Furthermore, it grants access to information about how public digital services collect, use, and protect health data.

		Enhancing Transparency and Participation This right also supports transparency and encourages public participation in decisions concerning telemedicine and digital platforms. Young people are empowered to request records or seek explanations regarding government-operated health apps and programmes, fostering accountability in digital health initiatives. **Mechanisms for Challenging Withholding of Information** Article 35 provides avenues to challenge the wrongful withholding of information. Individuals can pursue such matters through the Access to Information Act, lodge complaints with the Ombudsman, or take legal action in court. **Exceptions and Accountability** While there are limited exceptions to this right, such as privacy concerns or national security, these must be narrowly interpreted. On balance, Article 35 promotes greater accountability, safer digital health services, and informed choice for young users.
The Constitution of Kenya, 2010	Article 43 of the Constitution **guarantees every individual the right to the highest attainable standard of health.** For young people, this right is increasingly relevant to digital health services and information. The provision of online and mobile health platforms must be ensured to be available, accessible, acceptable and of high quality. This includes requirements such as non-discrimination, affordability, clinical reliability, and safety.	**State and Provider Responsibilities** It is the duty of the State and health providers to guarantee that telemedicine, eHealth tools, and online health information are within reach for all young people, including those from marginalised groups. Confidentiality and informed consent must be safeguarded, and professional standards maintained in remote care. Additionally, arbitrary barriers—whether financial, technical, or legal—that hinder access to these services must be eliminated. **Remedies and Enforcement** Article 43 also provides for remedies in cases where digital health services do not meet required standards, or when denial, substandard quality, or unsafe digital care causes harm. Young people have the right to seek enforcement through regulators, the courts, or constitutional petitions to ensure that the State or health providers deliver safe, equitable, and effective digital health services.

Data Protection Act, 2019

The Data Protection Act, 2019 treats health information as a specially protected category of **"sensitive personal data", as defined in section 2 of the Act.**

Under this legislation, any processing of health data must adhere to strict requirements including the core **data protection principles:**

Section 25: Data Protection Principles
Under the Act, anyone handling personal data must follow these core principles:

1. Lawfulness, Fairness, and Transparency
- Data must be processed in a lawful, fair, and transparent manner.
- Individuals should be informed about how their data is being used.

2. Purpose Limitation
- Data must be collected for explicit, specified, and legitimate purposes.
- It should not be used for other purposes unless legally allowed.

3. Data Minimisation
- Only adequate, relevant, and limited data should be collected.
- No excessive or unnecessary data collection.

4. Accuracy
- Personal data must be accurate and kept up to date.
- Incorrect data should be corrected or deleted promptly.

5. Storage Limitation
- Data should be kept only for as long as necessary for its purpose.
- After that, it should be deleted or anonymised.

6. Integrity and Confidentiality (Security)
- Data must be protected against unauthorised access, loss, or damage.
- Appropriate technical and organisational safeguards must be in place.

Data controllers are obliged to embed security into their services from the outset, following the concept of "data protection by design and by default". Technical and organisational safeguards such as encryption and access controls must be implemented (section 41).

		Young people are granted clear statutory rights under the Act. They must be informed about what health data is collected and the reasons for its collection. **They have the right to access their records, request correction or erasure of data, object to or withdraw consent for processing, and receive or transmit their data (portability)**. Providers have specific duties to inform individuals and respond to their requests (sections 26, 29, 38, 40, 32). The Act recognises enhanced protections for children, requiring parent or guardian consent and age verification, though certain exceptions exist for counselling and child protection services (section 33). Processing of health data is restricted so that it may only be carried out by, or under the responsibility of, a healthcare provider or someone bound by professional secrecy, unless public health grounds apply (section 46). For high-risk digital health projects—such as large-scale profiling, AI applications, or national health programmes—a data protection impact assessment must be conducted, and the Data Commissioner consulted (section 31). Controllers are required to notify the Data Commissioner and affected persons in cases of serious breaches (section 43). The Office of the Data Protection Commissioner has powers to investigate, require remedies, and impose sanctions as laid out in sections 5 to 9.
Health Act, 2017	This is an act of parliament to establish a unified health system, to coordinate the inter-relationship between the national government and county government health systems, to provide for regulation of health care service and healthcare service providers, health products and health technologies and for connected purposes.	**Key Legal Protections for Young People in Digital Health under the Health Act, 2017** **Recognition of Digital Health Services** The Health Act, 2017 explicitly recognises e-Health and telemedicine as legitimate modes of delivering healthcare services. Both are referenced within the Act's definitions and Part XV (sections 2 and 103), confirming that digital consultations, electronic health records, and health applications are fully within the law's scope of regulated health provision.

Right to Privacy, Dignity, and a Standard of Care

Every person is entitled to be treated with dignity and to have their privacy respected as a matter of legal standard in healthcare (section 5(1)-(2)). This requirement, which stems from constitutional rights, also applies to digital health services, ensuring that the same level of privacy and respect is guaranteed in digital care as in traditional settings.

Information, Consent, and Youth

Healthcare providers are obligated to inform users, including, where relevant, their guardians about their health status, available treatment options, associated risks, and the right to refuse treatment. This information must be provided in a manner the user can understand (section 8). No health service may be administered without informed consent, except for narrowly defined exceptions (section 9). For young people, this means that providers must clearly explain digital health services and obtain appropriate consent. If disclosing information to a guardian would not serve the best interests of the young person, the Act allows for such disclosure to be withheld.

Confidentiality of Health Information

Information about a user's health status, treatment, or time spent in a medical facility is confidential under the Act. Disclosure of this information is only permitted with the user's written consent, by court order or other legal mandate, or when non-disclosure would present a serious threat to public health (section 11). This confidentiality extends to electronic health records and digital communications.

Health Information Systems and Provider Responsibilities

The Ministry of Health is required to establish a national, integrated health information system, with the power to set minimum standards, formats, and interoperability requirements. All healthcare providers must create and maintain health

information systems that comply with national standards, and adherence to these requirements is a precondition for operating licences (sections 105(1)-(5)). Additionally, the Cabinet Secretary is mandated to develop e-health legislation covering the management, protection, and use of personal health information—including telemedicine and health information banks (section 104). These provisions provide a legal framework for data security, responsible handling, and accountability in digital health platforms, especially those serving young people.

Complaints and Accountability Mechanisms

The Act grants every individual the right to file complaints about their treatment. Health facilities and government bodies must publish clear procedures for submitting complaints, investigate concerns, and provide appropriate responses (section 14). This system gives young people a way to seek redress if their rights are violated when using digital health services.

What This Means for Young People: Practical Takeaways

- Digital health services, including online consultations, health records, and mobile applications are fully regulated by the Health Act. These services must meet the same requirements for information provision, obtaining informed consent, and maintaining confidentiality as in-person healthcare.
- Healthcare providers are responsible for explaining how digital health data will be used and must secure informed consent from users. If sharing information with a guardian would not serve the young person's best interests, the Act allows for this information to be withheld (section 8(1)).
- There are legal obligations for providers to implement secure, interoperable health information systems. Compliance with these requirements is necessary for providers to be licensed, giving regulators the authority to enforce safer digital health services.

Digital Health Act, No. 15 of 2023	An Act of Parliament to provide for the establishment of the Digital Health Agency; to provide a framework for provision of digital health services; to establish a comprehensive integrated digital health information system; and for other connected purposes.	**Key Legal Protections for Young People in Digital Health under the Digital Health Act, 2023** **Recognition and Classification of Sensitive Health Data** The Digital Health Act, 2023 establishes a legal framework that specifically protects the digital health rights of young people. A core feature is the classification of "sensitive personal level health data" in Part IV (sections 19-20), which mandates that such data is handled with privacy, confidentiality, and equity as guiding principles. This ensures that young people's personal health information is given extra protection within digital systems. **National Health Information System and Governance** The Act requires the creation of a national integrated health information system, overseen by a dedicated Digital Health Agency (sections 15-18, 5-6). This agency is tasked with setting and maintaining standards for interoperability, ensuring that digital health platforms work together and adhere to the same protections for young people's data nationwide. **Privacy, Security, and Confidentiality Obligations** Mandatory security and privacy measures are required, with the Cabinet Secretary responsible for ensuring the confidentiality of sensitive data (section 24(1)-(5)). These measures include personalised authentication, role-based access controls, audit trails, and encrypted backups. Health data must be retained for a minimum of 20 years (section 25), with provisions for de-identification or archiving of records when they are no longer retained. The Act also establishes national and county health data banks and sets out rules for secure transmission of health data (section 26(1), (4)-(5)). **Permitted Uses and Limits on Disclosure** The permitted uses of health databanks are limited to care provision, public health, and research (sections 27-28). Unauthorized

uses of sensitive health data are strictly limited, and data controllers must implement administrative, technical, and physical safeguards to protect sensitive information (section 33). Offences and penalties are prescribed for tampering with, improperly disclosing, or sharing sensitive health data (section 35).

Consent and Youth-Specific Rules
Section 31 requires that consent is obtained before processing sensitive health data, and allows individuals to withdraw their consent (section 31(4)). There are expressly tailored rules for minors and persons without capacity (section 32), where a guardian or parent acts in the best interests of the young person and additional controls are placed on processing their data. Controllers have a duty to protect sensitive data through robust safeguards.

Access, Correction, and Data Portability Rights
Young people have the right to access and obtain copies of their personal health information, as well as to request the rectification or erasure of records (sections 36 and 39). The Act also mandates data portability and cross-references compliance with the Data Protection Act, 2019. There are strict requirements and limited grounds for releasing sensitive health data, with clear procedures set out before such release is permitted (sections 37-38).

Regulation of E-Health and Telemedicine
The Act recognises and regulates e-health and telemedicine services, imposing obligations on providers to deliver information, facilitate access to records, manage data as prescribed by law, and obtain appropriate consent for minors or persons with mental illness (sections 40-44, especially section 43(1)(a)-(c), (g), (h)).

Guiding Principles and Equity
The Act's guiding principles (section 4) state that digital health must be equitable and support the highest attainable standard of health, reinforcing youth-sensitive design and non-discriminatory access. Compliance with

Digital Health Act, No. 15 of 2023	An Act of Parliament to provide for the establishment of the Digital Health Agency; to provide a framework for provision of digital health services; to establish a comprehensive integrated digital health information system; and for other connected purposes.	the Data Protection Act, 2019 is explicitly required (section 61). **Summary of Young People's Rights** • Statutory rights to confidentiality of digital health data • Informed consent and the right to withdraw consent • Secure handling, access, and correction of their health records • Limited disclosure and strict procedures for data release • Remedies and penalties where breaches of these rights occur
Computer Misuse and Cybercrimes Act, 2018	This is an act of parliament to provide for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with computer and cybercrime matters; and for connected purposes.	The Computer Misuse and Cybercrimes Act, 2018 protects young people's digital health by criminalising common threats to the confidentiality, integrity and availability of their online health information and by giving law enforcement powers to investigate and stop abuses. Practical effect for young people: the Act makes hacking, unlawful access or sharing of health records a crime; it prohibits online harassment and impersonation that could expose or shame a youth seeking care; and it gives authorities powers to preserve evidence, compel service providers to assist, and prosecute offenders - all reinforcing the privacy and safety rights set out in the Constitution, the Data Protection Act 2019 and the Health sector laws.

A spotlight on Technology facilitated abuse

1. What is technology facilitated abuse/ technology facilitated violence?

This is an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person.

Any act that is committed, assisted, aggravated, or amplified by the use of information communication technologies or other digital tools that results in or is likely to result in physical, sexual, psychological, social, political, or economic harm or other infringements of rights and freedoms.

2. What are some of the acts that constitute technology facilitated abuse?

Doxing: Posting personal and sensitive information including home and work addresses, telephone numbers, email addresses and family names without their permission.

Cyber Stalking: Persistent, unwanted and/ or threatening surveillance, contact and/ or pursuit by technological means. Cyberstalking can turn to offline stalking and vice versa.

Cyber Bullying: A form of online harassment, the constant and intentional infliction of damage through digital technologies to undermine a target's self-esteem.

Online Harassment: Repeated conduct that threatens posters, scares, or abuses someone by sending degrading, offensive or insulting comments or images. Online sexual harassment mainly affects women, girls, and LGBTQ individuals.

Non-Consensual Ponography/ Revenge Porn: non- consensual sharing of intimate imagery. While commonly used "Revenge porn" is objectionable as it suggests consent from and wrongdoing by the survivor to provoke retribution.

Sextortion: A type of electronic blackmailing- the demand for money, sex or additional explicit images in exchange for not exposing intimate images or private information.

Online impersonation: Creating a fake profile and assuming someone's identity for nefarious purposes, including destroying someone's reputation or threatening her safety.

Online Defamation: Defamation involves the public release of false information that damages a person's reputation and that has the intention of humiliating, threatening, intimidating, or punishing the survivor. Given the strict gender norms that govern female sexuality, defamatory statements about women's sexuality are particularly harmful to survivors' reputations. In fact, most online defamatory attacks against women and girls often focus on their sexuality.

Online Sexual Exploitation: This term encompasses a number of sexually exploitative and harmful behaviors that occur or are facilitated online and through the use of digital technologies. They include online grooming, live-streaming of sexual abuse, online sexual coercion and extortion, online sex trafficking, and image-based sexual abuse.

3. What leads technology facilitated abuse?

Its mainly triggered by revenge, jealousy, political agenda, anger, sexual desire, monetary needs/desire, and ideological agenda. Additionally, TF GBV can be a manifestation of power dynamics, such as sexism, misogyny, or other forms of discrimination.

People also fail to realise it is a crime

4. Why is this an issue now?

Technology facilitated abuse is big now. While the internet and mobile technologies have created new opportunities for people to connect, share resources and experiences, and form communities, **these digital spaces have also provided tools and platforms for the replication and continuation of violence.** Abusers are now using technology to spread misinformation, hate campaigns, harassment based on gender, and intimate partner violence, among other harms.

5. What are the effects of technology facilitated abuse?

It has a negative impact on survivors' mental, emotional, and even physical health. Many survivors feel ashamed, afraid, and powerless as their personal lives are invaded and abused through online channels.

Sustained online harassment has severe effects on the mental health of individuals, including anxiety, depression, and post-traumatic stress disorder The compromised mental well-being of the victim may make them more vulnerable to physical or sexual aggression offline.

- HIV peer educator stops posting informational content online because of cyber bulling
- Women politicians leave social media-which is a great campaign tool, because of cyber stalking or online harassment. A younger woman looking to join politics is discouraged from joining politics because she sees how female politicians are harassed online.
- Women human rights defenders, activists and public figures who speak out on issues in society are increasingly being targeted with online harassment, doxing and censorship and this silences their voices.

6. What does the law say about it?

Sections 14 of the computer misuse and cybercrimes Act: unauthorised access and unauthorised inception: *Applicable to doxing, cyber-surveillance, cyber-stalking and non-consensual sharing of intimate images undertaken by accessing a survivor's computer and personal information or data.*

The Act says that you can be fined a Fine not exceeding five million shillings / imprisonment for a term not exceeding three years / both.

Section 16 of the computer misuse and cybercrimes Act: unauthorised interference: *Applicable to doxing, cyber-surveillance, cyber-stalking and non-consensual sharing of intimate images undertaken by intercepting the survivors' computer and transmitting data therefrom*
The Act says that you can be fined a Fine not exceeding ten million shillings / imprisonment for a term not exceeding five years / both

Section 22: of the Act: False publication: Applicable to online defamation and cyberbullying.
Fine not exceeding five million shillings / imprisonment for a term not exceeding two years, / both

Section 27: Cyberharassment: Applicable to cyberharassment, cyberbullying. A fine not exceeding twenty million shillings / imprisonment for a term not exceeding ten years / both.

Section 37: Wrongful distribution of obscene or intimate images: A fine not exceeding two hundred thousand shillings / imprisonment for a term not exceeding two years / both.

Sexual harassment: Section 23 of the sexual offences Act: Imprisonment for a term of not less than three years or to a fine of not less than one hundred thousand shillings or to both.

7. What can you do if this happens to you?

Report and file a case in court
Other Reporting avenues:

- To the platform
- National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) (KE-CIRT – Communications Authority of Kenya)

Always keep a record of the attacks. This will be used as evidence-so keep all the screenshots.

DHRP
Digital Health & Rights Project

KELIN
Reclaiming Rights, Rebuilding Lives

KCAT
KENYA COMMUNITY ADVISORY TEAM