



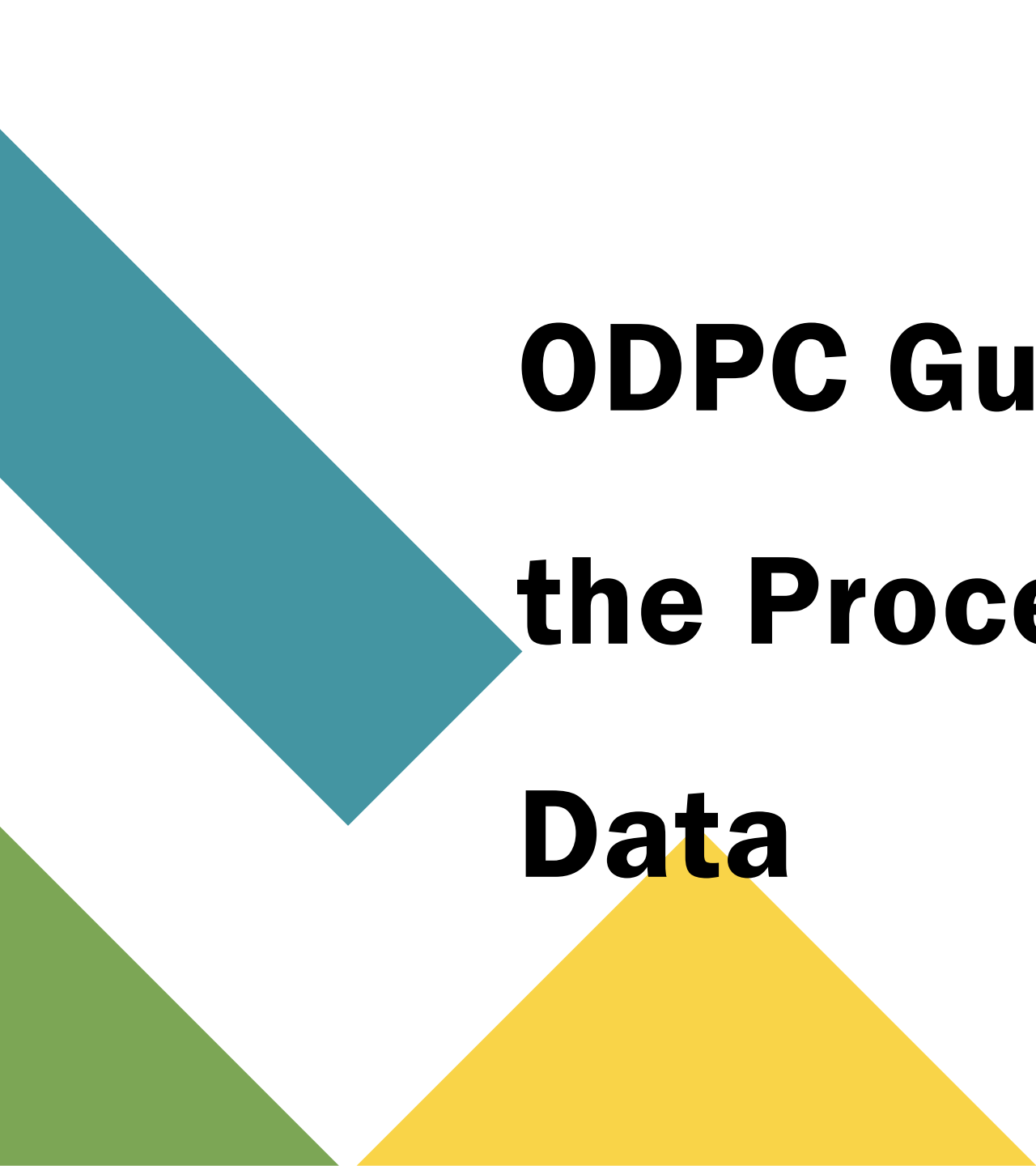
ODPC Guidance Note on the Processing of Health Data

Date: Thursday, June 13, 2024

Time: 7:30 am - 8:30 am



KHF Digital Health Committee



ODPC Guidance Note on the Processing of Health Data

Agenda

- Data protection Law in Healthcare
- Data Protection Key issues
- Guidance Note: Key Compliance Points
- Tools for Compliance



Data Protection Law in Healthcare



- Data Protection Act and Regulations
 - HAPCA, other health laws, projected laws (HIPAA), best practice
- ODPC Guidelines: Consent, Registration, DPIAs, Education
- ODPC Guidance Note on the Processing of Health Data
- Guidance Note: Key Compliance Points
- Tools for Compliance

Data Protection: Some Key Issues



- Weak Link game
- A principle-based law
- Sensitivity of Health data and special/protected categories of data subjects
- Convoluted compliance – High Cost of compliance
- Highly punitive law – Higher Cost of non-compliance
- Third party risk
- Ease of prosecution – Low barrier to litigation

Guidance Note: Key Compliance Points



- Setting up Governance structures
- Application of Principles
- Data Processing and Management - Processing, retention, commercial purposes
- Policies and communication/Privacy Notices
- Data Subject Rights Management
- Third Party Risk Management
- Health Data Transfer

Guidance Note: Tools for Compliance



- Training
- Vendor due diligence and compliance management – contracts/DPAs, notices, communication on breach
- IT – Privacy by design and default in systems, InfoSec, Technical controls

Guidance Note: Tools for Compliance



- Register of Data Protection Obligations
- Data Mapping and Inventory
- Record of Processing Activities
- Data Processing Impact Assessment
- Communication – policies, and Privacy notices

Guidance Note: Governance



- Privacy program, frameworks and strategy
 - Data Protection Officer(s)
 - Multi-disciplinary approach
 - Leadership from the top
- Policies, Privacy Notices, and Communication
 - Privacy policy, Processing policy and practices, Retention and destruction policies, data lifecycle management, retention schedules
- Monitoring and awareness
 - Training – CX, HR, IT, Clinical, Finance, other risky
- Privacy champions
- Vendor management – register of data processors
- Data Breach incidents Management - Privacy incident response playbook, data breach notification templates for third parties (may be contained in contracts)

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
<p>We respect the right to privacy as a fundamental human right as provided by Article 31(c) and (d) of the Constitution</p>	<p>Well implemented privacy program</p>
<p>We have identified an appropriate legal basis for our processing under Section 30 of the Data Protection Act (DPA).</p>	<p>Record of Processing Activities (RoPA)</p>
<p>In Health Sector, we process sensitive data, we have identified permitted grounds under section 44 of the DPA</p>	<p>Data Inventory and ROPA, Proper vendor management, notices issued to data subjects, policies in place</p>

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
We restrict processing where the legal basis ceases to apply	Proper Data Lifecycle management – Data Mapping and Inventory, ROPA , User awareness, technical measures/automation of cessation of processing – default to privacy/anonymizations and pseudonymization, data deletion and destruction policies and practices
We do not do anything generally unlawful with the personal data or inconsistent with the purpose for processing	ROPA - We have established the why How – training, privacy by design and default, technical measures

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
<p>If we are subject to mandatory registration, we have submitted to the ODPC accurate and up-to-date information concerning our processing activities</p>	<p>Registered with ODPC – submitted DPIAs, etc Controllers and Processors/Third parties are also compliant</p>
<p>We have considered how the processing may affect the individuals concerned and can justify any adverse impact</p>	<p>DPIAs – self, controllers and processors, vendors Special considerations for special categories of data subjects– Children, compromised capacities Consider - nature, scope, context and purposes</p>
<p>We only handle data about individuals in ways they would reasonably expect, or we can clearly explain why any unexpected processing is justified</p>	<p>Data subject Rights Management including communication, Privacy Notices, ROPA</p>

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
<p>We do not allow any discrimination or exploitation of the needs or vulnerabilities of a data subject</p>	<p>Data Subject Rights Management Principle of fairness Privacy by design and default</p>
<p>We do not deceive or mislead people when we collect their personal data</p>	<p>Privacy notices – detailed No such thing as over clarifying and over communication But be careful about setting up unrealistic expectations – You will be held accountable against your policies and communication.</p>
<p>We have clearly identified our purpose or purposes for processing and have clearly documented those purposes</p>	<p>ROPA - Many have argued that a ROPA is not mandated by Kenyan law as other laws clearly spell out and require the maintenance of a ROPA. However,</p>

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
We include details of our purposes in our privacy notices	Good privacy notices are founded upon a proper understanding of data movement, impact and processing activities so that the data subject is notified properly of all reasonable information Principle of transparency, fairness, lawfulness (LFT) Principle of purpose limitation
We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation	Purpose limitation Data Minimization Privacy by Design and default ROPA periodic updates
If we plan to use personal data for a new purpose, we check that this is compatible with our original purpose or we obtain specific consent for the new purpose	User knowledge Purpose Limitation Establishment of Lawful basis of processing through

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
We use technical measures to limit the possibility of repurposing personal data	Multi purpose - IT and InfoSec role CX as a common defaulter Data Minimization – Lower probabilities Data Anonymization and Pseudonymization Data Masking Data Access management Clarity on data retention, deletion and destruction ROPA - Which should contain sources/ collection point and purpose Restriction of access
We only collect personal data which is adequate, relevant, and limited to what is necessary for our specified purposes	ROPA
We can demonstrate the relevance of the data to the processing	ROPA

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
We periodically review the data we hold, and delete anything we don't need	Clarity on data retention, disposal, destruction, deletion Options such as masking, anonymization and pseudonimization
We avoid the creation of more copies or entry points for data collection than is necessary	Data Mapping exercise and data inventory should lead to a clean up of data collection and distribution ROPA will assist in establishing sources of data and can also inform clean up on data sourcing
We ensure that it is not possible to re-identify anonymised data or recover deleted data and test whether this is possible	Technical measures

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
<p>We ensure the accuracy of any personal data we process and the reliability of our sources</p>	<p>Data Quality Tools:</p> <ul style="list-style-type: none">• Data Profiling: This analyzes the structure and content of your data to identify inconsistencies, missing values, and potential errors.• Data Cleansing: This process corrects or removes inaccurate or incomplete data from your systems. Tools can automate this process for common errors.• Data Validation: This verifies that data conforms to pre-defined rules and formats. For example, ensuring email addresses follow a valid format or phone numbers have the correct number of digits.• Data Matching: This compares data from different sources to identify and eliminate duplicates.• Data Monitoring: This involves setting up ongoing processes to continuously check data quality and identify potential issues.

Guidance Note: CHECKLIST

CRITERIA

We ensure the accuracy of any personal data we process and the reliability of our sources

PRACTICAL COMPLIANCE

Data Source Reliability Techniques - May include

- **Source Verification:** Verify the legitimacy and reputation of the sources you collect data from. This might involve checking credentials, references, and industry expertise.
- **Data Lineage:** Track the origin and flow of data through your systems. This helps identify where errors might be introduced and simplifies troubleshooting.
- **Data Governance:** Implement policies and procedures to ensure data quality and consistency throughout your organization. This includes defining roles and responsibilities for data management.
- **Third-Party Agreements:** When obtaining data from third parties, establish contracts that clearly define data quality expectations and responsibilities.

Guidance Note: CHECKLIST

CRITERIA

We ensure the accuracy of any personal data we process and the reliability of our sources

PRACTICAL COMPLIANCE

Train employees for accuracy and importance to avoid high error rate in the first place
Automation of certain processing activities (there are rules on automation of data processing as well which we are not able to cover in this training)

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
<p>We have appropriate processes in place to check and verify the accuracy of the data we collect, and we record the source of that data</p>	<p>See previous examples - measures differ based on context</p> <p>This is also good from a business perspective – inaccuracies in data further the risks of fraud, errors, losses, litigation etc</p>
<p>We carry out tests for accuracy at critical steps</p>	<p>Data Map would show critical data heat points and critical steps at which data may/should be verified</p> <p>See previous examples - measures differ based on context</p> <p>Simple measures could be sampling of data</p> <p>Crowdsourcing – e.g HR data – ask employees to verify their data on platforms e.g HiBob will show you your own data as an employee but also reporting structures etc if a person is using such a platform they would be able to verify other information as well.</p>

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
<p>We use technological and organizational design features to decrease inaccuracy and mitigate the effect of an accumulated error in the processing chain</p>	<p>Data map - processing chain - critical points</p>
<p>We have a process in place to identify when we need to keep the data updated to fulfill our purpose properly, and we update it as necessary</p>	<p>ROPA Retention schedule or policy could also include update requirements</p>
<p>If we need to keep a record of a mistake, we clearly identify it as a mistake</p>	

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of personal data.	
As a matter of good practice, we keep a note of any challenges to the accuracy of personal data	
We know what personal data we hold and why we need it.	Data Mapping and Inventory Impact assessments Data retention and deletion ROPA Principles – data minimization, purpose limitation.

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
We carefully consider and can justify how long we keep personal data	Data retention schedule Data deletion and destruction ROPA
We have a policy with standard retention periods where possible	Retention Schedule - consider other legal obligations outside data protection Data Minimization Principle Retention and Destruction Policy Vendor Management Health Data may in some cases require to be permanently maintained Digital Health Act considerations
We regularly review our records with a view of identifying	Data retention policies and practices Third party risk for vendors – are they concious

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
<p>We have appropriate processes in place to comply with individuals' requests for rectification and/or erasure of false or misleading data about them.</p>	<p>Data Subject Rights management Data Subject Access Rights (DSAR)</p>
<p>We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.</p>	<p>Data Retention and deletion policies, practices and procedures</p>

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
<p>We do not transfer data outside Kenya unless there is proof of adequate data protection safeguards or valid consent from the data subject</p>	<p>Transfer Impact Assessments Data Mapping to identify transfers by yourselves, data processors Establishing lawful basis of transfer as a processing activity Establish schedule of countries where transfer can be done - use lists such as CNIL and for countries where you vary with an established authority, document your reasons Transfers can be in simple situations such as emails, WhatsApp etc because of cloud based systems, data centers located in foreign countries</p>

Guidance Note: CHECKLIST

CRITERIA	PRACTICAL COMPLIANCE
We checked and fulfilled all conditions set under part VI of the DPA and Regulations 2021	
We have documented those purposes.	If it's not documented, it didn't happen In God we trust, all other must present evidence Better still if you presented this evidence to ODPC before had eg DPIAs. ROPA
We include details of our purposes in our privacy notices	



QUESTIONS, COMMENTS



Thank you

Victory Loch

0757895131

gudoloch@gmail.com