Patient Data Privacy Compliance Checklist

1. Consent & Patient Rights

| Obtain informed and explicit patient consent before collecting data.

| Provide clear privacy policy outlining data usage and rights.

| Enable patients to access, correct, or delete their data upon request.

2. Data Collection & Minimization

| Collect only data necessary for the platform's core functions.

| Limit sensitive data collection unless essential for care or operation.

3. Data Security Measures

| Implement encryption in transit and at rest for all patient data.

| Require strong authentication and authorization for data access.

| Regularly update and patch systems handling patient information.

4. Data Sharing & Disclosure

| Restrict data sharing to authorized entities with patient consent.

| Maintain detailed records of all disclosures of patient data.

5. Compliance & Monitoring

| Comply with applicable data protection regulations (e.g., HIPAA, GDPR).

| Conduct regular privacy and security audits.

| Train staff on data privacy and confidentiality best practices.

6. Incident Response

| Have a defined process for breach detection and notification.

| Inform affected individuals and authorities promptly if a data breach occurs.