POLICIES AND STRATEGIES TO MONITOR LEGAL, ETHICAL AND SAFETY MEASURES RELATED TO TECHNOLOGY

RAHBAR COLLEGE
OF DENTISTRY

PRINCIPAL
PROF. DR. MUHAMMAD NASIR SALEEM
RAHBAR COLLEGE OF DENTISTRY

No.102/RCoD/P-37 Dated: 5 Aug 2024

To: Director Admin

Info: Medical Branch

Prof. Dr. Muhammad Nasir Saleem
BDS (Hons), FCPS, MSc, ICMT,
FDS RCPSG, PhD (Scholar),
Principal
HOD Operative Dentistry,
Rahbar College of Dentistry, Lahore

No.102/RCoD/P-37 dated 5 Aug 2024

Info: Medical Branch

1. Introduction

This document outlines the comprehensive policies and strategies implemented at Rahbar College of Dentistry (RCoD) to ensure the responsible use of technology, adherence to legal requirements, and commitment to ethical standards and safety. These measures align with national regulations and international best practices, ensuring the protection of patient data, staff, and students.

2. Data Protection and Privacy Policies

2.1 Legal Compliance

- **PECA Compliance:** RCoD ensures compliance with the Pakistan Electronic Crimes Act (PECA) 2016 by implementing safeguards against unauthorized access and breaches.

2.2 Data Security Measures

- **Data Encryption:** All sensitive data must be encrypted during transit and at rest to ensure its protection from unauthorized access.
- **Access Control:**
    - **Role-Based Access Controls (RBAC):** Access to sensitive information is restricted based on the individual's role and responsibilities within the institution.
    - **Multi-Factor Authentication (MFA):** Mandatory for accessing critical systems and sensitive data, requiring two or more verification methods.

2.3 Regular Audits and Monitoring

- **Audit Logs and Monitoring:** Regular audits, including maintaining comprehensive logs of data access and modifications, are mandatory to ensure compliance and identify potential issues.
- **Third-Party Security Assessments:** Regular security assessments, including penetration testing, are conducted to identify and mitigate vulnerabilities.

3. Ethical Use of Technology

3.1 Informed Consent and Transparency

- **Informed Consent:** Patients must be provided with detailed consent forms explaining the use of technology in their treatment.
- **Transparency:** Patients should be informed about the technologies used in their care and their associated benefits.

3.2 Professional Conduct and Boundaries

- **Social Media Policy:**
  - **Professional Boundaries:** Staff and students must maintain professional boundaries online and refrain from sharing confidential patient information.
  - **Representation of RCoD:** Individuals associated with RCoD must present themselves professionally on social media, avoiding any actions that could harm the institution's reputation.
  - **Personal Use:** Personal social media accounts must not be used for communication with patients or discussing confidential matters.

3.3 Academic Integrity

- **Plagiarism Policy:**
  - **Original Work Requirement:** All student work must be original.
  - **Turnitin Usage:** Turnitin software is employed to detect and prevent plagiarism, ensuring academic integrity.
  - **Consequences of Plagiarism:** Any instance of plagiarism will be addressed according to institutional guidelines, which may include academic penalties and mandatory retraining on academic integrity. HEC Plagiarism Policy
- **Ethical Research Practices:** Guidelines for conducting ethical research are established, ensuring proper data collection, analysis, and reporting.

4. Health Management Information System (HMIS)

4.1 HMIS Integration

- **Data Management:** The Health Management Information System (HMIS) is used to manage patient data and ensure its accuracy and security.
- **System Security:** HMIS must comply with data protection regulations, including encryption and access control measures to safeguard patient information.

5. Cybersecurity Measures

5.1 Network Security

- **Network Security:** The institution must protect its network from cyber threats through robust firewalls and antivirus protection.
- **Secure Wi-Fi Access:** Only secure, encrypted Wi-Fi networks are to be used to prevent unauthorized access.

[illegible]

No.102/RCOD/P-37 dated 5 Aug 202

5.2 Incident Response and Data Breach Management

- **Incident Response Plan:**
    - **Detection and Response:** A clear protocol for identifying, reporting, and responding to cybersecurity incidents, including data breaches, must be in place.
    - **Containment and Eradication:** Procedures to contain and address the root cause of a breach.
    - **Recovery:** Defined steps to restore systems and data to normal operations and prevent future incidents.
    - **Communication:** Established channels for notifying affected individuals and authorities, ensuring compliance with legal obligations.

6. Training and Education

6.1 Staff and Student Training

- **Data Privacy and Security Training:** Regular training sessions on data privacy, cybersecurity, and ethical technology use are mandatory for all staff and students.
- **Patient Confidentiality:** Additional training sessions are conducted to emphasize the importance of patient confidentiality and the ethical handling of patient information.

6.2 Patient Education

- **Patient Information:** Patients should be informed about the technologies used in their care and the measures taken to protect their data.

7. Legal Compliance and Governance

7.1 Licensing and Accreditation

- **Regulatory Compliance:** All technologies, software, and equipment must be properly licensed and comply with the standards set by relevant authorities, including the PM&DC.

7.2 Ethical Review and Oversight

- **Ethical Review:** An ethics committee must review new technologies and their implementation to ensure adherence to ethical standards.

No.102/RCOD/P-37 dated 5 Aug 2024

8. Monitoring and Reporting

8.1 Continuous Monitoring

- **System Monitoring:** Tools are used to monitor technology and data usage, ensuring adherence to policies.
- **Performance Metrics:** Metrics are established to assess the effectiveness of technology-related policies.

8.2 Reporting Mechanisms

- **Whistleblower Policy:** Encourages the reporting of unethical or illegal activities, providing a safe and anonymous means for individuals to raise concerns.
- **Incident Reporting System:** A formal system for reporting data breaches, safety issues, and ethical concerns is in place.

9. Policy Violation and Disciplinary Actions

9.1 Identification and Reporting

- Any potential policy violations, whether related to data protection, ethical use of technology, or other guidelines, must be reported immediately to the appropriate authority, such as the IT department, ethics committee, or college administration.

9.2 Investigation and Assessment

- A thorough investigation will be conducted to assess the nature and extent of the violation. This may involve reviewing access logs, interviewing involved parties, and assessing the impact on affected individuals or systems.

9.3 Disciplinary Actions

- Depending on the severity of the violation, disciplinary actions may range from warnings and mandatory retraining to suspension, termination, or legal action. The institution reserves the right to involve law enforcement authorities if necessary.

9.4 Remediation and Prevention

- Following a violation, steps will be taken to address any weaknesses in the current policies and systems. This may include updating security measures, revising policies, and providing additional training to prevent future incidents.