Organization for Promotion of
Health & Community Development

Confidentiality & Data Protection Policy

OPHCD

Organization for Promotion of Health and Community Development



Table of Contents

1. INTRODUCTION AND LEGAL STATUS 2
1.1. VISION 2
1.2. MISSION STATEMENT 2
WELCOME TO ORGANIZATION FOR PROMOTION OF HEALTH AND COMMUNITY DEVELOPMENT 3
1. INTRODUCTION 3
1.1 BACKGROUND AND PURPOSE 3
1.2 SCOPE AND APPLICABILITY 3
1.3 OBJECTIVES OF THE POLICY 4
2. DEFINITIONS 4
3. DATA PROTECTION PRINCIPLES 5
4. CONFIDENTIALITY 6
4.1 EMPLOYEES 6
4.2 CONTRACTORS 6
4.3 SUPPLIERS: 7
4.4 PARTNERS OR SUB-PARTNERS 7
4.5 CONFIDENTIALITY CLAUSE 7
5. DATA SECURITY 8
5.1 PERSONAL DATA: 8
5.2 FINANCIAL DATA: 9
5.3 OPERATIONAL DATA: 10
6. DATA SECURITY MEASURES 11
7. POLICY BREACHES OVERVIEW 12
7.1 MINOR POLICY BREACHES: 12
7.2 MODERATE POLICY BREACHES: 13
7.3 MAJOR POLICY BREACHES: 13
8. POLICY REVISION AND UPDATES: 14
8.1 REVIEW CYCLE AND REVISION PROCESS: 14
8.2 NOTIFICATION OF POLICY CHANGES: 14
8.3 ACKNOWLEDGEMENT OF POLICY UPDATES: 14
CHANGE CONTROL HISTORY 15

Forward Note

Dear Esteemed Team Members,

It is with great pride and gratitude that we present the Confidentiality and Data Protection Policy of the Organization for Promotion of Health & Community Development (OPHCD). This comprehensive policy is a testament to our shared commitment to excellence, transparency, and accountability in all our operations.

As stewards of OPHCD's mission and values, the Board of Trustees is devoted to fostering an environment where every team member upholds the highest standards of confidentiality and data security. This policy serves as a vital framework to ensure that our organization operates with integrity, ethically, and in full compliance with all relevant regulations.

The Confidentiality and Data Protection Policy embodies the collective wisdom, expertise, and best practices of our dedicated team. It outlines a wide range of guidelines and procedures governing the handling of sensitive information, from collection and storage to sharing and disposal.

We strongly encourage each of you to familiarize yourselves with this policy, as it not only provides guidance but also reflects our organizational values and expectations. By adhering to these procedures, we reinforce the bedrock upon which our shared mission stands.

Should you have any questions, require clarification, or wish to propose enhancements to any aspect of this policy, we invite you to reach out to the Policy Review Committee or the Board directly. Your insights and feedback are invaluable as we continuously strive for excellence in safeguarding sensitive information.

Thank you for your steadfast dedication to the cause of OPHCD and the transformative work we undertake. Together, we are shaping a brighter future for those we serve.

Warm regards,

Muhammad Aziz Paewaston

General Director (OPHCD)

1. Introduction and legal status

Organization for Promotion of Health & Community Development (OPHCD) is a non-government, non-profit, non-political, impartial and independent organization registered with:

- the NGOs Department of the Ministry of Economy of the Government of Islamic Republic of Afghanistan with license No 4160
- the Ministry of Public Health of the Government of Islamic Republic of Afghanistan with the registration No 762

The organization established to serve the community and advocate for better coordinating and directing the available resources and activities for provision of quality services to the communities with an equitable manner. OPHCD, as a non-governmental organization committed for a joint mission with having dedicated and expert staff in public health, Water Sanitation and Hygiene, education, community development as well as volunteers who have been working in technical and managerial positions with national and international NGOs since more than one and half decade.

The members of the Board of Directors, senior Management Team (SMT) as well as the volunteers of the organization having appropriate experience, dedication and voluntarism which is a professional contribution to the health, education and development sector for achieving of more sustainable results. The core staff of OPHCD have more than one and half decade of successful experience of being directly involved in developing different policies and strategies as well as designing and implementation of projects in the areas of health, WASH, education and community development sectors such as; Primary Health care (PHC), Basic Package of Health Services (BPHS), Essential Package of Health Services (EPHS), Water & Sanitation and Hygiene, Primary education and Literacy programs, youth awareness and development, Public Nutrition, emergency preparedness and response and disaster risk reduction, trainings and coordination of different humanitarian Aids. Furthermore, the SMT and core Technical, Administration and Finance staff of the organization have up to date knowledge and rich experience of Grant Management, Project Management as well as conducting professional tasks of supportive Supervision, Monitoring, Evaluation, and Researches. Likewise, developing and on-time reporting (monthly, quarterly, annual, end of project and ad-hoc reports) to the donors and stakeholders, presenting the results of the aforementioned programs at the community, organizational, national and international levels are the expertise of the organization's technical and administrative staff.

1.1. Vision

An empowered society with sustainable and self-reliance health, social and economic stability at the community level.

1.2. Mission Statement

OPHCD, as a non-governmental organization is striving for well-being of the society with promotion of health and sustainable development of the communities through advocating

for better coordinating and directing the national policies and strategies as well as available resources and activities for provision of quality health, educational, social safety, human right and social welfare, economic, environmental and development services to the communities with the focus on the women and children, drugs users, IDPs and other marginalized group of the society with an equitable manner.

Overview of the Policy Manual

Welcome to Organization for Promotion of Health and Community Development

This personnel policy is provided to all OPHCD employees with clear guidelines regarding acceptable behavior and standards of operation. The outlined policies are effective and are valid until further notice. The English language version of this handbook is the legally binding document.

1. Introduction

This section of the policy sets the foundation for the entire framework. It provides an overview of the policy's purpose, scope, and commitment to upholding confidentiality and data protection principles within OPHCD. Additionally, it outlines the process for periodic review and revision to ensure the policy remains current and effective.

1.1 Background and Purpose

OPHCD handle a wide range of sensitive data, including information from donors, beneficiaries, and stakeholders. This policy is our commitment to safeguarding this data, ensuring confidentiality and compliance with legal obligations. It provides clear guidelines for our employees to protect the privacy and rights of all parties involved in our humanitarian efforts.

1.2 Scope and Applicability

This policy applies to all employees, contractors, suppliers, partners, sub-partners and stakeholders of the OPHCD who handle, process, or have access to personal data. It covers data pertaining to donors, beneficiaries, contractors, suppliers, and any other individuals or entities with whom OPHCD engages. Additionally, this policy extends to all forms of data encountered in the course of OPHCD operations, emphasizing the importance of confidentiality and protection across the board. Compliance with this policy is mandatory and non-negotiable for all parties within the scope of its applicability.

1.3 Objectives of the Policy

The primary objectives of this policy are to:

- **Ensure Legal Compliance:** To uphold the highest standards of data protection in accordance with applicable laws and regulations.
- **Protect Privacy Rights:** To safeguard the rights and privacy of individuals whose data is collected, processed, and stored by OPHCD.
- **Foster Trust and Transparency:** To instill confidence in our stakeholders by demonstrating a commitment to responsible data handling and transparency in our practices.
- **Mitigate Risks:** To identify and mitigate potential risks associated with the collection, processing, and storage of personal data.
- **Promote a Culture of Responsibility:** To instigate a culture within OPHCD that prioritizes the responsible handling of data among all employees and stakeholders.
- **Enable Effective Data Management:** To provide clear guidelines and procedures for the secure and efficient management of data across the organization.

2. Definitions

In this section, we provide various definitions pertaining to the policy and related concepts. These definitions aim to establish clear and precise meanings for key terms essential to understanding and implementing data security and privacy.

- **Personal Data:** Personal data refers to any information that relates to an identified or identifiable individual. This includes but is not limited to names, addresses, contact details, identification numbers, and online identifiers.
- **Sensitive Personal Data:** Sensitive personal data encompasses information of a more private or sensitive nature, such as racial or ethnic origin, political opinions, religious beliefs, health information, sexual orientation, and biometric data. Special care is taken when processing this type of data.
- **Data Controller:** A data controller is the entity or person responsible for determining the purposes and means of processing personal data. They are accountable for ensuring that data processing activities comply with applicable data protection laws and regulations.

- **Data Processor:** A data processor is an entity or person that processes personal data on behalf of the data controller. They act under the direction of the data controller and are responsible for implementing appropriate technical and organizational measures to protect the data.

- **Data Subject:** A data subject is the individual to whom the personal data relates. They have rights regarding the processing of their data and may include beneficiaries, employees, clients, or other individuals whose data is collected and processed.

- **Consent:** Consent is the voluntary, informed, and unambiguous agreement given by the data subject for the processing of their personal data. It should be specific, revocable, and obtained through clear and easily understandable language.

- **Processing:** Processing refers to any operation or set of operations performed on personal data, whether automated or manual. This includes collection, recording, organization, storage, retrieval, alteration, use, disclosure, and erasure.

- **Data Breach:** A data breach is a security incident where there is unauthorized access, disclosure, alteration, or destruction of personal data. It poses risks to the rights and freedoms of data subjects and requires timely notification and remediation.

- **Anonymization:** Anonymization is the process of removing or modifying personal data in such a way that the data subject can no longer be identified directly or indirectly. Properly anonymized data does not fall under the scope of data protection regulations

3. Data Protection Principles

OPHCD must be able to demonstrate compliance with the data protection principles, which are:

- **Lawfulness, Fairness and Transparency**: Personal Data must be Processed lawfully, fairly and in a transparent manner.

- **Limitation**: Personal Data must only be collected for specified, explicit and legitimate purposes.

- **Minimal Processing**: Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are Processed. Where possible, OPHCD must apply anonymization to Personal Data to reduce the risks to the Data Subjects concerned.

- **Accuracy**: Personal Data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified in a timely manner.

- **Storage Period Limitation**: Personal Data must be kept for no longer than is necessary for the purposes for which the Personal Data is Processed.

- **Integrity and Confidentiality**: Appropriate technical or organizational measures must be adopted to ensure security of Personal Data, including protection against accidental or unlawful destruction, loss, alteration, unauthorized access, or disclosure.

- **Accountability**: Data Controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

All Staff shall adhere to these principles when Processing Personal Data. Staff shall undertake data protection training within 3 months of joining OPHCD. This must be refreshed every 12 months, or more frequently if directed.

4. Confidentiality

Confidentiality is a cornerstone of the policy. It ensures that sensitive information, including donor, beneficiary, and stakeholder data, is kept private and accessible only to authorized personnel. Employees, contractors, and suppliers are required to adhere to strict procedures to maintain confidentiality.

4.1 Employees

Employees play a vital role in upholding confidentiality within the organization. Each staff member is bound by a confidentiality agreement *(annex-1)* upon joining, underscoring their responsibility to protect sensitive data. Access to confidential information is strictly limited to personnel with specific job-related requirements, ensuring that only those who require access have it. Regular training and awareness programs further educate employees on the importance of maintaining confidentiality.

4.2 Contractors

Contractors engaged by OPHCD play a critical role in maintaining confidentiality. As a standard part of their contractual agreement, they are bound by a confidentiality clause that

underscores their obligation to protect sensitive data. Access to confidential information is strictly restricted to contractors who require it for specific tasks, and they must adhere to the same confidentiality standards as employees. This ensures that all parties involved in our projects are aligned in upholding the confidentiality and integrity of sensitive information.

4.3 Suppliers:

Ensuring confidentiality extends to our relationships with suppliers. All agreements with suppliers will include a confidentiality clause, emphasizing their responsibility to protect sensitive data. Access to confidential information will be restricted to suppliers who require it for specific tasks, and they will be held to the same high standards of confidentiality as our employees and contractors. This ensures that our entire network of partners is aligned in upholding the integrity and security of sensitive information.

4.4 Partners or Sub-Partners

Partners and sub-partners engaged by the OPHCD are integral to our mission. Any agreements or collaborations with partners or sub-partners will incorporate a stringent confidentiality clause. This clause underscores their obligation to uphold the confidentiality of sensitive data, ensuring it is used solely for the intended purpose. Access to confidential information will be restricted to those directly involved in the relevant projects, and they will be held to the same exacting standards of confidentiality as our employees and contractors. This collective commitment to data security underscores our dedication to protecting sensitive information and maintaining the trust of our stakeholders.

4.5 Confidentiality Clause

The following confidentiality statement is hereby deemed an obligatory and integral component of all forthcoming contracts and agreements executed between OPHCD and its Suppliers, Contractors, Partner, Sub-partners, and any other involved party. This provision underscores the paramount importance of safeguarding sensitive information and upholding the organization's commitment to data security and privacy.

We (The Contractor) acknowledge and agrees that in the course of providing services to the Organization for Promotion of Health & Community Development (OPHCD), we may have access to and become acquainted with confidential information, including but not limited to donor lists, beneficiary data, financial records, and organizational strategies ("Confidential Information"). We shall maintain the confidentiality of all such information and shall not disclose, reproduce, or use it for any purpose other than the performance of their contractual duties for OPHCD.

We (The Contractor) further agree to take all necessary precautions to prevent unauthorized disclosure or use of Confidential Information. This obligation of confidentiality shall continue beyond the termination of the contract. Upon completion of the contract or at any time upon request by OPHCD, we (The Contractor) shall promptly return or, at OPHCD's option, destroy all copies of Confidential Information in our possession or control.

In the event of a breach of this confidentiality clause, we (The Contractor) shall be subject to a financial penalty, the amount of which shall be determined by OPHCD in its sole discretion, commensurate with the nature and extent of the breach. Such penalty shall be paid by the Contractor within 30 days of notification of the breach. Additionally, OPHCD reserves the right to pursue legal remedies available to it for any damages incurred as a result of the breach.

5. Data Security

Data security is of paramount importance to the OPHCD. It encompasses the protection of sensitive information from unauthorized access, disclosure, alteration, or destruction. This applies to all forms of data, including personal, financial, operational, and other sensitive information. The following outlines detailed procedures for various types of data and the security measures employed by OPHCD.

5.1 Personal Data:

Personal data includes information such as names, addresses, contact details, identification numbers, and any other data that can directly or indirectly identify an individual.

Procedure:

- **Access Control:** Authorized personnel with specific job-related requirements have access to personal data.
- **Data Encryption:** Personal data is encrypted during transmission and storage.
- **Regular Training and Awareness:** Ongoing training programs educate staff on personal data protection, privacy policies, and best practices.
- **Incident Response Plan:** An incident response plan is established to address potential breaches or unauthorized access to personal data.
- **Data Minimization:** Only the necessary minimum amount of personal data required for the intended purpose is collected and retained.

- **Secure Disposal and Deletion:** Personal data that is no longer required or has exceeded its retention period is properly disposed of or deleted.

5.2 Financial Data:

Financial data encompasses any information related to financial transactions, including bank account details, credit card numbers, and financial statements.

Procedure:

- **Access Control:** Only authorized personnel directly involved in financial operations shall have access to sensitive financial data.
- **Data Encryption:** Financial data, including transaction records and account details, shall be encrypted both during transmission and when stored in databases or electronic files.
- **Secure Storage:** Physical copies of financial documents shall be stored in locked cabinets or safes in a designated and controlled access area.
- **Secure Electronic Storage:** Electronic financial data shall be stored on secure, password-protected servers or systems. Access to these systems shall be restricted to authorized personnel.
- **Regular Backup and Recovery:** Financial data shall be regularly backed up and stored in secure offsite locations to ensure data recovery in case of unexpected incidents.
- **Vendor and Third-Party Management:** When engaging with vendors or third-party service providers for financial services, a thorough due diligence process shall be conducted to ensure they comply with data protection and security standards.
- **Anti-Fraud Measures:** Implement anti-fraud measures such as segregation of duties, two-factor authentication, and transaction monitoring to detect and prevent unauthorized or fraudulent financial activities.
- **Financial Data Retention:** Financial data shall be retained for the period required by regulatory authorities and based on OPHCD policies. After this period, it shall be securely disposed of using approved methods.
- **Employee Training:** All employees handling financial data shall receive specialized training on data protection, fraud prevention, and compliance with financial regulations.

- **Incident Response Plan for Financial Data:** A dedicated incident response plan shall be in place to address any breaches, unauthorized access, or other incidents involving financial data. This plan shall include clear roles, responsibilities, and communication protocols.

- **Compliance with Financial Regulations:** All financial data management and processing shall be conducted in compliance with relevant financial regulations and industry standards.

5.3 Operational Data:

Operational data pertains to information concerning the day-to-day activities of OPHCD, including project plans, logistics, and program data.

Procedure:

- **Access Control:** Access to operational data shall be limited to authorized personnel who require it for their job functions.

- **Data Encryption:** Operational data, including process logs, task lists, and workflow information, shall be encrypted during transmission and when stored in databases or electronic files.

- **Secure Storage:** Physical copies of operational documents shall be stored in designated, controlled-access areas, with restricted entry.

- **Secure Electronic Storage:** Electronic operational data shall be stored on secure, password-protected servers or systems. Access shall be limited to authorized personnel.

- **Regular Backup and Recovery:** Operational data shall be regularly backed up and stored in secure offsite locations to ensure data recovery in case of unexpected incidents.

- **Vendor and Third-Party Management:** When engaging with vendors or third-party service providers for operational services, a thorough due diligence process shall be conducted to ensure they comply with data protection and security standards.

- **Data Minimization:** Only essential operational data required for the intended purpose shall be collected and retained.

- **Employee Training:** All employees handling operational data shall receive specialized training on data protection, compliance with organizational policies, and adherence to operational procedures.

- **Incident Response Plan for Operational Data:** A dedicated incident response plan shall be in place to address any breaches, unauthorized access, or other incidents involving operational data. This plan shall include clear roles, responsibilities, and communication protocols.

- **Compliance with Organizational Policies:** All handling and processing of operational data shall be conducted in compliance with relevant organizational policies and procedures.

6. Data Security Measures

OPHCD places a paramount emphasis on safeguarding data integrity and confidentiality. OPHCD employs a comprehensive set of security measures to ensure the protection of sensitive information. This includes strict access controls, robust encryption protocols, and regular employee training on recognizing potential security threats.

- **Strong Password Policy:** Employees must create strong, unique passwords for their accounts, using a combination of upper and lower-case letters, numbers, and special characters. Passwords should be changed every three months to enhance security.

- **Access Control and User Permissions:** Access to sensitive data should be restricted based on job roles and responsibilities. Employees should only have access to information necessary for their specific duties.

- **Logout and Lock Workstations:** Employees should log out of their computers when leaving their desks, even for short breaks, to prevent unauthorized access. Workstations should be locked when unattended.

- **Shutdown Computers:** Employees should ensure that their computers are turned off when leaving the office for an extended period to prevent unauthorized access.

- **Confidentiality of Passwords:** Employees must keep their passwords confidential and refrain from sharing them with anyone, including colleagues and superiors.

- **Two-Factor Authentication (2FA):** Enable 2FA for all accounts, including email and sensitive systems. This adds an extra layer of security by requiring a second form of authentication.

- **Data Encryption:** Sensitive data, especially when transmitted over networks, should be encrypted to protect it from interception by unauthorized parties.
- **Secure Wi-Fi Networks:** Ensure that Wi-Fi networks used in the office are secure, with strong encryption protocols (e.g., WPA2 or WPA3) and a complex password.
- **Phishing Awareness:** Train employees to recognize and report phishing attempts. They should not click on suspicious links or provide personal information in response to unsolicited emails.
- **Secure File Storage and Sharing:** Use secure, encrypted file storage solutions and be cautious when sharing sensitive documents. Implement access controls to limit who can view or edit files.
- **Regular Software Updates:** Keep operating systems, applications, and security software up-to-date to protect against known vulnerabilities.
- **Firewall and Antivirus Software:** Ensure that firewall and antivirus software is installed and active on all devices to provide an additional layer of protection against malware and unauthorized access.
- **Data Backup and Recovery:** Regularly back up critical data and test the backup and recovery processes to ensure data can be restored in case of emergencies.
- **Employee Training and Awareness:** OPHCD regular training sessions on data security best practices, emphasizing the importance of safeguarding donor, beneficiary, and stakeholder information. Multi-Factor Authentication (MFA): Implement MFA for critical systems and applications to add an extra layer of security.

7. Policy Breaches Overview

Policy breaches refer to instances where employees or stakeholders deviate from established organizational policies and procedures. OPHCD takes policy breaches seriously, as they can potentially compromise the organization's integrity, security, and effectiveness. The following outlines detailed procedures for various types of breaches and the corresponding actions to be taken.

7.1 Minor Policy Breaches:

Minor breaches involve actions or omissions that are relatively minor in nature and have limited impact on operations or security.

Procedure:

- **Identification:** Identify and document the minor breach promptly after becoming aware of it.
- **Investigation:** Conduct a thorough investigation to gather facts and assess the severity of the breach.
- **Notification:** Notify the relevant parties involved, including the individual responsible for the breach and their immediate supervisor.
- **Correction and Education:** Provide corrective action, which may include additional training, counseling, or written warnings. Emphasizing the importance of compliance with policies.

7.2 Moderate Policy Breaches:

Moderate breaches involve actions or omissions that have a more significant impact on operations, security, or compliance.

Procedure:

- **Identification:** Promptly identify and document the moderate breach, ensuring that all relevant information is collected.
- **Investigation:** Conduct a comprehensive investigation, possibly involving multiple departments or stakeholders, to ascertain the extent and implications of the breach.
- **Notification:** Notify the relevant parties, including the individual responsible, their supervisor, relevant department heads, and the HR department.
- **Corrective Action:** Implement appropriate corrective action, which may include formal reprimands, probation, or suspension. Provide additional training and support as necessary.

7.3 Major Policy Breaches:

Major breaches are severe infractions that significantly impact the OPHCD's integrity, security, or compliance.

Procedure:

- **Identification and Escalation:** Immediately identify and escalate major breaches to the highest level of management and the Board of Trustees, if necessary.
- **Forensic Investigation:** Conduct a thorough forensic investigation, possibly involving external experts, to uncover all details and impacts of the breach.
- **Notification and Reporting:** Notify all relevant stakeholders, including the individual responsible, their supervisor, relevant department heads, the HR department, legal counsel, and regulatory authorities if required by law.
- **Disciplinary Action:** Administer appropriate disciplinary action, which may include termination of contract or legal action, depending on the severity and legal implications of the breach.

8. Policy Revision and Updates:

Policy revision and updates are essential to ensure that the Confidentiality and Data Protection Policy remains current and effective in addressing evolving challenges and regulatory requirements. This section outlines the processes and procedures employed by OPHCD to review, revise, and communicate policy changes.

8.1 Review Cycle and Revision Process:

OPHCD has a dedicated committee responsible for overseeing the policy review process (The Policy Review Committee). At defined intervals, usually annually, a comprehensive analysis is conducted to identify gaps in policy coverage and assess its overall effectiveness. Based on the outcomes of this review, proposed revisions are drafted, approved by The Board of Trustees, and then implemented.

8.2 Notification of Policy Changes:

Upon approval of policy revisions, OPHCD ensures that all relevant parties are promptly notified. Clear and concise notifications are distributed via various communication channels, including email, intranet announcements, and official notices. These notifications inform recipients of the nature of the policy changes and their implications.

8.3 Acknowledgement of Policy Updates:

To confirm that all stakeholders are aware of and understand the policy updates, OPHCD requires formal acknowledgment of receipt and comprehension of the revised policy. Stakeholders, including employees, contractors, and partners, are asked to confirm their understanding and commitment to adhering to the updated policy provisions. This acknowledgment serves as a record of compliance.

Change control history

Version No:	Approval date:	Approved by:	Change:
001	Jan,2021	Board of Trustee General Director	

Signature..... Date.....2021.....

APPROVED BY:

After the review of the policy, on behalf of the OPHCD Board of Trustees, the said manual is hereby approved and ready to be implemented henceforth.

Reviewed and Approved: Board of trusty.