

The CLINIC Guard Method™

CLINIC Guard Workbench — Free Starter Worksheet

Staff Quick Guide: What Not to Enter Into Public AI Tools

A one-page reminder your team can keep at the desk about information that should never go into a public AI tool.

Organization: _____

Date: _____

Do not enter

- Patient or client names, initials, or record numbers
- Dates of birth, addresses, phone numbers, or email addresses
- Diagnoses, medications, notes, images, or lab results tied to a person
- Insurance or payment details
- Staff personal information or credentials
- Passwords, API keys, or system logins
- Anything from a document you would not email outside the organization

Safer habits

- Remove identifying details before you paste anything in.
- Ask general questions instead of person-specific ones.
- Use only the tools your organization has approved.
- Treat every answer as a draft: verify facts before you use them.
- A person, not the tool, makes the final call on anything clinical or sensitive.

If something goes in by mistake

- Tell the named owner of the tool right away.
- Write down what happened and when.
- Do not try to fix it quietly on your own.

Questions or concerns _____

This guide is educational. It is not legal, clinical, HIPAA, cybersecurity, or compliance-certification advice. Consult qualified professionals for guidance specific to your organization.