Research and Study on Achieving Transparency in Health Sector through e-Governance

Ministry of Health and Population
Ramshahpath, Kathmandu
FY, 2081/82

Achieving Transparency in the Health Sector through e-Governance

Abstract

Improvements in healthcare service transparency and access combined with better accountability become possible through e-Governance integration in Nepal's health sector. The report investigates ways of attaining these goals by implementing Electronic Medical Record (EMR) dashboards. This study examines how information and communication technology gets adopted in both public health facilities and private healthcare institutions but also analyzes challenges regarding data security and compliance requirements as well as difficulties with infrastructure. The analysis includes an examination of worldwide best practices coupled with evaluation of three foreign nations: Estonia, Singapore and the United States. The adoption of modern digital technologies in Nepal will generate an efficient healthcare system that serves citizens with integrity while enhancing their medical care experience.

Keywords: Health Sector Transparency, Electronic Medical Records (EMR), Digital Health, Digital Governance, Healthcare Data Management, Interoperability, Health Dashboard.

Table of Contents

Chapter 1: Introduction

The Ministry of Health and Population (MoHP) develops health-related policies while directing collaboration and enhancing healthcare status throughout multiple population levels. Modern information technology enables the health sector to become more transparent while encouraging accountability and improved accessibility through enhanced service delivery. The report investigates the methods to reach the mentioned goals through e-governance systems and provides recommendations for the development of an Electronic Medical Record (EMR) dashboard.

1.1 Objectives

The primary objectives are:

1. To identify the types and formats of medical service data that hospitals must display on dashboards and websites to ensure transparency.
2. To evaluate the delivery of health services by hospitals and health institutions.
3. To promote accountability among health institutions, making health services more effective and accessible to citizens.

1.2 Scope of Work

1. Research and study into existing legislative acts which regulate hospital data privacy coupled with healthcare delivery policies will take place during this stage.
2. The research assesses both domestic as well as international leading practices used to publish healthcare data and services.
3. Research teams must investigate public and private health institutions which use information and communication technologies for patient data management to determine their security protocols.
4. Standard Development creates standardized hospital and health institution protocols that define which healthcare service information needs prompt website posting or dashboard accessibility, so the government and public receive full transparency.
5. Through Stakeholder Engagement officials meet and discuss with the concerned authorities and health workers and other associated stakeholders.
6. The presentation of the draft report to MoHP and its subsequent enhancement based on feedback will finalize the report.

Chapter 2: Methodology

2.1 Survey of Federal Hospitals

A survey was conducted across 30 federal hospitals to assess the current status of their Electronic Medical Record (EMR) systems.

2.1.1 Purpose

To understand how hospitals digitally manage patient and service-related data and evaluate their readiness for transparency initiatives.

2.1.1.1 Key Questions Addressed

- What is the status of EMR implementation in the hospital?
- What challenges do hospitals face in adopting and maintaining EMR systems?
- How secure and comprehensive are the existing EMR systems?

2.1.1.2 Methodology for Data Collection

- Structured questionnaires were designed and distributed to hospital administrators.
- On-site interviews were conducted with IT staff and healthcare providers.
- Observations were made regarding the infrastructure and usage of EMR systems.

2.2 Dashboard Content Analysis

Hospitals were engaged in discussions to identify essential information for inclusion in public dashboards.

2.2.1 Key Variables and Indicators

- Hospital infrastructure and service capacity.
- Analysis and monitoring of trending diseases.
- Availability of resources on critical care (e.g., ICU beds, ventilators, etc.).
- Monthly reports on patient admissions, discharges, and referrals.
- Real-time data on emergency services and response times.
- Patient flow in the health institutions.
- Availability of specialized medical services, medicines, and equipment.
- Staffing details, including qualifications, schedules, and expertise.

2.2.2 Process

- Workshops were organized with stakeholders to finalize the list of variables.
- Feedback from community representatives was incorporated to ensure relevance and accessibility.

2.3 Legislative and Policy Review

A detailed review of national laws, policies, and regulations concerning data privacy, health service delivery, and ICT applications was conducted.

2.3.1 Focus Areas

- Ensuring compliance with existing legal frameworks.
- Identifying gaps and recommending amendments to support transparency.

2.4 Best Practices Analysis

International examples of successful e-Governance initiatives in the health sector were studied to draw actionable insights.

2.4.1 Examples Included

- Open data initiatives in health from countries like Estonia and Denmark.
- Hospital transparency dashboards implemented in the United States and Singapore.

2.4.2 Focus

- Identifying strategies for balancing transparency and data privacy.
- Adopting scalable and cost-effective technologies.

2.5 Stakeholder Engagement

A participatory approach was adopted to ensure comprehensive input from all relevant parties.

2.5.1 Key Stakeholders Consulted

- Representatives from the MOHP and health sector regulators.
- Hospital administrators, IT managers, and health workers.
- Patients and civil society organizations.

2.5.2 Methods

- Focus group discussions to gather qualitative data.
- Structured interviews for in-depth understanding.
- Community surveys to capture user perspectives on transparency needs.

2.6 Data Analysis and Standard Development

Data collected from surveys, interviews, and workshops were analyzed to identify patterns, strengths, and gaps.

2.6.1 Output

- Draft guidelines specifying mandatory data categories for publication.

- Templates for dashboards and data visualization.

2.6.2 Validation

- The draft guidelines and templates were shared with stakeholders for feedback.
- Adjustments were made based on practical feasibility and stakeholder input.

2.7 Report Preparation and Validation

- A draft report consolidating all findings and recommendations was prepared.
- A validation workshop was conducted to review the draft report with MOHP officials and key stakeholders.
- Final adjustments were made to incorporate feedback, resulting in a comprehensive and actionable report.

Chapter 3: Legislative Review

Constitutional Provisions (Fundamental Rights)

Article No. 27: Right to information: Every citizen shall have the right to demand and receive information on any matter of his or her interest or of public interest. Provided that no one shall be compelled to provide information on any matter of which confidentiality must be maintained by law.

Article No. 35: Right relating to health: (1) Every citizen shall have the right to free basic health services from the State, and no one shall be deprived of emergency health services. (2) Every person shall have the right to get information about his or her medical treatment. (3) Every citizen shall have equal access to health services. (4) Every citizen shall have the right of access to clean drinking water and sanitation.

3.1 Individual Privacy Act, 2018 (2075)

The protection of personal data, and health information managed by hospitals and health institutions in Nepal depends mainly on the Individual Privacy Act of 2018 (2075). The legislation establishes both personal data protection mechanisms and individual privacy guarantees through the Nepal Law Commission (2018).

3.1.1 Key Provisions of the Individual Privacy Act, 2018

According to the privacy legislation, every individual possesses an absolute right to defend their body and personal boundaries when it comes to their property and residence also their documents, data, personal information and online information.

All parties must receive direct consent from people before personal data collection and keep them informed about data retention duration and its intended use. Organizations must not conduct unauthorized practices involving personal information collection or storage alongside forbidden retention or analysis or publication activities.

The Act designates particular information types as sensitive personal information that includes details about caste, ethnicity, political affiliation, religious beliefs, physical or mental health conditions, sexual orientation along with property details. All public authorities need proper authorization to process these sensitive information categories.

Organizations dealing with personal data must establish sufficient security systems to guard against any unauthorized alteration, disclosure and use as well as access attempts or broadcasting of personal data.

Violating the Act will lead to total fines reaching up to NPR 500,000 with the possibility of both prison time and financial penalties. The Act provides financial assistance to people whose privacy has been violated and their personal information has led to losses.

3.2 Electronic Transaction Act, 2008 (ETA)

The Electronic Transaction Act of 2008 serves as Nepal's foundational statute, controlling electronic transactions, cybersecurity, and digital signatures. The Act supports secure electronic information transactions through legal binding processes that specifically apply to EHR management and patient data operations by health and hospital services (Nepal Law Commission, 2008).

3.2.1 Key Provisions of the ETA

The Act enables electronic records and digital signatures through legal recognition, making them comparable to traditional handwritten and paper documents. Under the Electronic Transaction Act, all electronic contracts and documents or agreements have the same legal force as physical documents.

The ETA implements laws to prohibit illegal entry into electronic systems, data disclosure violations, and restrictions on the wrong usage of digital healthcare platforms. Penalties and imprisonment exist as sentencing options based on crime severity.

The act requires organizations to protect all sensitive patient data by establishing procedures that safeguard against unauthorized access, theft, and misuse. The regulation supports digital signatures for authenticating and verifying electronic health transactions by establishing their integrity while maintaining confidentiality.

CIO obtains penalties through monetary fines and imprisonment terms, including unauthorized medical database entry and breaches of private medical information.

3.3 National Cyber Security Policy 2023

The National Cyber Security Policy 2023 was approved by the Cabinet on August 8, 2023, to become Nepal's latest framework for cybersecurity development (Ojha, 2023). The policy works to build a safe digital environment that defends users from mounting cyber security threats, including hacking attempts, phishing activities, and online harassment.

3.3.1 Key Objectives of the National Cyber Security Policy 2023

The policy works to create both a shielded digital environment and complete protection of data structures with safeguards for individual and organizational information.

Through establishing a Cyber Security Center the policy aims to create a dedicated operational unit which will improve coordination between sectors when implementing cybersecurity measures. Human resources play a vital role in cybersecurity according to this policy so it implements digital literacy programs targeting women children and seniors among others. The policy recommends installing one National Internet Gateway (NIG) for central traffic control to prevent cyber attacks.

3.3.2 Concerns and Criticisms

Experts and advocacy groups express multiple concerns about the National Cyber Security Policy 2023, even though it was originally intended to be progressive. Public privacy stands under threat because the National Internet Gateway forces increased surveillance capabilities, generating widespread privacy concerns. According to critics, implementing policy provisions might result in increased censorship measures that restrict freedom of speech and reduce information access. The implementation success of this policy faces challenges because experts argue for stronger legislative support through defined laws, which will determine its effectiveness.

3.4 Right to Information Act, 2007

Access to information held by public entities through the Right to Information Act of 2007 enables Nepalese citizens to advance transparency establish good governance and increase public accountability. The Act establishes vital effects on health delivery systems, public health administration, and patient service rights. This law affects the health sector as follows:

3.4.1 Key Provisions of the Right to Information Act, 2007

People who are citizens can ask for documents that belong to public institutions by sending requests to both hospitals and health departments. Public health institutions must share health policies with their programs, budget plans, and performance records. Health department offices and all public organizations must actively disclose details about public health responsibilities alongside epidemic information and healthcare service details. Healthcare initiatives, facility information, and scheme updates must be available to the public through regular updates. It is free to ask for that information under the Act unless the subject approves its release or the law requires it. The Act upholds personal data privacy. This legislation enables the population to obtain essential data while still maintaining patient privacy standards. The law allows for disclosing sensitive data to protect public health when such measures can stop widespread health risks like pandemics and epidemics. The law mandates that health institutions establish duty positions to receive and process requests while they need to uphold open information practices.

3.4.2 Implications for the Health Sector

Through the Act public health institutions receive encouragement to share complete details about their policies and funding as well as resource distribution which enables public oversight. The transmission of data concerning diseases outbreaks and vaccination drives and health emergencies must occur in quick succession.

Patients and citizens who sign up for healthcare services have the right to ask for detailed documentation that includes information about protocols and periods of waiting time and expenses. This function allows them to make educated choices regarding their healthcare plans. The system gives people full awareness regarding the medical services funded by the government.

Through the Act the government develops better health governance by maintaining accountability which allows the detection of healthcare system inefficiencies alongside combating corruption. When the public can review performance reports of hospitals and health programs, they can experience quality health service delivery.

Next the Act maintains all healthcare data as private while allowing disclosure by public healthcare needs or patient agreement. Patients have security through this policy because it prevents their medical data from being wrongly used.

The Act promotes timely critical information distribution throughout health emergencies such as pandemics while decreasing public misinformation which leads to better crisis responses.

3.5 National Health Policy 2019

The National Health Policy of 2019 represents a complete blueprint that the Ministry of Health and Population of the Government of Nepal established to enhance health system capability and provide equal opportunities for quality health care services at every level of society. The policy exists as per Nepal's constitutional requirements to deliver basic health services while assisting in reaching the Sustainable Development Goals (SDGs).

3.5.1 Key Objectives of the Policy

The policy of Universal Health Coverage (UHC) aims to provide equal quality healthcare services no matter what status, geographic position or discriminatory factors might be present. The policy supports building a robust health system by adjusting infrastructure, human resources, governance framework, and funding strategies. The policy aims to eliminate health service inequalities by defending vulnerable groups and marginalized populations from healthcare disparities in coverage and results. The health system will benefit from increased prevention and promotion of healthcare that helps reduce disease burdens. Integration of Modern and Traditional Medicine for fostering collaboration between allopathic, Ayurvedic, and other traditional healthcare practices.

3.6 Telecommunication Act, 1997

- Electronic communication and network usage in Nepal are regulated.
- Ensures that healthcare institutions utilizing telemedicine or remote consultation services comply with telecommunication regulations.

3.7 Nepal Health Service Regulations, 2055 (1999)

These regulations outline the standards and procedures for health services in Nepal, including aspects related to the management and confidentiality of patient information (Nepal Law Commission, 2013).

By following these guidelines, health institutions can ensure compliance with Nepal's data privacy laws and protect the personal information of individuals they serve.

3.8 National Cyber Security Center Advisory 2024

The advisory document released on 21 January 2025 outlines comprehensive cybersecurity measures, focusing on e-governance systems in Nepal's health sector to enhance transparency and secure digital operations. Here is a summarized version tailored to the theme of health sector transparency:

3.8.1 System and Data Security

- Regular updates of websites, applications, and IT frameworks.
- Mandatory security audits and immediate resolution of identified issues.
- Backup and archival of critical data with a robust business continuity plan.
- Deployment of genuine, licensed hardware and software.

3.8.2 Access and Identity Management

- Implementing multi-factor authentication for access control.
- Enforcing strong password policies and regular password updates.
- Limiting access based on the "Need to Know" and "Least Privilege" principles.

3.8.3 IT Infrastructure and Network Security

- Utilizing advanced security tools (e.g., firewalls, IDS/IPS) with appropriate configurations.
- Network segmentation and SSL certificate deployment for sensitive applications.
- Enabling centralized management systems like Active Directory.

3.8.4 Awareness and Capacity Building

- Conducting regular cybersecurity training for staff.
- Educating stakeholders about phishing attacks, safe browsing, and email security.

3.8.5 Incident Response and Monitoring

- Maintaining detailed logs of access and system activities.
- Encouraging prompt reporting and resolution of anomalies or breaches.

3.8.6 Transparent Communication Channels

- Ensuring secure email communication through encryption and verified sources.
- Avoiding unauthorized third-party platforms for official communication.

3.8.7 Physical and Mobile Device Security

- Securing physical access to data centers and sensitive areas.
- Implementing secure practices for mobile devices and removable media.

By integrating these cybersecurity and governance measures, the health sector can ensure transparency, improve public trust, and maintain the integrity of sensitive health data and services.

3.9 Digital Nepal Framework, 2076 (2019)

In the context of the health sector, the Digital Nepal Framework serves as a roadmap to transform healthcare delivery using digital technologies. It includes:

- Developing robust digital health infrastructure, such as electronic health records (EHR), electronic health management information systems (eHMIS), and telemedicine platforms.
- Promoting e-health governance to improve access and transparency in healthcare services.
- Increasing digital literacy among healthcare providers and the public to use digital tools effectively.
- Strengthening public-private partnerships for health-tech innovations, ensuring costeffectiveness and better service delivery.

3.10 Directive for Operation and Management of Nepal Government's Information Technology Systems, 2071 (2014)

This directive, applied to the health sector, ensures the effective management of IT systems supporting healthcare delivery. Key provisions include:

- Establishing and maintaining secure health information systems.
- Standardizing protocols for data collection, storage, and sharing to enhance accountability.
- Ensuring IT systems are updated to meet the demands of healthcare management.
- Facilitating interoperability of health IT systems for seamless coordination between hospitals, clinics, and other healthcare entities.

3.11 Directive for Construction and Management of Government Office Websites, 2078 (2021)

In healthcare, this directive mandates the development of transparent and accessible websites for public health offices and hospitals. It focuses on:

- Providing up-to-date information on healthcare services, policies, and resources.
- Ensuring sites are user-friendly and accessible to all, including differently-abled individuals.
- Publishing performance metrics like hospital wait times, success rates, and patient feedback.
- Securing sensitive health data to maintain patient confidentiality.

3.12 Directive for Operation and Management of the National Information Technology Emergency Response Team (ITERT), 2075 (2018)

Applied to the health sector, this directive ensures robust cybersecurity to protect sensitive health data and maintain service continuity during emergencies. Objectives include:

- Preventing and responding to cybersecurity breaches in health IT systems.
- Ensuring the integrity of electronic health records and other critical data.
- Providing a framework for incident reporting and resolution for healthcare facilities.
- Coordinating with stakeholders to enhance cyber resilience in healthcare.

3.13 Directive for Electronic Correspondence (Email) Management in Government Entities, 2075 (2018)

This directive facilitates secure and transparent communication among health professionals and institutions in healthcare (MOCIT, Nepal, 2018). It ensures:

- Use of encrypted email systems for patient and policy-related communications.
- Regulation of access to email systems based on roles and responsibilities within healthcare entities.
- Use of government email for communication and use of digital signatures.
- Secure data exchange, including critical health data, to maintain confidentiality and transparency.
- Adoption of standardized communication practices to prevent errors and enhance service efficiency.

3.14 Standard for Mobile Applications of Government Entities, 2075 (2018)

In the health sector, this standard ensures the development of mobile apps that improve transparency and accessibility of healthcare services (Department of Information Technology, 2018). It focuses on:

- The app should be developed using Government Enterprise Architecture.
- Enhancing data security to protect patient information within mobile apps.
- The app should follow Open Web Application Security Project (OWASP) mobile security guidelines.
- Ensuring user-friendly design is in English and Nepali for broader public engagement.
- The app should work on poor network connectivity and offline mode.

Chapter 4: Study on National and International Best Practices

The dashboard is used mainly for work monitoring, policy-making, and transparency.

4.1 Nepal: Emerging Practices in Healthcare Transparency

Nepal has started adopting e-governance in healthcare, with some initiatives aiming to enhance transparency:

- Current Status:
  - Partial implementation of Electronic Medical Records (EMR) in federal, provincial, and local level hospitals.
  - Limited public dashboards providing healthcare data.
- Key Features:
  - MOHP has piloted health dashboards showcasing data on vaccination, maternal health, and emergency response efforts in DHIS2.
  - Focus on providing aggregate statistics for policymakers.
- Challenges:
  - Lack of standardized data collection.
  - Limited ICT infrastructure in rural areas.

4.2 Estonia: Pioneer in Digital Health

Estonia is renowned for its highly advanced e-Governance and health data systems:

- System Overview:
  - A unified electronic health record system accessible to all citizens and healthcare providers.
  - Interoperable data exchange among hospitals, clinics, and government agencies.
- Key Practices:
  - For Policymakers:
    - Real-time analytics on national health trends, hospital utilization, and disease outbreaks.
    - Data-driven resource allocation and policy formulation.
  - For Citizens:
    - Secure access to personal health records via the e-Estonia portal.
    - Transparency on medical bills and prescriptions.
- Success Factors:
  - Nationwide adoption of digital ID cards.

○ Strong legal frameworks for data privacy.

4.3 Singapore: Centralized and Accessible Health Information

Singapore has implemented a National Electronic Health Record (NEHR) system to streamline data sharing:

● System Features:

○ Integration of public and private healthcare providers.

○ Centralized dashboards for monitoring hospital performance and patient outcomes.

● Best Practices:

○ For Policymakers:

■ Aggregated data on healthcare utilization, population health metrics, and resource allocation.

■ Insights into chronic disease management and preventive care outcomes.

○ For Citizens:

■ A public-facing portal that lists hospitals, available services, and estimated costs.

■ Alerts on health campaigns and outbreak notifications.

● Impact:

○ Improved coordination across healthcare providers.

○ Enhanced patient satisfaction through transparent communication.

4.4 Denmark: Open Data for Healthcare Transparency

Denmark emphasizes transparency through open healthcare data initiatives:

System Overview:

○ The Health Data Authority publishes detailed reports and dashboards.

● Key Practices:

○ For Policymakers:

■ National datasets on patient outcomes, hospital efficiency, and healthcare spending.

■ Focus on evidence-based policymaking.

○ For Citizens:

■ Interactive dashboards showing hospital ratings, treatment success rates, and patient feedback.

■ Accessibility tools for non-expert users to interpret data easily.

● Strengths:

○ High public trust in government data systems.

○ Comprehensive legal frameworks for open data sharing.

4.5 United States: Hospital Transparency Initiatives

The United States focuses on empowering patients and improving accountability through healthcare transparency initiatives like Hospital Compare:

- Key Features:
  ○ Detailed reports on hospital performance, including infection rates, readmissions, and patient satisfaction.

○ Public access to cost estimates for standard procedures.

- Applications:
  ○ For Policymakers:

■ Regional dashboards with aggregated metrics for resource planning.

■ Insights into healthcare inequalities and system inefficiencies.

○ For Citizens:

■ A searchable database for comparing hospitals by quality, cost, and location.

■ Educational resources to help patients navigate the healthcare system.

- Challenges:
  ○ Balancing data transparency with privacy concerns.

4.6 Rwanda: Leveraging Digital Health for Transparency

Rwanda, a low- and middle-income country (LMIC), has made remarkable progress in digital health and transparency through its Rwanda Health Management Information System (RHMIS) and Rwanda Biomedical Centre (RBC) initiatives.

4.6.1 System Overview

- Rwanda has developed a centralized health data platform integrating information from public health facilities, community health workers, and private health providers.
- Emphasis is placed on making real-time data available for decision-making and public access.

4.6.2 Key Practices For Policymakers

- Integrated Health Dashboards:

- Aggregated data on disease surveillance, vaccination coverage, maternal health, and child mortality rates.
- Real-time monitoring of resource utilization, such as hospital beds and medical supplies.

- Data-Driven Policy Formulation:
  - Data collected from R-HMIS supports evidence-based health policy decisions and international reporting obligations (e.g., SDGs).

4.6.3 Key Practices For Citizens

- Community-Level Data Access:
  - Transparency in community health programs, including malaria prevention, family planning, and nutrition initiatives.
- Public Health Campaigns:
  - Dashboards display ongoing public health programs, vaccination drives, and disease prevention campaigns.
  - Citizens receive SMS updates for vaccination appointments or health emergencies.

4.6.4 Success Factors

- Strong Government Commitment:
  - Investments in e-Governance and public health infrastructure.
  - Close collaboration between the Ministry of Health, the RBC, and international donors (e.g., WHO, Global Fund).
- Community Health Worker Engagement:
  - An extensive network of trained community health workers supports data collection and reporting, ensuring grassroots-level coverage.
- Scalable Technology Solutions:
  - Use affordable and scalable ICT tools like mobile health (mHealth) platforms.

4.6.5 Challenges

- There is limited ICT infrastructure in remote areas, though mobile technology is bridging the gap.
- Ensuring long-term funding for digital health programs.

4.6.6 Impact

- Improved Transparency:

○ Policymakers can access timely and accurate data, enabling better resource allocation and health system performance evaluation.

○ Citizens are empowered with information on healthcare services and initiatives.

- Global Recognition:

○ Rwanda's digital health efforts have been recognized as a model for LMICs. They demonstrate how technology can improve health outcomes even in resource constrained settings.

4.6.7 Key Insights from Rwanda's Example

- **Community Engagement is Vital**: Leveraging local networks (e.g., community health workers) ensures comprehensive data collection and dissemination.
- **Affordable Solutions Work**: mHealth and SMS campaigns are cost-effective yet impactful methods for improving transparency and public awareness.
- **Strong Leadership Drives Success**: Government ownership and coordination with international partners are critical for sustained progress.

4.7 Key Insights from Case Studies

4.7.1 Segregated Information for Different Audiences

- Policymakers require aggregated, analytics-driven data for planning and evaluation.
- Citizens need simplified, service-oriented information to make informed choices.

4.7.2 Legal and Technical Infrastructure

- Strong legal frameworks are critical for privacy.
- Reliable ICT infrastructure ensures data availability and security.

4.7.3 Interoperability and Standardization

- Shared protocols like HL7 and FHIR enable seamless data exchange across systems.

4.7.4 Community Engagement

- Transparency builds public trust and empowers citizens to take active roles in their health management.

Nepal can learn from these global best practices to create an efficient, transparent, citizen-friendly health data system.

Chapter 5: Research and Study on the use of ICT in Nepalese Health Institutions

This study evaluates ICT adoption in Nepal's public and private health institutions, focusing on health services, patient data management, and security measures.

5.1 Methodology

5.1.1 Sample Selection

1. **15 health institutions** (10 public and 5 private hospitals) were selected to represent Nepal’s healthcare ecosystem.
2. Institutions were chosen from urban and rural areas to capture diverse ICT usage contexts.

5.1.2 Data Collection Methods

○ **Surveys**: Distributed to hospital administrators and IT departments.

○ **Interviews**: Conducted with healthcare providers, IT personnel, and data management officers.

○ **On-site Observations**: Reviewed ICT infrastructure, data handling processes, and patient management systems.

5.1.3 Evaluation Metrics

○ Extent of ICT integration in health services (e.g., EMR, telemedicine).

○ Data security practices and protocols.

○ Challenges in ICT implementation and maintenance.

5.2 Findings

5.2.1 ICT Use in Health Services and Patient Data Management

Public Hospitals ● Status:

○ 60% have partially implemented EMR systems.

○ Limited telemedicine adoption due to infrastructural and budgetary constraints.

● Applications:

○ Digital registration and appointment systems in major urban hospitals.

○ Electronic health management information system (eHMIS) in major health institutions (Majorly in Health Posts, UHC, CHU, BHSC,etc.)

○ Basic patient recordkeeping, with manual backups in rural areas.

Private Hospitals ● Status:

○ 80% have fully integrated ICT systems, including EMR, billing, and inventory management.

○ Telemedicine services are more prevalent in private facilities, especially in urban areas.

● Applications:

○ Advanced patient data management systems, including digital prescriptions and online patient portals.

○ Integration with diagnostic tools (e.g., lab and radiology reports).

5.2.2 Security Measures Employed

Data Protection Practices ● Public Hospitals:

○ Most rely on essential password protection for EMR systems.

○ Limited use of encryption or advanced security protocols.

○ Manual records are still retained for redundancy.

● Private Hospitals:

○ Advanced security protocols, including two-factor authentication (2FA) and data encryption.

○ Regular audits and compliance checks for data privacy regulations.

○ Firewalls and antivirus software to prevent unauthorized access. Access Control

● Public hospitals often lack role-based access controls (RBAC), leading to potential data breaches.

● Private hospitals implement RBAC, ensuring that only authorized personnel access sensitive data.

Data Backup and Recovery

● Public hospitals rely on manual or outdated backup methods, such as physical storage drives.

● Private hospitals use automated cloud-based backups with disaster recovery plans.

Compliance:

● Private hospitals adhere more to international data protection standards (e.g., ISO 27001).

- Public hospitals are in the initial stages of developing compliance frameworks.

5.2.3 Challenges in ICT Adoption

Public Hospitals

- **Resource Constraints**: Insufficient budgets for ICT infrastructure and maintenance.
- **Lack of Training**: Limited technical expertise among staff to manage and utilize ICT systems.
- **Connectivity Issues**: Poor internet access in rural areas hampers ICT functionality. Private Hospitals
- **Cost of Security Compliance**: High costs associated with implementing advanced security protocols.
- **Vendor Dependency**: Reliance on third-party vendors for ICT solutions leading to potential risks.

In summary, Nepal's healthcare institutions are gradually adopting ICTs, with private hospitals leading the integration and security measures. However, significant gaps remain, particularly in public hospitals. Addressing these challenges through targeted investments, capacity building, and policy development will enhance ICT adoption, improve data security, and increase transparency in healthcare services.

Chapter 6: Standard Formats and Guidelines for Data Publication

These guidelines provide a standardized approach for hospitals and health institutions to publish data and information on their websites or dashboards, ensuring transparency. They outline the data categories, update frequencies, and publication formats to communicate with the government and general public effectively.

6.1 General Principles for Data Publication

1. **Transparency**: All published information must be accurate, clear, and accessible.
2. **Timeliness**: Information must be updated regularly based on the defined frequency.
3. **Accessibility**: The dashboard must be user-friendly and available in multiple languages (e.g., Nepali and English).
4. **Data Security**: Sensitive and personal health data must comply with privacy regulations.

6.2 Data Categories to Be Published

6.2.1 Hospital Infrastructure and Capacity

Data Type	Details	Update Frequency	Format
Total Beds	General, ICU, NICU	Weekly	Table/chart
Equipment Availability	Ventilators, oxygen cylinders, dialysis machines	Weekly	Bar chart
Emergency Resources	Ambulances, stretchers	Real-time	Real-time counter

6.2.2 Service Performance Metrics

Data Type	Details	Update Frequency	Format

Patient Statistics	Admissions, discharges, referrals	Realtime	Line graph/table
Waiting Times	For outpatient, emergency, and specialist services	Weekly	Table
Service Utilization	Number of diagnostics/tests performed	Realtime	Pie chart/graph

6.2.3 Emergency and Critical Updates

Data Type	Details	Update Frequency	Format
Outbreak Alerts	Disease outbreaks and containment zones	As needed	Alert box on the homepage
Resource Shortages	ICU beds, oxygen, or critical medicines	Real-time	Live dashboard element

6.2.4 Community Health Programs

Data Type	Details	Update Frequency	Format
Vaccination Drives	Locations, dates, target groups	Weekly	Calendar/list
Health Camps	Specialist consultations, diagnostics	Monthly	Event details with registration links

6.2.5 Workforce Information

Data Type	Details	Update Frequency	Format

Health Staff Availability	Doctors, nurses, technicians	Weekly	Table/list
Schedules	OPD timings, specialist availability	Daily	Timetable format

6.2.6 Program-Wise Indicators

Data Type	Details	Update Frequency	Format
Immunization Program	Vaccination coverage, immunization schedules, Children's Immunized	Monthly	Bar chart/Table
Maternal and Newborn Health (MNH)	Maternal mortality, antenatal/postnatal care, newborn health statistics	Monthly	Line Graph/Table
Tuberculosis (TB)	TB case detection, treatment success rates, drug-resistant TB trends	Monthly	Table/Chart
NonCommunicable Diseases (NCDs)	Diabetes, hypertension, cardiovascular diseases, cancer screening, etc.	Realtime	Bar Chart
Other Programs	Major Indicators of other Health Management	Realtime	Bar Chart/Table

	Information System programs.		

6.2.7 Trend Analysis

1. **Historical Comparisons:** Visual representations of past and current health statistics.
2. **Epidemiological Trends:** Patterns in disease outbreaks and seasonal variations.
3. **Population Health Insights:** Changes in healthcare utilization, mortality, and morbidity over time.

6.2.8 Trending Diseases

1. **Outbreak Surveillance:** Identification of increasing cases of infectious diseases.
2. **Disease Mapping:** Geospatial representation of disease prevalence.
3. **Real-Time Alerts:** Notifications about emerging public health threats.

6.2.8 Additional Considerations

1. **Health Facility Performance Metrics:** Availability of staff, equipment, and services.
2. **Public Engagement:** Mechanisms for public feedback and inquiry.
3. **Interoperability:** Integration with national health information systems and databases.
4. **Data Visualization:** Graphical and interactive tools for better interpretation of data.

6.3 Data Publication Guidelines

6.3.1 Content Guidelines

1. Accuracy:

   ○ Verify all data before publication.

○ Indicate the source of the data.

2. Clarity:
   - ○ Use visual aids (charts, graphs) to make complex data comprehensible.

○ Provide explanatory notes where necessary.

3. Language:
   - ○ Publish in Nepali and English to ensure accessibility.

6.3.2 Dashboard Features

1. **Search Functionality**: Enable users to search for specific data.
2. **Real-Time Updates**: Use automation to update emergency and critical resource data.
3. **Mobile Compatibility**: Ensure the dashboard is responsive and works seamlessly on mobile devices.

6.3.3 Accessibility Standards

1. **Inclusive Design**: Ensure content is accessible to users with disabilities (e.g., screen reader compatibility).
2. **Multiple Formats**: Provide data in visual (graphs, charts) and downloadable formats (CSV, PDF).

6.4 Compliance and Monitoring

1. Periodic Audits:
   - ○ Conduct regular audits to ensure adherence to publication guidelines.
2. Feedback Mechanism:
   - ○ Incorporate user feedback to improve dashboard usability.
3. Reporting to Authorities:
   - ○ Submit monthly reports on data updates and transparency metrics to the Ministry of Health and Population (MOHP).

6.5 Templates for Data Publication

6.5.1 Example: Service Availability Table

Service	Available (Yes/No)	Total Capacity	Last Updated
ICU Beds	Yes	20	Jan 22, 2025

Oxygen Cylinders	No	--	Jan 22, 2025

Example: Patient Statistics Chart

- Line graph showing monthly admissions, discharges, and referrals.

Chapter 7: Discussions, Meetings, and Consultations with Stakeholders

Conducting talks, meetings, and consultations with relevant stakeholders is critical in ensuring the successful design, implementation, and adoption of e-governance initiatives in the healthcare sector. This section outlines the approach taken, key findings from these engagements, and their implications for achieving transparency in the health sector.

7.1 Approach to Stakeholder Engagement

7.1.1 Identification of Stakeholders

The following groups were identified as key stakeholders:

1. Government Authorities:
   - ○ Ministry of Health and Population (MOHP).

○ Provincial and local health offices.

2. Health Institutions:
   - ○ Administrators of public and private hospitals.

○ IT departments managing health data systems.

3. Health Workers:
   - ○ Doctors, nurses, and allied health professionals.

○ Community health workers, especially in rural settings.

4. Citizens and Civil Society Organizations:
   - ○ Patient groups and local health advocacy organizations.

7.1.2 Methods of Engagement

1. Focus Group Discussions (FGDs):
   - ○ Conducted with health workers and hospital administrators to understand ICT adoption and data management challenges.
2. Workshops and Seminars:
   - ○ Interactive sessions with government authorities and IT experts to design dashboard formats and set data publication standards.
3. Interviews and Surveys:
   - ○ Structured interviews with stakeholders to capture qualitative insights.

○ Online and in-person surveys to gauge the public’s expectations for transparency.

7.2 Key Findings from Stakeholder Engagement

7.2.1 Insights from Government Authorities

1. Policy Challenges:

   ○ There is a need for clear legal frameworks and guidelines to govern data transparency and privacy.

○ Limited inter-agency coordination in implementing digital health initiatives.

2. Capacity Gaps:

   ○ Lack of trained personnel to manage and analyze health data effectively.

7.2.2 Insights from Health Workers

1. Operational Challenges:

   ○ Overburdened with patient care, leaving limited time for data entry and management.

○ Resistance to adopting new ICT tools due to lack of training.

2. Recommendations:

   ○ Simplify data reporting processes to reduce workload.

○ Provide regular training on using ICT systems for health services.

7.2.3 Insights from Health Institutions

1. Public Hospitals:

   ○ Struggle with outdated infrastructure and inconsistent data management systems.

○ Require financial support to upgrade ICT capabilities.

2. Private Hospitals:

   ○ More advanced in ICT adoption but lack standardized data formats for public reporting.

7.2.4 Insights from Citizens and Civil Society Organizations

1. Expectations:

   ○ Citizens demand real-time updates on hospital services, waiting times, and emergency resources.

○ Advocacy groups emphasize the need for localized data to address disparities in healthcare access.

2. Concerns:

   ○ Potential misuse of personal health data and lack of clarity on privacy protections.

7.3 Recommendations Based on Stakeholder Input

1. Policy and Regulatory Framework:

   ○ Develop comprehensive laws governing health data privacy and transparency.

○ Establish clear roles and responsibilities for all stakeholders in data reporting and usage.

2. Capacity Building:

   ○ Train health workers on ICT tools and data management best practices.

○ Provide workshops for hospital administrators on implementing and maintaining dashboards.

3. Technology Upgrades:

   ○ Invest in ICT infrastructure, especially in public hospitals and rural areas.

○ Ensure systems are user-friendly and interoperable with existing health information systems.

4. Data Standardization:

   ○ Adopt standardized formats for reporting health data to ensure consistency across institutions.

5. Public Awareness Campaigns:

   ○ Educate citizens on accessing and interpreting health data dashboards.

○ Promote trust in the system by addressing data privacy concerns transparently.

7.4 Next Steps for Stakeholder Collaboration

1. Regular Consultations:

   ○ Schedule quarterly meetings with stakeholders to monitor progress and address challenges.

2. Feedback Mechanisms:

- Set up an online platform for stakeholders to provide feedback on the data dashboards.

3. Pilot Testing:
    - Implement pilot dashboards in select hospitals and gather stakeholder input for refinement.
4. Collaborative Partnerships:
    - Foster partnerships between the public and private sectors to leverage expertise and resources.

In Summary, engaging stakeholders through discussions, meetings, and consultations has provided invaluable insights into the needs, challenges, and expectations for e-governance in Nepal's health sector. These engagements have laid a strong foundation for creating a transparent, accountable, and user-centric health data system.

Chapter 8: Conclusion and Recommendations

Transparency in the health sector through e-Governance enhances service delivery and public trust. The successful implementation of this initiative hinges on the following:

1. Establishing clear and enforceable guidelines.
2. Ensuring robust ICT infrastructure and training.
3. Engaging stakeholders through collaborative efforts.

8.1 Recommendations for International Standard

- Adopt International Standards: Implement interoperable systems like FHIR/HL7 for consistent data sharing.
- Develop User-Specific Dashboards: Tailor dashboards separately for policymakers and citizens.
- Strengthen ICT Infrastructure: Focus on improving connectivity in rural and underserved areas.
- Enhance Legal Frameworks: Establish robust laws ensuring data privacy and transparency.
- Encourage Public Participation: Educate citizens on accessing and using health data effectively.

8.2 Recommendations from Stakeholder Engagement

- Strengthen ICT Infrastructure in Public Hospitals:
  - Invest in EMR systems and telemedicine capabilities, especially in rural areas.

○ Upgrade internet connectivity for seamless operation.

- Enhance Data Security Measures:
  - Implement encryption, RBAC, and automated backups in all health institutions.

○ Develop a unified data protection framework aligned with international standards. ● Capacity Building:

○ Provide ICT training to healthcare workers, emphasizing data management and security.

○ Promote knowledge sharing between public and private institutions.

- Public-Private Partnerships:

  - Leverage private sector expertise to improve public hospitals' ICT adoption and data security.
  - Jointly develop telemedicine solutions for underserved areas.
- Policy and Regulation Development:
  - Introduce comprehensive laws on health data protection and cybersecurity.
  - Monitor and enforce compliance through regular audits.

With strategic planning and commitment, e-governance can revolutionize the health sector, making it more transparent, efficient, and citizen-focused.

Reference

Nepal Law Commission. (2018, September 18). वैयक्तिक गोपनीयिा सम्बन्धी ऐन, २०७५. https://lawcommission.gov.np/content/12261/12261-the-privacy-act-2075/

Nepal Law Commission. (2013, May 13). नेपाल स्वास्◌्य सेवा ननयमावली, २०५५. https://lawcommission.gov.np/content/12671/12671-nepal-health-service-regulatio/

Nepal Law Commission. (2008). ववद्यु◌ि◌ीय (इलेतरोननक) कारोबार ऐन, २०६३. https://lawcommission.gov.np/content/13397/electronic--electronic--traded-international-act-2063/

Department of Information Technology. (2018). सरकारी ननकायका मोवाइल एप्पहरुको मापदण्ड – २०७५. https://doit.gov.np/content/12/12-%E0%A4%B8%E0%A4%B0%E0%A4%95%E0%A4%B0%E0%A4%A8%E0%A4%95%E0%A4%AF%E0%A4%95%E0%A4%AE%E0%A4%B5%E0%A4%87%E0%A4%B2-%E0%A4%8F%E0%A4%AA%E0%A4%AA%E0%A4%B9%E0%A4%B0%E0%A4%95/

Ojha, A. (2023, August 17). Government’s cybersecurity policy raises privacy and implementation concerns. *The Kathmandu Post*. https://kathmandupost.com/sciencetechnology/2023/08/17/government-s-cybersecurity-policy-raises-privacy-and-implementationconcerns

MOCIT, Nepal. (2018, November 13). सरकारी ननकायमा ववद्यिीयु पत्राचार (इमेल) व्यवस्थापन सम्बन्धी ननदेशिका | | Ministry of Communication and Information Technology.

MOCIT. https://mocit.gov.np/content/1176/1176-directives-regarding-the-manag/