7. Compliance and Governance Documentation

Professional medical AI development in the UK requires thorough **compliance documentation** to demonstrate adherence to data protection laws, medical device regulations, and clinical safety standards. This ensures patient safety, ethical AI use, and readiness for NHS adoption or MHRA scrutiny.

Key documents reside in /docs/compliance/ as PDFs or Markdown files, with clear references to current (2025) guidance.

Data Protection Statement

- **GDPR/UK Data Protection Act 2018 Compliance**:
    - No real patient data is stored, processed persistently, or included in the repository.
    - All testing uses only public, fully anonymised datasets (e.g., MIMIC-CXR, TCIA).
    - Pipeline enforces mandatory anonymisation (DICOM PS3.15 profile) upon ingestion.
    - Temporary in-memory processing only; no logging of sensitive attributes.
    - Data minimisation: Only necessary metadata retained for clinical utility.
    - DPIA (Data Protection Impact Assessment) outline included, noting low risk due to no personal data handling.

Risk Assessment and Medical Device Classification

- **Potential Classification**: Likely **Class IIa** under UK MDR 2002 (as amended) for Software/AI as a Medical Device (SaMD/AIaMD) that provides information used for diagnostic purposes (e.g., highlighting findings to inform reporting).
    - Rationale: Assists in detection/characterisation of abnormalities in radiology imaging but does not provide standalone diagnosis.
    - Reference: MHRA "Software and AI as a Medical Device" guidance (updated February 2025) and Change Programme Roadmap.
- **Risk Management**: ISO 14971-aligned risk register included, covering bias, overfitting, false positives/negatives, with mitigations (human oversight, explainability).

Notes on Regulations

- **MHRA Guidance**:
    - Aligns with "Software and artificial intelligence (AI) as a medical device" (GOV.UK, latest 2025 updates).
    - Follows Good Machine Learning Practice (GMLP) principles (IMDRF/MHRA/FDA/Health Canada).
    - Intended purpose statement: "Assistive tool for clinicians in reviewing medical images and drafting reports; not for independent diagnosis."
- **NHS Adoption**:

    - DTAC (Digital Technology Assessment Criteria) self-assessment completed (current version under review in 2025; baseline standards applied).
    - Covers clinical safety (DCB 0129/0160), data protection, technical security, interoperability, usability/accessibility (WCAG 2.1 AA).
    - Prepared for procurement frameworks.

Human-in-the-Loop Emphasis

- Core design principle: AI outputs are advisory only; mandatory clinician review, editing, and approval required.
- Enforced via UI flags, audit logs, and documentation stating: "The system never replaces professional judgement; full accountability remains with the overseeing clinician."

Industry-Level Example Diagrams and Visuals

Figure 59: MHRA Software and AI as a Medical Device qualification flowchart (Decision tree for SaMD classification.) Suggested filename: fig59-mhra-samd-flowchart.pdf

Figure 60: MHRA AIaMD regulatory roadmap and change programme overview (2025 reform timeline.) Suggested filename: fig60-mhra-ai-roadmap.pdf

Figure 61: GDPR-compliant data flow in medical AI systems (Privacy-by-design architecture.) Suggested filename: fig61-gdpr-medical-ai-flow.pdf

Figure 62: NHS DTAC framework pillars and assessment criteria (National baseline standards diagram.) Suggested filename: fig62-nhs-dtac-pillars.pdf

Figure 63: Human-in-the-loop framework in AI-assisted radiology (Clinician oversight workflow.) Suggested filename: fig63-human-in-loop-radiology.pdf

Figure 64: Risk classification matrix for AI medical devices (MHRA/IMDRF aligned) (Device class determination.) Suggested filename: fig64-ai-risk-classification.pdf

Evidence Artefacts for Repository

- data_protection_statement.md
- risk_assessment_register.pdf
- dtac_self_assessment.xlsx (completed form)
- intended_purpose_statement.pdf
- clinical_safety_case_outline.pdf (DCB 0129 compliant)

This documentation positions the project as responsibly developed, regulator-aware, and NHS-ready, with clear emphasis on safety and human accountability. For future deployment, consider MHRA AI Airlock participation for live validation.