SOP: Procedures for PHI Transmission (Fax, Email, Electronic Portals)

This SOP details the **procedures for PHI transmission** via fax, email, and electronic portals to ensure secure and compliant handling of Protected Health Information. It highlights protocols for verifying recipient identity, using encryption and secure networks, maintaining confidentiality, and documenting transmissions. The purpose is to safeguard patient data during electronic communication and comply with relevant privacy regulations.

1. Purpose

To establish secure procedures for transmitting Protected Health Information (PHI) and maintain compliance with applicable privacy regulations.

2. Scope

Applicable to all staff transmitting PHI via fax, email, or electronic portals.

3. Responsibilities

- Staff must follow these procedures to ensure PHI confidentiality and security.
- Supervisors must ensure staff are trained and compliant with procedures.

4. Procedures

4.1 Fax Transmission

1. Verify recipient fax number before sending PHI.
2. Use a cover sheet stating â€œConfidential: Protected Health Information.â€
3. Confirm recipient is authorized to receive PHI.
4. Immediately retrieve transmitted faxes from the machine.
5. Double-check fax recipient details before transmission.
6. Document transmission in PHI transmission log.

4.2 Email Transmission

1. Confirm recipient's email address and authorization to receive PHI.
2. Transmit PHI only via encrypted email systems approved by the organization.
3. Indicate in the subject line that the email contains PHI (if required by policy).
4. Avoid including PHI in the email subject line.
5. Limit PHI in email content to the minimum necessary.
6. Include a confidentiality statement in the email footer.
7. Maintain a record of PHI emails per organizational policy.

4.3 Electronic Portal Transmission

1. Utilize only secure, organization-approved electronic health portals.
2. Validate recipient access rights to the portal before sharing PHI.
3. Require recipient authentication (e.g., login and password).
4. Limit PHI shared to the minimum necessary.
5. Document all portal-based PHI sharing in accordance with policy.

5. Verification and Documentation

- All transmissions must be logged with the date, time, recipient, sender, and method.
- Any errors or breaches must be reported immediately in line with organizational incident response protocol.

6. References

- HIPAA Privacy and Security Rules
- Organizational Privacy Policies and Procedures

7. Review & Revision

- This SOP will be reviewed annually and updated as necessary.