Standard Operating Procedure (SOP): Telemedicine Platform Setup and Login Procedures

This SOP details the **telemedicine platform setup and login procedures**, covering initial system configuration, user account creation, secure authentication methods, password management, multi-factor authentication setup, user role assignments, troubleshooting login issues, and maintaining data privacy and security.

1. Initial System Configuration

1. Install the telemedicine platform software according to vendor documentation.
2. Configure server and client settings:
   - Set up domain, SSL/TLS certificates, and firewall rules.
   - Enable secure (HTTPS) access only.
   - Update system and apply security patches.
3. Test connectivity and performance before onboarding users.

2. User Account Creation

1. User onboarding requests must be submitted by department heads or designated personnel.
2. Administrator creates user accounts, assigning unique usernames and initial temporary passwords.
3. Assign user roles (e.g., Administrator, Healthcare Provider, Patient) based on job function and platform permissions.
4. Notify users via registered email with account setup instructions.

3. Secure Authentication Methods

1. Require strong, unique passwords adhering to policy guidelines (minimum length, character complexity, no dictionary words).
2. Enable Multi-Factor Authentication (MFA) for all users:
   - Provide options such as SMS, email, authentication apps, or hardware keys.
   - Guide users through initial MFA setup during first login.
3. Ensure login pages enforce account lockout on repeated failed login attempts.

4. Password Management

1. Prompt users to change temporary passwords at first login.
2. Enforce password expiration and periodic change intervals per institutional policy.
3. Provide self-service password reset options:
   - Utilize secure recovery (e.g., email/SMS validation, security questions)

5. User Role Assignments

1. Assign roles based on principle of least privilege.
2. Document user roles and permissions in the access control register.
3. Review and update roles at regular intervals or upon staff changes.

6. Troubleshooting Login Issues

1. Verify username and password are entered correctly.
2. Check for account lockout/disablement and reset as necessary.
3. Assist with password reset procedures as required.
4. Verify MFA device is functioning and accessible.
5. Escalate persistent or systemic issues to IT Support.

7. Maintaining Data Privacy and Security

1. Educate users on secure login practices and phishing risks.
2. Audit login attempts and maintain security logs.
3. Report any suspicious activity or breaches immediately to the Security Officer.
4. Ensure compliance with HIPAA, GDPR, or any applicable data protection laws.
5. Regularly review and update SOP as platform or security requirements evolve.

Note: All users must confirm understanding of these procedures before being granted access to the telemedicine platform.

Effective Date: [Insert Date]

Review Cycle: Annually or as required

Approved By: [Insert Approver Name & Title]