HowbeckHealthcare
Primary Care Innovation

ADOPTION OF AI IN PRIMARY CARE: BEST PRACTICE FRAMEWORK

Sharon Forrester-Wild
HOWBECK HEALTHCARE LIMITED
CREATED: JUNE 2025
VERSION: 3.0
WWW.HOWBECKHEALTHCARE.CO.UK

Contents

Introduction

This document articulates a comprehensive set of best practices for healthcare administrators and digital transformation leaders tasked with overseeing the deployment of artificial intelligence (AI) tools in clinical consultation environments.

Importantly, these AI systems are not intended to engage in diagnostic or therapeutic decision-making. Their use lies in augmenting administrative efficiency through functionalities such as real-time transcription, consultation summarisation and coding assistance.

The framework is aligned with UK General Data Protection (UK GDPR), Data Protection Act 2018, and NHS digital and ethical governance protocols.

Effective implementation of AI systems within health consultations requires careful orchestration of legal, ethical and procedural considerations. As healthcare organisations increasingly adopt digital tools to streamline workflows, the integration of AI must be handled with caution and foresight to maintain trust and ensure compliance. This document provides a detailed procedural roadmap to aid healthcare leaders in operationalising such systems.

By following these best practices, healthcare organisations can ensure AI is employed in a way that preserves clinician autonomy, protects patient data rights and improves the overall efficient of clinical administration. Each section in this framework is designed to guide implementation teams through the critical stages of adoption, monitoring and evaluation.

Articulate a clear operational scope

Defining the operational parameters of an AI system is essential to maintaining both legal clarity and clinical confidence. This requires clearly delineating what the AI tool is designed to do (e.g. transcribing a consultation) and what it is explicitly not authorised to do (e.g. diagnose or recommend treatments). Misrepresenting the tool's role can have serious ethical and legal implications.

By defining a precise scope, healthcare organisations prevent function (scope) creep and safeguard against overreliance on machine-generated output. Users must be aware that AI tools serve purely in a support function and that they remain accountable for patient care. Scope documentation should be embedded within training and operational documentation and patient-facing communications.

The AI system's role should be framed in a broader clinical governance structure, where accountability for decision-making is retained by qualified professionals. This approach not only mitigates risks but also reinforces the AI system's intended value as a tool that enhances clinical workflows. Structured documentation of the AI system's operational scope provides a consistent basis for internal audits, regulatory scrutiny and patient reassurance.

Implement staff training

Training staff is a critical success factor in the deployment of AI systems in health consultations. Users must be trained not only in how to use the system but also in understanding its limitations, purpose and compliance implications. This includes awareness of data protection principles, how AI integrates into existing systems and the necessity of human oversight.

Users should receive instruction on verifying AI-generated outputs, while administrative personnel might need guidance on error reporting and secure handling of AI outputs. Tailoring

the training experience ensures that each user engages with the AI system responsibly and effectively.

Training should be ongoing, not limited to initial onboarding. Scheduled refresher sessions and updates are necessary, particularly in response to software updates or changes in legislation. This continuous learning approach supports both individual competence and organisational preparedness, reinforcing safe and compliance usage over time.

Integrate real-time patient communication

Transparent communication with patients is essential when deploying AI systems in clinical environments, even for non-decision-making purposes. Clinicians should clearly explain the role of the AI system at the start of a consultation, e.g. stating that the system is being used to support transcription. This proactive disclosure respects patient autonomy and reinforces trust in the clinical process.

Effective patient communication should go beyond a one-time notice. Educational materials, such a posters, digital displays or patient leaflets/newsletter, can supplement in-person explanations. These resources should use plain language, avoid technical jargon, which offering accessible descriptions of what the AI system does and does not do.

Communication must emphasise that the AI system does not influence clinical decisions and that a human clinician remains fully responsible for all care-related judgements. This distinction should be reiterated across different patient point-of contacts to ensure a consistent message. Embedding transparency into everyday interactions enhances confidence and supports ethical alignment with informed consent principles.

Consent requirements

Explicit consent is necessary to uphold individual rights and ensure legal compliance. It must be informed, freely given and clearly documented. Consent mechanisms should allow patients to understand the scope of the data processing, the identity of the data controller and processor and their right to refuse or withdraw consent. Any digital interfaces or in-person forms should be designed with clarity in mind, ensuring they are accessible to diverse patient populations, including those with limited digital literacy.

Beyond initial consent collection, organisations must also establish systems for ongoing consent management and revocation. This includes recording when consent was obtained, any changes to the processing scope that may require renewed consent, and secure handling of withdrawal requests. Embedding these controls helps maintain patient autonomy and aligns with the accountability principle of data protection law.

Provide accessible opt-out pathways

Respecting the principle of individual autonomy, healthcare organisations must provide patients with clear and accessible options to opt out of AI-assisted elements of their care. This reinforces transparency and builds confidence in the integrity of care delivery.

Opt-out options should be embedded into clinical workflows and patient communications. For example, clinicians should be trained to offer an opt-out choice at the start of the consultation, especially when AI is being used for transcribing. Opt-out preferences can be recorded in patient management systems ensuring choices are respected across all encounters.

Effective opt-out mechanisms also include processes for review and escalation. Where patients express concern or confusion about the presence of AI in their care, staff must be empowered to provide clarification or escalate the matter to a designated Information Governance Lead. These processes should be documented, auditable and aligned with broader policies on patient rights and data protection.

Notify the practice population

Effective AI governance includes a proactive public communication strategy to inform the broader practice population about the introduction of the AI system. This is essential for maintaining transparency, fostering public trust and demonstrating organisational accountability. Patients must understand not only that AI is being used but also how it functions, what functions it performs and what safeguards are in place.

Communications should use multiple channels to maximise reach and accessibility, such as:

- Digital/physical signage in waiting areas
- Website announcement
- Newsletter bulletins
- Posts on social media platforms

The message should clarify at the AI system is used for non-clinical functions only (supporting administrative processes such as transcribing) and that clinicians maintain full responsibility for all healthcare decisions.

In crafting public messages, healthcare organisations should consider co-designing materials with their PPG or other patient representatives to ensure they are clear, respectful and appropriately tailored. Feedback should also be incorporated into the communication plans, allowing the organisation to measure understanding and respond to patient questions or concerns. In doing so, healthcare organisations can ensure that the introduction of the AI system is not only legally compliant but is also ethically and socially responsible.

Clarify the AI system's role publicly and internally

Ensuring that patients clearly understand the role of the AI system within healthcare consultations is crucial for transparency, risk management and trust-building. Internally, healthcare organisations should adopt consistent messaging and training materials that define the AI system's scope, its functions and its limitations. This should be standardised across all departments so that staff can confidently communicate the AI system's purpose and boundaries in their interactions with patients.

Externally, the organisation must publicly reinforce that the AI system is a support tool and not a substitute for clinical judgement. Public messaging should emphasise that while the AI system may assist with workflow optimisation, all diagnoses and treatment decisions are made solely by qualified health professionals. Such clarity is particularly important in avoiding patient misconceptions that could lead to distrust or unnecessary anxiety.

Supporting materials such as FAQs, information leaflets, posters and digital content should be regularly updated and co-designed with staff and patient groups to reflect evolving practices and technologies. Incorporating patient feedback into these resources strengthens clarity and demonstrates responsiveness and respect for patient perspectives.

Ensure human oversight and accountability

AI systems can assist in automating or expediting administrative tasks, however responsibility for clinical documentation, interpretation and patient communication remains with the system users. This ensures that outputs generated by AI systems are critically reviewed for context, accuracy and relevance to individual patient needs.

To operationalise system-user oversight, organisations should embed verification steps into all workflows that include AI outputs, e.g. clinicians must be required to review and approve any AI-generated transcriptions, summaries or coded entries before they are finalised in the patient's record. This may involve a structured checklist or audit trail that captures human review and sign-off, reinforcing both clinical safety and legal accountability.

It is essential to establish a governance framework that includes defined roles for clinical leads, IG panels and system administrators in monitoring how AI tools are used. Accountability structures must be clear, with escalation pathways for addressing incidents or discrepancies in AI output.

Monitor output quality and accuracy

The reliability of AI systems in healthcare is intrinsically tied to their ability to generate accurate output, therefore it is imperative that organisations adopt regular monitoring mechanisms to assess the quality and performed of AI-generated content. Monitoring should evaluate technical accuracy and clinical coherence, relevance and completeness. Errors or omissions in this context can lead to miscommunication, inefficiency or potential risks to patient safety if left unchecked.

To formalise the process, healthcare organisations could establish KPIs and benchmarks against which AI outputs are regularly assessed. Feedback should be integrated into these reviews, allowing clinicians and administrators to report inconsistencies or suggest improvements. A quality assurance team or internal governance panel could oversee this process and ensure that findings are used to improve system performance and inform retraining of the AI models where necessary.

Create structured feedback and escalation systems

To maintain a responsive and adaptive AI implementation, healthcare organisations must establish structured systems for collecting feedback and managing concerns relating to the AI system. Feedback from both staff and patients can uncover previously unidentified issues, useability challenges or subtle errors in AI-generated outputs. A formalised approach to gathering and evaluating this input is important for continual improvement.

Clinicians should be provided with straightforward mechanisms to report AI performance issues. Patients should have access to transparent reporting channels if they suspect inaccuracies or experience discomfort with AI involvement. These inputs must be triaged efficiently, with clear criteria for prioritising and responding to different types of concerns.

Escalation pathways must also be well-defined and embedded within the organisation's wider clinical governance framework. Issues that potentially affect patient safety, data protection or public trust should be elevated to a signeted AI oversight committee. Regular review of feedback trends can help inform retraining needs, policy adjustments or even discontinuation of underperforming systems.

Apply data minimisation and purpose limited principles

Data minimisation is a core principle of the UK GDPR and must guide all decisions relating to the configuration and use of AI systems during consultations. The data collected and processed should be strictly limited to what is necessary for the explicit, stated purpose of the AI system, which should be configured to access only the data it requires. Such controls can be enforced through system permissions, user role restrictions and access control policies.

The AI system should be regularly reviewed to prevent scope/function creep. Documentation should clearly define the intended data inputs and outputs for each system, with audit logs available to verify compliance. Adhering to minimisation and purpose limited not only ensures regulatory compliance but reinforces public trust in how AI systems are governed in healthcare settings.

Register AI use in Information Governance records

AI system deployment in healthcare settings must be full captured in an organisation's Information Governance records, include the Information Asset Register (IAR) and the Records of Processing Activities (RoPA). These formal registries are essential for demonstrating compliance with data protection regulations, identifying potential risks and maintain oversight over how patient data is processed through digital technologies.

When registering an AI system, the organisation must document key attributes, such as the name and version of the software, its primary functions, the categories of personal data it processes, the lawful basis for processing, third-party involvement, data flow diagrams and risk mitigations in place. These details should be maintained and updated regularly as part of the organisations standard IG procedures.

A well-maintained IAR and RoPA allow for timely audits, support investigations following incidents or complaints, and provide and accessible inventory of systems that can be evaluated for fairness, necessity and proportionality. Including AI systems into the existing IG infrastructure ensures transparency and strengthens accountability across clinical and administrative teams.

Schedule regular reviews and reassessments

AI systems in healthcare must be subject to periodic review to ensure continued alignment with clinical objectives, regulatory compliance, and organisational values. A formal schedule should be established for reviewing the AI system's performance, legal status, data protection impacts and user satisfaction. These reviews should be comprehensive, covering technical efficacy, operational reliability, and the contextual relevance of outputs.

Reviews should be multidisciplinary, involving clinical safety officers, digital transformation leads, IG panels and frontline healthcare staff who use the system. These sessions provide an opportunity to reassess whether the system is fit for purpose, identify any emerging risks and ensure the system's continued alignment with the original DPIA and organisational values. Stakeholder feedback gathered from patients should also be incorporated to ensure that the review process is ethically sound and community-informed. Outcomes from these sessions can guide system updates, inform vendor accountability measures, or lead to system replacement when necessary. Documenting each review and its recommendations demonstrates good governance and builds resilience into the lifecycle management of AI deployments.

Summary

Purpose

This summary outlines best practice procedures for the implementation and governance of Artificial Intelligence (AI) tools used to support clinical consultations. The aim is to ensure ethical use, legal compliance, patient trust, and enhanced administrative efficiency, without compromising clinician autonomy or patient care quality.

Scope

Applies to all clinical and administrative staff involved in the use, governance, and oversight of AI systems within consultation settings. The AI systems addressed are non-decision-making tools used for functions such as transcription, summarisation, and coding.

Statements

1. **Operational Scope**
    - AI tools must have clearly defined functions and limitations.
    - Must not be used for diagnostic or treatment decisions.
    - Scope documentation should be available in staff and patient materials.
2. **Training Requirements**
    - Ongoing training must be provided to all users.
    - Training includes system use, data protection, and verification procedures.
    - Updates must reflect legal changes and system upgrades.
3. **Patient Communication & Consent**
    - Clinicians must explain AI usage at the point of care.
    - Informed consent must be obtained and documented.
    - Patients must be offered opt-out options without affecting their care.
    - Use multiple formats (leaflets, signage, digital) for public communication.
4. **Transparency & Role Clarity**
    - Reinforce that AI is a support tool, not a clinical decision-maker.
    - Internal and external messages must be consistent and understandable.
    - Support materials should be co-designed with patient representatives.
5. **Oversight & Accountability**
    - Human review of AI outputs is mandatory.
    - Clinicians remain fully responsible for documentation and decisions.
    - Governance roles must be clearly assigned (e.g. clinical leads, IG officers).

6. **Monitoring & Quality Assurance**
    - Implement KPIs to monitor AI accuracy and reliability.
    - Establish feedback tools for users to report issues or suggest improvements.
7. **Feedback & Escalation**
    - Enable structured reporting from staff and patients.
    - Escalate safety, trust, or data concerns to designated oversight committees.
8. **Data Protection Compliance**
    - Adhere to data minimisation and purpose limitation principles.
    - Maintain system access controls and clear documentation of data usage.
    - Register all AI tools in the IAR and RoPA.
9. **Review & Reassessment**
    - Schedule periodic reviews of AI systems for performance and alignment.
    - Involve multidisciplinary teams and integrate patient feedback.
    - Document outcomes and use insights for updates or decommissioning decisions.

Governance requirements for adopting AI ambient software in General Practice

When general practices want to adopt AI solutions, such as ambient voice recording technology, it is essential to complete a series of governance documents and assessments to ensure compliance with data protection, clinical safety, and digital technology assurance standards. Three key documents typically required are the DTAC, DPIA, and DCB0160.

DTAC: Digital Technology Assessment Criteria

The Digital Technology Assessment Criteria (DTAC) is a national baseline standard developed by NHS England to assess digital health technologies for safe use within the NHS. It covers five key areas:

- Clinical safety
- Data protection
- Technical security
- Interoperability
- Usability and accessibility

Who completes it?
The supplier is responsible for completing and maintaining the DTAC assessment. However, general practices must ensure that any technology they adopt has passed or aligns with DTAC standards.

When is it required?
Before the deployment of any digital health technology that processes NHS data, especially when involving patient-identifiable information.

Best practice
- Ask suppliers to provide a completed DTAC assessment and supporting evidence.
- Review the DTAC status during procurement.
- Maintain DTAC compliance records for audit.

DPIA: Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a mandatory process under the UK GDPR that helps organisations assess and mitigate privacy risks associated with personal data processing.

Who completes it?
The data controller must complete the DPIA. Supplier input is often needed, especially in understanding how data is processed, stored, and safeguarded.

When is it required?
Whenever a new data processing activity is introduced that is likely to result in high risk to individuals, including:

- Recording and analysing patient consultations
- Use of AI or automated decision-making

Best practice
- Conduct the DPIA early, before deployment.
- Engage with the supplier for technical and security details.
- Consult your Data Protection Officer (DPO).

DCB0160: Clinical Risk Management: IT Systems

DCB0160 is a standard issued by NHS England that applies to health organisations deploying or using health IT systems. It ensures that clinical safety risks associated with digital systems are identified and mitigated.

Who completes it?
The healthcare provider organisation is responsible for ensuring a clinical safety case is produced. This may require appointing a Clinical Safety Officer (CSO) to oversee the assessment.

When is it required?
Before introducing any clinical IT system that impacts patient care, such as:

- AI transcription or voice recording software used in consultations

Best practice

- Appoint a qualified Clinical Safety Officer (CSO)
- Work with the supplier to complete necessary hazard logs and safety case reports
- Use DCB0129 (supplier equivalent) and DCB0160 together to ensure full coverage

Summary of Required Documents for AI Ambient Voice Recording

Document	Who Completes	When Required	Purpose
DTAC	Supplier	Before procurement	Assurance that the tool meets NHS standards
DPIA	Practice/ICB	Before go-live	Assess and mitigate privacy risks
DCB0160 and associated documents	Practice/ICB	Before go-live	Ensure clinical safety of IT system

DCB0160 for the AVT

What is a DCB0160?

A DCB0160 is a clinical risk management standard. It forms part of the NHS's statutory and regulatory framework and outlines how healthcare organisations must assess and manage clinical safety risks when using digital technologies that affect patient care.

What is the purpose of a DCB0160?

It makes sure healthcare providers:

- Protect patient safety during digital transformation
- Identify and mitigate clinical risks associated with the system

It also makes sure the chosen system does not introduce errors into workflows and that safety assurance is a continuing process.

Who must complete a DCB0160?

The DCB0160 needs to be completed by the healthcare organisation, NOT the supplier.

If you are implementing a new health system, modifying how an existing system is used or are integrating third party tools which interact with patient identifiable data (such as AI AVT) than a DCB0160 must be completed.

Core components of the DCB0160

Appointment of a Clinical Safety Officer (CSO)

Requirement

The CSO must be a registered clinician who is trained in clinical risk management.

Role of the CSO

- Oversees the risk management process
- Reviews and approves all safety documentation
- Ensures appropriate mitigations are in place for identified risks

Hazard log

What is it?

A structured log which potential clinical hazards of the system are listed. They include:

- Risk description
- Likelihood and impact
- Risk rating (red, amber, green or numerical)
- Mitigation measures
- Residual risk after controls

Purpose

To proactively identify and manage risks to patient safety.

Clinical Safety Case report

What is it?

A document which justifies why the system is safe to be used in a clinical setting. It provides:

- A summary of the system and its clinical function
- Description of the deployment environment
- Key hazards (from the Hazard Log) and how they are mitigated
- The CSO's signed statement of assurance that the system is safe

Purpose

To demonstrate that clinical safety has been assessed and managed throughout the deployment.

Clinical Risk Management plan

What is it?

A document which outlines how the clinical risk management will be applied to the system's implementation and ongoing use. It includes:

- Objectives and scope
- Roles and responsibilities (especially of the CSO)
- Processes for hazard identification, mitigation and review
- Review timelines and procedures for updates

Purpose

To provide a clear governance plan for clinical safety over the lifecycle of the system.

Change control and incident management process

What is it?

It is a process for:

- Managing system changes (new features, patch updates, etc)
- Investigating incidents or near misses
- Updating Hazard Logs and Safety Cases after changes or incidents

Purpose

To ensure safety documentation evolves with the system and any adverse impacts are addressed quickly.

Training records and Standard Operating Procedures (SOPs)

What are they?

They are:

- Documentation of staff training regarding operational and safe system use
- Written SOPs which reflect approved workflows.

Purpose

To make sure consistent use and understanding of the system's capabilities, limitations and fail-safes.

DCB0160 summary checklist

Document/Step	Required?	Owner	Purpose
CSO appointment	Yes	Healthcare provider	Oversees safety process
Hazard log	Yes	CSO/implementation team	Identify and mitigate clinical risks
Clinical Safety Case report	Yes	CSO	Declare system safe for use
Clinical Risk Management plan	Yes	CSO	Governance framework
Incident and change control procedures	Yes	Healthcare provider	Respond to change and issues
Training and SOPs	Yes	Practice Manager/COS	Ensure staff competency
DPIA (GDPR)	Yes	DPO/SIRO/IG Lead	Identify and mitigate data protection risks
Supplier DCB0129 and DTAC	Yes	Supplier	Assure safe and compliant design

Medicines and Healthcare products Regulatory Agency (MAHRA) Certification of the AVT supplier

AI scribe software is considered a medical device if it does more than just records and transcribes a consultation. Any AVT identified as a medical device under the UK Medical Devices Regulations (2002 as amended) must:

- Be registered with the MHRA and classified at least as a ClassI medical device (or higher, if applicable)
- Provide a UKCA marking or evidence of valid CE marking under transitional arrangements
- Supply a declaration of conformity and risk clarification rationale
- Be assessed for conformity with DCB0129 clinical safety standards.

Action required

- Verify classification with supplier
- Request MHRA registration number and copy of conformity assessment documents
- Log certification details on the DCB0160 Clinical Safety Case report.

Standard Operating Procedures (SOPs) for adoption of AI ambient voice technology during clinical consultations

Title:	Use of AI Ambient Voice Technology in Clinical Consultations
Purpose:	To ensure safe, effective and consistent use of AI-powered transcription systems in clinical settings, whilst maintaining high standards of patient confidentiality, clinical accuracy and legal compliance.
Applicability:	The SOPs apply to all clinical and administrative staff in the healthcare organisation who interact with or support the AI AVT system being used during patient consultations.
Review:	This SOP document must be reviewed on an annual basis, or whenever a significant change occurs (upgrade, a new risk identified, following an incident)

Version:	1.0
Date:	June 2025
Updated:	Initial version created
Reviewed by:	[Name of reviewer (SIRO/PM/IG Lead/Caldicott)]
Review due:	June 2026

System overview and purpose

The AI ambient transcription system is a voice-enabled tool that passively records spoken interaction during patient consultations and uses machine learning to generate a written transcript. This transcript is intended to assist clinicians in documenting the consultation but must not be used as a final medical record without human review and verification. The system operates without making diagnoses, suggesting treatments, or interpreting clinical data. Its sole function is to support documentation by transcribing conversations, which can enhance efficiency and reduce administrative burden of clinicians.

Roles and responsibilities

Clearly defined responsibilities ensure the system is used correctly and that any clinical or data protection risks are promptly addressed. The following table outlines the key roles involved in system operation and oversight:

Role	Responsibilities
Clinical Safety Officer	The Clinical Safety Officer ensures that AI technologies used in clinical settings are safe, effective, and support patient care. Key responsibilities include: • Conducting Clinical Safety Assessments (CSAs) for AI systems in accordance with DCB 0129/0160 standards. • Working with development and implementation teams to identify and mitigate clinical safety risks. • Reviewing AI-related incidents and safety reports, and initiating corrective actions where needed. • Providing expert input on clinical risk during procurement, development, and deployment of AI tools. • Supporting clinicians in understanding and using AI safely and effectively.
Clinical staff	Clinical users are responsible for the proper and ethical use of AI systems within their roles. Responsibilities include: • Using AI systems in accordance with approved clinical protocols and governance frameworks. • Providing feedback on the usability, effectiveness, and clinical impact of AI technologies. • Reporting any issues, incidents, or concerns related to AI system performance, safety, or compliance to the Clinical Safety Officer or appropriate governance teams. • Participating in training and awareness activities to ensure safe and responsible AI use in clinical practice.

Practice Manager	The Practice Manager plays a key coordinating role in overseeing operational readiness and staff engagement for AI adoption. Responsibilities include: • Supporting the integration of AI systems into practice workflows. • Ensuring staff training and compliance with relevant governance protocols related to AI. • Coordinating communication between governance leads (e.g. DPO, IG Lead, CSO) and frontline teams • Managing operational risks and ensuring that administrative and clinical teams are supported in AI use. • Updates the Record of Processing Activity (RoPA) and Information Asset Register (IAR).
Administrative/IT staff	The Administration and IT Team is crucial in enabling the technical and operational functionality of AI systems. Responsibilities include: • Assisting with the installation, configuration, and maintenance of AI systems. • Maintain system functionality • Supporting data input accuracy and system access controls. • Collaborating with the IG Lead and CSO to ensure data integrity, security, and clinical safety compliance. • Reporting system performance issues or concerns to governance leads and aiding in system audits or updates • Manage access credentials • Co-ordinate with the system provider
Senior Information Risk Owner (SIRO)	The SIRO has overall responsibility for managing information risks related to AI technologies. Their role includes: • Ensuring the organisation has effective risk management processes, policies, and controls in place for AI governance. • Overseeing the identification and mitigation of potential risks associated with AI deployment. • Collaborating with stakeholders, including the DPO, Caldicott Guardian, IG Lead, and Clinical Safety Officer, to address risks and compliance concerns. • Providing strategic oversight and direction to promote the responsible and ethical use of AI technologies within the organisation.

System operation

Pre-consultation checks

Before starting a consultation, clinicians must ensure the AI-enabled device is functioning correctly. This includes confirming that the microphone is active, the software is connected to the secure network, and the clinician is logged in using their individual, authorised credentials. A visual or audio system check may be prompted by the software and must be completed.

Patients must be made aware that the consultation will be recorded for transcription purposes. Consent must be obtained and documented prior to the recording starting.

During consultation

Clinicians should speak clearly and maintain a moderate pace. Background noise should be minimised, and where possible, both parties should avoid talking over one another, as this can reduce transcription accuracy. The AVT system should operate passively in the background and should not disrupt clinical engagement. If the system issues a warning or error (eg. audio interruption or low-quality capture), the clinician should acknowledge it and, if necessary, repeat or rephrase information.

If the clinician leaves the room whilst the patient remains in it, the AVT *must* be turned off until the clinician resumes the consultation.

Post consultation

Following the consultation, the clinician should review the transcription. The system may flag uncertain or low-confidence segments, and these must be reviewed carefully. Any corrections should be made before integrating the notes into the official medical record. The clinician holds final responsibility for ensuring the transcription reflects the consultation accurately.

Verification and editing

The output generated by the AVT is a draft and must verified by the clinician before becoming part of the patient's official health record. The verification process involves:

- Reading through the transcription for omissions, inaccuracies or contextual misunderstandings
- Editing any terms, figures or statements that may have been transcribed incorrectly
- Ensuring clinical summaries and outcomes are recorded correctly.

Clinicians must never file transcribed consultations without first confirming their content. Inaccurate records pose clinical, data protection issues and legal risks.

The table below outlines the minimum requirements for transcription verification:

Verification task	Required action
Review patient details	Confirm correct patient name and identifiers
Review clinical narrative	Check for accuracy in symptoms, history and dialogue
Correction of clinical outcomes	Ensure assessments, diagnoses, figures or onward steps are clear
Formatting and structure	Adjust formatting to meet electronic health records input requirements

Handling system failures or errors

When the AVT fails or performs inconsistently, it is critical that issues are reported and resolved without compromising patient care or documentation standards.

Common failure scenarios

Issue	Example
Audio not captured	Microphone muted or poor connectivity
Partial or incorrect transcription	Medication names misheard or missed
Access issues	User unable to access the system

Immediate response protocol

If a system error is encountered, the user must:

- Stop and document the issue as part of the incident and change control procedure
- Manually document the consultation notes using standard clinical recording methods
- Notify administrative or IT staff if technical support is needed
- Report repeated or serious errors to the CSO for review and potential escalation.

A named individual should be responsible for logging all failures, and patterns should be monitored to identify system issues.

Patient confidentiality and data security

All data processed by the AVT must be treated as confidential patient information, subject to the UK GDPR, the Data Protection Act 2018 and NHS guidance. Staff and users must follow these core data protection practices:

- Access to the system is role-based and limited to trained personnel
- Devices must be password protected and locked when left unattended
- Transcripts and audio files must be encrypted in transit and at rest
- No data should be stored locally unless approved by the SIRO or IG Lead.

Breaches of data security must be reported to the DPO and logged according to the organisation's data breach reporting policy. If relevant, breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

Consent and patient communication

Patients must be informed that their consultation will be transcribed for clinical documentation purposes. Best practice includes:

- Placing visible signage in public waiting areas
- Notifying patients and users via the organisation's website and social media
- Providing a verbal statement at the start of the consultation (eg."With your permission, this consultation will be transcribed to assist with documentation. You may refuse to give your consent or withdraw it at any time during the consultation."
- Documenting patient decisions if they decline or withdraw their consent to be recorded.

If a patient declines to be recorded or withdraw their consent, clinicians must switch to manual note taking immediately.

Training and competency

All users must receive formal training on the AVT before being granted access. Training should include:

- Step-by-step system operation
- Identification and correction of common transcription errors
- Data protection principles specific to AI and voice data
- The SOPs outlined in document.

Training completion must be documented using a training and competency declaration form, signed by both trainer and trainee. Regular refresher training is recommended or required when significant system updates occur or a new risk identified.

AI and voice data privacy requirements

All AI systems, including those processing biometric voice data or using natural language models, must comply with the following UK data protection laws, principles and regulations:

Legal frameworks

- UK GDPR (General Data Protection Regulation retained from EU law)
- Data Protection Act 2018 (DPA 2018)
- Common Law Duty of Confidentiality (CLoC)
- Human Rights Act (Article 8: Right to a private life)
- NHS Code of Practice on Confidentiality

Key Principles for AI and voice data (Article 5 of the UK GDPR)

Lawfulness, fairness and transparency

- Conduct a Data Protection Impact Assessment (DPIA) for high-risk processing
- Explicit consent is obtained to record and transcribe the consultation
- Explain how the AVT will be used and what its scope is

Purpose limitation

- Use voice data solely for the specified and legitimate purposes disclosed to the patient
- No secondary use unless compatible with the original purpose and has been identified within the DPIA.

Data minimisation

- Only process the minimum amount of voice/audio data necessary.

Accuracy

- Ensure the AVT are regularly tested to prevent misinterpretation or omissions
- Document errors, the rate of occurrence and correction mechanisms.

Storage limitation

- Store voice recordings only as long as necessary for clinical or auditing purposes
- Apply automatic deletion or review cycles.

Integrity and confidentiality (security)

- Voice data must be encrypted both a rest and in transit
- Use approved platforms for storing or analysing transcriptions
- Log access and actions taken if not the authorised user.

Accountability

- Align with DCB3058 (Data Security and Protection Toolkit – DSPT) and Caldicott Principles
- Maintain detailed records of processing issues involving the AVT