

# HIPAA & GDPR Compliance — Early Assessment

## PillBox Care Medication Management App

| #                           | Requirement                       | Details                                                                                                                                     | Applies to | Compliant                           |
|-----------------------------|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------|
| Consent & legal basis       |                                   |                                                                                                                                             |            |                                     |
| 1                           | Lawful basis for processing       | Every type of data collected must have a documented legal basis — consent, contract, or legitimate interest.                                | GDPR       | <input checked="" type="checkbox"/> |
| 2                           | Explicit consent flow             | Consent must be obtained before data collection. It must be granular, freely given, and as easy to withdraw as to give.                     | GDPR       | <input checked="" type="checkbox"/> |
| 3                           | Consent for sensitive health data | Health data requires explicit consent under GDPR Art. 9. A separate, clear consent step is required for medication and symptom data.        | GDPR       | <input checked="" type="checkbox"/> |
| 4                           | Authorisation to access PHI       | Users must authorise access to their Protected Health Information (PHI) before it is stored or shared.                                      | HIPAA      | <input checked="" type="checkbox"/> |
| 5                           | Caregiver access consent          | When a caregiver is granted access, the patient must explicitly approve the scope and duration of that access.                              | Both       | <input checked="" type="checkbox"/> |
| Data minimisation & purpose |                                   |                                                                                                                                             |            |                                     |
| 6                           | Data minimisation                 | Only data strictly necessary for each feature may be collected. Every data field must be documented with its justification.                 | GDPR       | <input checked="" type="checkbox"/> |
| 7                           | Purpose limitation                | Data must be used only for the purpose it was collected. Secondary use (analytics, marketing) requires separate consent.                    | GDPR       | <input checked="" type="checkbox"/> |
| 8                           | Minimum necessary standard        | HIPAA requires that only the minimum PHI necessary for each function is collected. Every data field must be reviewed against this standard. | HIPAA      | <input checked="" type="checkbox"/> |
| 9                           | Data retention policy             | A defined retention period must exist for each data type. Data must be deleted automatically when it is no longer needed.                   | Both       | <input checked="" type="checkbox"/> |

| #                  | Requirement                         | Details                                                                                                                             | Applies to | Compliant                           |
|--------------------|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------|
| Security & storage |                                     |                                                                                                                                     |            |                                     |
| 10                 | Encryption at rest                  | All health and personal data must be encrypted at rest using AES-256 or equivalent.                                                 | Both       | <input checked="" type="checkbox"/> |
| 11                 | Encryption in transit               | All data must be transmitted over TLS 1.2+ with no insecure fallback permitted.                                                     | Both       | <input checked="" type="checkbox"/> |
| 12                 | Access controls                     | Role-based access controls must be in place. Only authorised users (patient, assigned caregiver) may access each record.            | Both       | <input checked="" type="checkbox"/> |
| 13                 | Audit logs                          | A complete audit trail of who accessed or modified patient data, and when, must be maintained.                                      | HIPAA      | <input checked="" type="checkbox"/> |
| 14                 | Breach notification procedure       | A documented process must exist to notify users within 72 hours (GDPR) or 60 days (HIPAA) of a data breach.                         | Both       | <input checked="" type="checkbox"/> |
| 15                 | Business Associate Agreements (BAA) | Any third-party service that handles PHI (cloud storage, analytics) must have a signed Business Associate Agreement (BAA) in place. | HIPAA      | <input checked="" type="checkbox"/> |
| User rights        |                                     |                                                                                                                                     |            |                                     |
| 16                 | Right to access                     | Users must be able to download or view all personal data the app holds about them.                                                  | GDPR       | <input checked="" type="checkbox"/> |
| 17                 | Right to erasure                    | Users must be able to permanently delete their account and all associated data. Deletion must be propagated to backups.             | GDPR       | <input checked="" type="checkbox"/> |
| 18                 | Right to data portability           | Users must be able to export their data in a machine-readable format (e.g. JSON, CSV).                                              | GDPR       | <input checked="" type="checkbox"/> |
| 19                 | Right to rectification              | Users must be able to correct inaccurate personal data at any time.                                                                 | GDPR       | <input checked="" type="checkbox"/> |
| 20                 | Right to restrict processing        | Users must be able to pause data processing without deleting their account.                                                         | GDPR       | <input checked="" type="checkbox"/> |
| 21                 | Patient right to access PHI         | Under HIPAA, patients are entitled to a copy of their PHI within 30 days of request. This must be supported in the app.             | HIPAA      | <input checked="" type="checkbox"/> |

| #                              | Requirement                                    | Details                                                                                                                                          | Applies to | Compliant                           |
|--------------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------|
| Transparency & documentation   |                                                |                                                                                                                                                  |            |                                     |
| 22                             | Privacy notice / policy                        | A clear, plain-language privacy policy must explain what data is collected, why, and how it is used.                                             | Both       | <input checked="" type="checkbox"/> |
| 23                             | Cookie / tracking notice                       | If the app uses analytics or tracking, users must be informed and given a meaningful choice to opt out.                                          | GDPR       | <input checked="" type="checkbox"/> |
| 24                             | Notice of Privacy Practices (NPP)              | HIPAA requires a formal Notice of Privacy Practices (NPP) to be presented to patients at first use.                                              | HIPAA      | <input checked="" type="checkbox"/> |
| 25                             | Data Processing Record (ROPA)                  | An internal Record of Processing Activities (ROPA) must be maintained as required by GDPR Art. 30.                                               | GDPR       | <input checked="" type="checkbox"/> |
| 26                             | Data Protection Impact Assessment (DPIA)       | A Data Protection Impact Assessment (DPIA) is required for large-scale processing of health data under GDPR.                                     | GDPR       | <input checked="" type="checkbox"/> |
| AI features                    |                                                |                                                                                                                                                  |            |                                     |
| 27                             | AI transparency                                | Users must be informed when a recommendation or alert is generated by an AI system.                                                              | GDPR       | <input checked="" type="checkbox"/> |
| 28                             | No automated decision-making without oversight | GDPR prohibits solely automated decisions with significant effects. All AI alerts must be advisory only and subject to human or clinical review. | GDPR       | <input checked="" type="checkbox"/> |
| 29                             | AI data sourcing                               | Data powering AI features must be sourced from verified, licensed medical databases.                                                             | Both       | <input checked="" type="checkbox"/> |
| 30                             | AI disclaimer in UI                            | The UI must clearly state that AI-generated content is informational only and not a clinical diagnosis or recommendation.                        | Both       | <input checked="" type="checkbox"/> |
| Caregiver & third-party access |                                                |                                                                                                                                                  |            |                                     |
| 31                             | Granular permission scopes                     | Patients must be able to define exactly what a caregiver can access (full vs. partial). Permission scopes must be documented and revocable.      | Both       | <input checked="" type="checkbox"/> |
| 32                             | Revocation of access                           | Patients must be able to remove caregiver access at any time, with immediate effect.                                                             | Both       | <input checked="" type="checkbox"/> |

| #  | Requirement               | Details                                                                                                                           | Applies to | Compliant                                                                           |
|----|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------|
| 33 | Data isolation on removal | When a caregiver removes a patient, the patient's data must be retained securely and remain inaccessible to the former caregiver. | Both       |  |