

Key Risks Do's & Don'ts

The following table reflects the latest [CQC guidance](#) and includes further information where available.

Key Risks		Recommendations
Data Privacy & Confidentiality	Entering sensitive adult social care data into AI tools (e.g., case notes, personal details) risks unintended storage, reuse, or exposure. Do not input identifiable personal data into public AI tools, i.e., names, Date of Births, care notes). Data must be protected against unauthorised access, loss, or breaches. It is your responsibility to ensure that platforms are secure, systems that you use are approved and access is controlled.	• Use approved, organisation-controlled AI systems with clear data protections • Anonymise or Pseudonymise data before using AI anonymised or fictional examples wherever possible • Only use the minimum amount of data and data that is necessary • Implement clear staff guidance and policies on acceptable use • Provide training so staff understand what “sensitive data” includes
Legal & Compliance Risk	Potential breaches of GDPR, confidentiality duties, and safeguarding obligations if data is mishandled or leaked.	• Conduct a Data Protection Impact Assessment (DPIA) before adopting AI tools

Key Risks in AI

	Your organisation is responsible for demonstrating compliance.	• Ensure suppliers provide GDPR-compliant contracts and data processing agreements • Involve your Data Protection Officer (DPO) if you have one, alternatively your Data Security Protection Lead (DSPL) or go to person responsible for Data Security, early on. • Keep records of what AI tools are used and what data is processed i.e., include in your current Information Asset Register (IAR) and Record of Processing Activities (RoPA) • Treat AI misuse as a reportable incident where appropriate
AI Data Use & Storage	Inputs may be processed and retained externally (AI commonly store or reuse inputs), raising concerns about control, ownership, and reuse.	• Data should only be used for the specific purpose it was collected for. Using care data to “test” or “experiment” with AI may break this rule. You cannot reuse data for new purposes without proper justification • Carefully review terms of service (many free tools reuse inputs) • Restrict access through approved accounts only with no personal logins for work tasks • Maintain a register of AI tools in use
Bias & Ethics	Risk of embedded bias in AI outputs could affect decision-making for vulnerable individuals.	• Treat AI outputs as guidance, <i>not</i> decisions. • Data must be accurate and up to date.

Key Risks in AI

		• AI can generate incorrect output so you must not rely on AI outputs without checking them • Keep human oversight in all care-related decisions • Build ethical guidelines for AI use (fairness, dignity, inclusion) • Test outputs for bias – especially in risk assessments and care recommendations
Cybersecurity Exposure	Platforms handling large volumes of data become attractive targets for hackers resulting in cyber attacks	• Only use AI tools that meet cyber security standards (e.g. Cyber Essentials, DSPT-aligned) • Enforce strong passwords and multi-factor authentication (MFA) • Use secure networks only (no public Wi-Fi and include AI in Business Continuity Plans) • Keep systems and software updated
Intellectual Property Risk	AI-generated content may inadvertently breach copyright, creating legal exposure	• Avoid using AI to generate content that mimics specific copyrighted sources • Use outputs as a <i>draft</i>, then review & check content before publishing externally (policies, training materials, public-facing documents etc.) • Keep records of where AI has been used in content creation