som
Supporting occupational health and wellbeing professionals

iOH

Artificial Intelligence (AI) Use Guidance for UK Occupational Health

Authors: Molly Healey, Janet O'Neill, Lucy Kenyon, Cameron Black, Su Chantry (iOH and the AI in OH Working Group)

January 2026

som.org.uk

Contents

1. Conflict of Interest (COI)

The authors have declared that there are no conflicts of interest.

2. Disclaimer

This guidance is designed to support OH professionals in using artificial intelligence (AI) responsibly, ethically and securely. It is not a substitute for legal, clinical or technical advice. Users must apply professional judgement and comply with relevant laws and standards. The Association of Occupational Health and Wellbeing Professionals (iOH), the Society of Occupational Medicine (SOM), and the AI in OH Working Group accept no liability for outcomes resulting from AI use based on this guidance. Technology references do not imply endorsement.

3. Introduction

This guide helps OH professionals navigate AI use in their practice. It brings together key principles from national policies and frameworks and is designed to be used alongside the AI risk assessment checklist. OH leaders are encouraged to oversee AI implementation, ensure staff are trained, and uphold governance and ethical standards. The goal is for AI tools to be reliable, accurate, and safe for use in occupational health settings without compromising people.

4. Ethical Use of AI

Transparency: Clearly communicate the purpose and function of the AI tools to staff and service users.

Fairness and Inclusivity: Use diverse, representative data to reduce bias. Regularly audit AI systems for fairness. Use non-discriminatory training data covering all demographics (age, gender, ethnicity, disability). Regularly check for and fix any biases.

Positive Impact: Prioritise AI applications that enhance health outcomes and workplace wellbeing.

Ethics Committee: Where feasible, establish or partner with an ethics committee to guide responsible use. Include technology, legal and clinical representatives. Partner with NHS trusts, academic institutions or external consultants as alternatives.

5. Data Protection and Privacy

Developer or adopter: Follow the checklists supplied for data compliance: Regulations and guidance for developers

AI and data protection risk toolkit: The ICO has the ICO AI and data protection toolkit designed to support organisations to reduce risks to individuals' rights and freedoms.

What data is being added: Consider what data is being used to develop the tool and whether any of the data is personal.

Where the data is going: Consider where the data is stored (which country), and what is happening to the data that is being used to train the tool. Consider interoperability, what systems the AI is integrated with, and how information is shared.

Confidentiality: Handle personal and sensitive information securely and follow data protection laws. Aggregate and anonymise data before using it in AI systems.

Consent: Get explicit consent for processing data with AI, as required by GDPR.

Data security: Protect AI systems from unauthorised access and data breaches. Regularly review and update security protocols.

Audits: Conduct regular audits and ethical reviews which consider the use and storage of data.

Appeals: Have a documented appeals process for AI-based decisions, which includes a clear pathway for appeal.

Protected health information (PHI) or sensitive data: Ensure PHI or sensitive data is not misused or exploited.

UK GDPR Article 6 **and** Article 9**:** Ensure you have a legal basis for processing data within these articles.

DPIA: Use a data protection impact assessment (ICO guidance and template).

6. Human Oversight

Decision-Making and Final Determination: Keep human oversight and remain human-centred in all decisions and final determinations involving AI. AI should support, not replace, human judgement.

Evidence: Check AI responses for inaccuracies and be aware of deepfakes (see glossary). Review AI responses against source documents.

Professional Review: Have appropriately qualified OH personnel review all AI-generated content before implementation.

Time and Resources: Clinicians must have the time and resources to oversee tools effectively.

7. Accountability and Transparency

Documentation: Keep records of AI use and contributions. Use an AI register and accountability report to track AI applications and outcomes.

Clear Processes: Establish clear processes for human review and an explanation of AI-driven decisions. Ensure stakeholders understand how AI tools are used and why.

8. Risk Management

Protocols: Develop ethical AI protocols outlining principles, governance and guidelines. Consider international and national laws, regulations and compliance frameworks.

- The EU Artificial Intelligence Act (AIA, Title III and Annex IV) does not apply in the UK but does influence standards.
- The UK Data Protection Act (2018, Part 2, Chapter 2). AI systems used in OH must process personal data lawfully, fairly and transparently.
- The UK Equality Act (2010, Section 19). Organisations deploying AI in OH must ensure systems do not discriminate, directly or indirectly, against individuals based on protected characteristics. Public sector bodies also have a legal duty to consider equality impacts under the Public Sector Equality Duty (PSED), making inclusive design and regular auditing essential for compliance.
- The UK AI Security Institute's AI governance guidelines are voluntary but have an influential role in developing policy and guidelines. We recommend monitoring published updates.
- ISO/IEC 42001 accreditation standards for the use of AI.
- HSE provides a guide to the regulatory approach to AI use in the workplace.
- MHRA guidance 'Software and artificial intelligence (AI) as a medical device' in the UK and EU MDR in Europe.
- The NICE evidence standards framework for digital technologies.

Risk assessment: Conduct thorough risk assessments and testing of AI systems, ensuring they perform accurately and reliably under various conditions. Appendix 2 provides a basic AI in OH risk assessment tailored to OH professionals.

Assess the tool for accuracy and reliability: Is the tool acting accurately and reliably under the conditions of use?

Bias: Consider the algorithm or AI bias, which can occur over time.

Model drift: Continuous monitoring – reporting AI compliance and AI output for limitations and errors, especially errors over time.

Regular updating: Regularly update AI systems based on new regulations and advancements.

Appeals process: Establish an appeals process so stakeholders can challenge AI-based decisions.

Balance benefit with risk: Use this evaluation of the NHS Artificial Intelligence Lab when considering benefits and risks: AILab_Evaluation_FinalReport_April25.

9. Training and Competency

Initial Training: Provide and document training and competency on effective AI use and ethical principles. Ensure all staff understand responsible AI use.

Expertise Level: Identify the skill levels required for different groups of users. (Schubert et al., 2024).

Specialised Training: Offer specialised training for AI applications in OH.

Prompt Library: Consider developing an OH prompt library.

Responsibilities: OH professionals must follow their professional codes of conduct and report any AI competence concerns to their managers.

Competency Base: Develop a core set of AI competencies for all staff which can be tailored and supplemented for specific user groups.

Regulatory Compliance: OH professionals must work within their competence and not rely on AI to supplement it.

10. AI and Regulatory Compliance

Risk assess the **health and safety implications** of using AI in OH as per the HSE guidance: HSE's regulatory approach to Artificial Intelligence (AI)

Consider whether the use of AI is **considered a product under product supply law**, which is regulated by HSE. HSE is responsible for monitoring the conformity of products against both health and safety risks: HSE's role as a market surveillance authority

Medical device regulation: Ensure the AI product has been considered for this regulation. Any product deemed to be a medical device must be registered with the UK MHRA (Medicines & Healthcare products Regulatory Agency) and the EU MDR for Europe.

Software as a medical device (SaMD): Any software that is a clinical decision-making tool, including those which don't simply transcribe, could be considered a medical device. AI as a medical device (AIaMD) is subject to regulatory oversight because it generates outputs that directly inform clinical diagnosis or treatment decisions, whereas AI used for administrative or operational support functions does not impact on clinical outcomes and therefore falls outside medical device classification.

Review the product against the guidance: see Appendix 2 for a checklist.

Change roadmap: Ensure a roadmap of change for software, including AI, is in progress so that software and AI are clear and people are protected.

The **MHRA** is reforming its approach to SaMD and AIaMD (AI as a medical device):

- AI-enabled software is regulated under UK medical device regulations, which are evolving post-Brexit.
- Classification depends on intended purpose, risk level and bias.
- Software and AI as a Medical Device Change Programme: A roadmap for reforming regulation across the product life cycle: qualification, classification, pre-market requirements and post-market surveillance.
- Emphasis is on the intended purpose statements, risk-based categorisation and bias mitigation.

11. Incident Reporting and Policy Review

Incident Documentation: Document and report any AI-related incidents. Use these reports to improve processes and AI systems.

Audit and Review: Regularly audit and review AI policies, risk assessment, use and outputs as per the organisation's management standards. Involve relevant stakeholders and OH leadership in the review process.

12. Sustainability and Environmental Impact

AI technologies, particularly those involving large-scale machine learning models, require significant computing power, which can lead to substantial energy consumption and carbon emissions. As OH professionals, it's important to consider the environmental footprint of AI tools and platforms.

Consider energy-efficient solutions – supporting providers who use renewable energy – and be mindful of the necessity and the scale of AI applications. This will reduce the environmental impact and contribute to more sustainable digital practices.

13. Further Resources

The AI in OH website, supported by iOH, the National School of Occupational Health (NSOH) and the University of Manchester, serves as a central hub for resources on AI in OH – helpful documents, details of training events, latest news, a discussion forum, and curated links to additional resources. This platform is designed to help OH professionals navigate the evolving role of AI in their field.

14. Conclusion

By following these guidelines, OH professionals can use AI safely, ethically and securely. Adhering to these principles will enhance workplace health and safety, improve OH practices and maintain trust in AI technologies.

15. References

Chantry, S. (2025).
AI usage policy for occupational health related to overall AI policy (Version 2).

Chartered Society of Physiotherapy. (2025).
Statement of principles to apply to the use of artificial intelligence (AI) in physiotherapy.

Health and Safety Executive (HSE). (n.d.).
HSE's regulatory approach to Artificial Intelligence (AI). Retrieved from
https://www.hse.gov.uk/news/hse-ai.htm

Information Commissioner's Office (ICO) (2025).
AI and data protection risk toolkit (Version 1.1). Retrieved from
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/

GOV.UK. (2020).
Data Ethics Framework.

Medicines & Healthcare products Regulatory Agency (MHRA). (2025).
Digital Mental Health Technology - Regulation and Evaluation for Safe and Effective Products.

Shemtob, L., Majeed, A., & Beaney, T. (2025).
Regulation of AI scribes in clinical practice. BMJ, 389:r1248.
https://www.bmj.com/content/389/bmj.r1248

Schubert, T., Oosterlinck, T., Stevens, R. D., Maxwell, P. H., & van der Schaar, M. (2024).
AI education for clinicians. eClinicalMedicine, 79, 102968.
https://doi.org/10.1016/j.eclinm.2024.102968

Windell, J. (2024).
EHS and AI: Handling Safety Data
https://www.ioshmagazine.com/2024/09/02/ehs-and-ai-handling-safety-data

16. Glossary of AI Terms for Health Research and Services

AI System
Any software or application using artificial intelligence capabilities.

Data Privacy
The practice of ensuring personal or sensitive data is protected from unauthorised access or disclosure.

Deepfake
Synthetic media created using AI, intense learning techniques, to manipulate images, videos or audio that convincingly imitate real-life appearances or voices. While it has legitimate applications, this technology raises concerns about its potential misuse to spread misinformation or commit fraud.

DeepSeek
A deep learning-based search engine designed to find relevant information from large datasets.

Explainability
The extent to which the internal mechanics of a machine learning model can be explained in human terms.

Generative AI
A type of artificial intelligence that can generate new content, such as text, images or music, based on the data it has been trained on.

Hallucinations
In the context of AI, hallucinations refer to instances where the AI generates content that is not based on the input data or reality.

Interoperability
The ability of systems, devices or applications to work together and exchange information seamlessly.

Machine Learning
A subset of AI that involves training algorithms to learn from and make predictions or decisions based on data.

Model Bias
A situation where a machine learning model produces results that are systematically prejudiced due to erroneous assumptions in the learning process.

Natural Language Processing (NLP)
A field of AI that focuses on the interaction between computers and humans through natural language.

Neural Networks
A series of algorithms that attempt to recognise underlying relationships in a set of data through a process that mimics the way the human brain operates.

Occupational Health Professional
Occupational health team members across the board.

Predictive Analytics
The use of data, statistical algorithms and machine learning techniques to identify the likelihood of outcomes based on historical data.

Protected Health Information (PHI)
Any identifiable health information covered under applicable privacy laws.

Reinforcement Learning
A type of machine learning where an agent learns to make decisions by taking actions in an environment to maximise the notion of cumulative reward.

Supervised Learning
A type of machine learning where the model is trained on labelled data, meaning each training example is paired with an output label.

Unsupervised Learning
A type of machine learning where the model is trained on unlabelled data and must find patterns and relationships in the data on its own.

Appendix i:
AI as a medical device checklist

Functional Assessment	
	Does the AI support or inform clinical decisions (e.g., diagnosis, treatment, risk stratification)?
	Does it summarise or interpret health data beyond simple transcription?
	Does it automate documentation that could influence care?
	Is it used to generate referrals, management plans, or clinical coding?

If you answer 'yes' to any of the above, the AI is likely to be classified as a medical device under MHRA regulations.

Regulatory Classification	
	Check if the product is registered with the MHRA (via the Public Access Registration Database).
	Determine the risk class (Class I, IIa, IIb, or III) based on functionality and impact.
	Confirm if the product has a UKCA or CE mark
Clinical Safety Compliance	
	Appoint a Clinical Safety Officer (CSO) – must be a qualified healthcare professional
	Complete DCB0129 (supplier-led safety documentation) (if applicable for the OH department, as this is a requirement under the Health and Social Care Act 2012))
	Complete DCB0160 (organisation-led clinical risk assessment) (If applicable for the OH department)
	Maintain a hazard log and clinical safety case.
	Implement a monitoring framework for ongoing safety review.
Data Protection & Privacy	
	Conduct a Data Protection Impact Assessment (DPIA).
	Update privacy notices to inform people about AI use.
	Ensure transparency during consultations (e.g. opt-out options).
	Confirm data retention policies and access controls.
Security & Technical Assurance	
	Comply with Cyber Essentials Plus and DSPT.
	Conduct CREST-approved penetration testing.
	Ensure UK-based data processing and secure storage.
Bias & Accuracy	
	Assess for bias in transcription or interpretation (e.g., accent, language).
	Ensure clinician review of AI outputs before integration into records.
	Train staff to identify and correct errors.
Training & Governance	
	Provide staff training on AI use, risks, and mitigation.
	Develop an AI policy for your Occupational Health service.
	Engage with your Data Protection Officer (DPO)

Appendix ii:
AI in OH Risk Assessment checklist

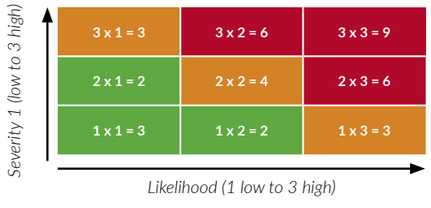
Risk definitions

Risk Level	Definition (AI Context)	Impact Level	Definition (AI Context)
High Risk	The AI tool is likely to produce errors, bias, or misuse due to poor design, lack of testing, or unclear boundaries. It may operate on sensitive data without adequate safeguards.	**High Impact**	Failure or misuse could cause serious harm—e.g. incorrect health advice, breach of medical confidentiality, reputational damage, or legal consequences.
Medium Risk	The AI tool has some vulnerabilities or uncertainties (e.g. limited explainability, moderate bias risk), but is generally well controlled and monitored.	**Medium Impact**	Issues may cause operational disruption or moderate reputational risk, but are unlikely to cause lasting harm (e.g. misclassification of non-critical data).
Low Risk	The AI tool is well-tested, transparent, and used in low-stakes contexts with strong controls and minimal exposure to sensitive data.	**Low Impact**	Minimal consequences—e.g. minor inconvenience, low-sensitivity data affected, or easily reversible errors.

Basic AI in OH Risk Assessment

Category	Checklist item	Impact *Low (1) / Medium (2) /High (3) Severity*	Probability *Low (1) / Medium (2) /High (3) Likelihood*	Risk Score *= Severity x Likelihood*	Comments	Supporting Evidence, e.g. DPIA, Vendor Assurance Statement or MHRA Registration
Data Ethics, Security & Privacy (Sections 4 & 5 of the guidance document)	Data source and quality: Ensure the data used is from a reliable source and has proper consent.					
	Privacy compliance: Follow GDPR, HIPAA or other relevant privacy regulations.					
	Data minimisation: Collect and keep only the necessary data.					
	Data protection: Use techniques to anonymise or pseudonymise personal data.					
	Access controls: Define who can access the data and under what conditions.					
	Security measures: Ensure the data is encrypted, securely stored and safely transmitted.					
Fairness & Representativeness (Section 8 of the guidance document)	Bias check: Evaluate the data and results for any demographic, geographic, economic or social biases.					
	Inclusivity: Ensure diverse groups are represented in the data and testing.					
	Fair outcomes: Make sure decisions do not unfairly harm or benefit specific groups.					
	Bias reduction: Use strategies to minimise or eliminate identified biases.					
Robustness & Reliability (Section 8 of the guidance document)	Stress testing: Check how the AI model performs under extreme or unusual conditions.					
	Error handling: Ensure the system can handle unexpected or incorrect inputs.					
	Performance monitoring: Watch for and address any decline in model performance over time.					
	Backup plans: Have backup systems or manual overrides in case of failure.					
Ethical Considerations (Sections 4 & 6 of the guidance document)	Purpose check: Ensure the AI is used for its intended and ethical purpose.					
	Privacy information and lawfulness: Identify, document and ensure valid legal grounds for the collection and use of personal data in compliance with applicable laws and regulations.					
	Meaningful human oversight: Include mechanisms for human decision-making in the process.					
	Transparency: Clearly document how the model is designed, works and makes decisions.					
	Accountability: Define roles and responsibilities for outcomes.					
	Respect for individual rights: Establish and document processes for handling individual rights requests (e.g. access, correction, objection) throughout the AI system's life cycle.					
Legal & Regulatory Compliance (Section 10 of the guidance document)	Accuracy and precision: Measure how well the model performs.					
	Explainability tools: Use tools to interpret and explain model decisions.					
	Traceability: Ensure you can trace decisions and data sources.					
	Documentation: Keep detailed records of models, datasets and system logs.					
Testing & Validation (Section 8 of the guidance document)	Pre-deployment testing: Test in simulations and sandbox environments before deployment.					
	User feedback: Collect feedback from diverse end users.					
	Ongoing validation: Continuously monitor and update the system after deployment.					
Governance & Documentation (Sections 11 & 5 of the guidance document)	Accountability: Conduct a data protection impact assessment (DPIA). View sample DPIA template.					
	Risk log: Keep a log of identified risks, their severity, and mitigation plans.					
	Regular reviews: Reassess risks and controls regularly.					
	Stakeholder involvement: Engage legal, technical, ethical and business stakeholders.					
Sustainability & Environmental Impact (Section 12 of the guidance document)	Necessity and efficiency: Determine if AI is the most appropriate and efficient solution for the task, or whether a less-resource intensive method would suffice.					
	Energy and emissions: Evaluate the energy use and carbon footprint of the AI system.					
	Green infrastructure: Check the AI is hosted on infrastructure powered by renewable energy or certified for sustainability.					
	Right-sized models: Select appropriately scaled AI models to avoid unnecessary computational and environmental costs.					
	Vendor transparency: Identify whether the provider shares clear information on sustainability practices and environmental impact.					

Risk ready-reckoner: severity x likelihood



User information

This risk assessment is designed for use alongside the accompanying guidance document. It is a basic guide and therefore the responsibility of the user to ensure it is adequate for their purposes and covers all all areas noted in the guidance document.

Authors: *Molly Healey, Janet O'Neill, Lucy Kenyon, Cameron Black, Su Chantry (iOH and the AI in OH Working Group)*

Disclaimer

This Basic Artificial Intelligence (AI) in Occupational Health (OH) Risk Assessment supports OH professionals in the safe, ethical and secure use of AI technologies. It does not constitute legal, clinical or technical advice, and users remain responsible for exercising professional judgement and complying with relevant laws, regulations and data protection standards. The Society of Occupational Medicine (SOM), The Association of Occupational Health and Wellbeing Professionals (iOH) and the AI in OH Working Group accept no liability for any outcomes resulting from the use of AI tools based on this risk assessment checklist. References to specific technologies do not imply endorsement, and users should conduct their own due diligence. This risk assessment checklist will be reviewed periodically to reflect evolving best practices and regulatory developments.

Supporting occupational health and wellbeing professionals

2 St Andrews Place, London NW1 4LB

Charity Commission No: 1184142
Scottish Charity No: SC049793
VAT No: 927 0030 57