

General Guidance on AI and Data Governance

This material is produced by the Ethics and Compliance Team at the BHBIA. It is meant as general, not specific, advice on the use of AI. The AI space is evolving rapidly and it is an AI deployer's responsibility to stay current on technical capabilities, limitations, and administrative risks.

Why this guidance is needed

Many AI tools maintain context through conversation histories, project workspaces, uploaded files and, in some cases, memory features that personalise future interactions.

This can create a reasonable concern for organisations working across multiple clients:

Could information shared while working for one client influence outputs generated for another?

The answer is similar to that applied to any consultant, researcher or analyst working across multiple engagements. Experience gained from previous work is not itself a conflict of interest. However, confidential information obtained from one client must never be disclosed, reused or relied upon inappropriately for the benefit of another.

Users therefore need to actively manage how AI tools store, organise and access information.

The Core Principle

AI should be treated as a workspace that requires the same level of information governance as any other business system.

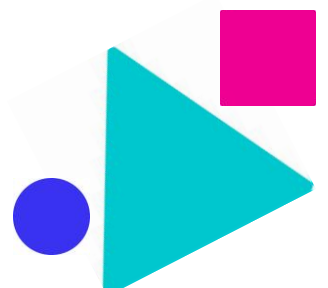
Client information should be separated wherever reasonably possible, and users should not assume that the AI tool itself will identify or enforce appropriate confidentiality boundaries.

Responsibility for maintaining those boundaries remains with the user and their organisation.

Separate Clients from the Start

Where possible:

- Use a separate conversation for each client.
- Use separate projects, folders or workspaces for different clients.
- Consider additional separation where internal client firewalls exist (for example commercial versus clinical teams).
- Clearly name conversations and projects so that information is easily identifiable.



Maintaining clear separation reduces the likelihood of inadvertently mixing information from different engagements.

Keep Client Documents Isolated

Many AI tools allow documents to be uploaded and referenced during future conversations.

To minimise risk:

- Store documents only within the relevant client workspace or project.
- Do not combine documents from multiple clients in a shared project.
- Remove files when they are no longer required in accordance with organisational retention policies.
- Ensure any uploads comply with client agreements, confidentiality obligations and information security requirements.

The simplest safeguard is often to ensure that a project contains information relating to only one client or engagement.

Be Cautious with Persistent Memory

Some AI platforms provide memory features that retain information between conversations.

Where such features exist:

- Understand whether memory is enabled and how it operates.
- Avoid storing client-specific information in persistent memory.
- Consider disabling memory for highly confidential activities.
- Use memory, where appropriate, only for personal working preferences rather than client information.

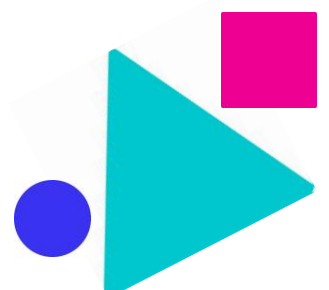
Users should understand what information may persist beyond an individual conversation and manage it accordingly.

Use Additional Protections for Sensitive Work

For particularly sensitive engagements:

- Consider temporary, private or non-persistent chat modes where available.
- Limit the amount of confidential information shared.
- Follow any client-specific restrictions regarding AI usage.
- Escalate unusual confidentiality concerns through normal governance channels.

The higher the sensitivity of the information, the higher the level of caution that should be applied.



A useful discipline is to share only the information needed to complete the task.

Where practical:

- Remove unnecessary personal data.
- Avoid sharing identifiable information unless required.
- Use generic descriptors or placeholders where appropriate.
- Limit disclosure to the minimum information necessary for the intended purpose.

Reducing the amount of information shared reduces the potential impact of any error.

Is This a Conflict of Interest Issue?

In most circumstances, the existence of AI memory or contextual awareness is not fundamentally different from an experienced professional retaining knowledge gained from previous projects.

The risk arises when confidential information from one client is disclosed, reused or influences work in a way that breaches contractual, professional or ethical obligations.

The appropriate response is therefore not to avoid AI entirely, but to apply the same standards of confidentiality, information governance and professional judgement that would be expected in any client engagement.

The BHBIA's Ethics & Compliance Committee is providing this guidance as general information for its members. It is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters. Whilst every reasonable effort is made to make sure the information is accurate, no responsibility for its accuracy or for any consequences of relying on it is assumed by the BHBIA.

Produced by the BHBIA's Ethics & Compliance Committee September 2026

British Healthcare Business Intelligence Association
Fountain Precinct, 4th Floor Orchard Lane Wing, Balm Green, Sheffield, S1 2JA
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk
A Private Limited Company Registered in England and Wales No: 9244455

Keeping you informed about changes in the UK legal ethical environment.

