Best Practice

Sorting, not banning: Triage card

The five-minute triage card. Use it for any new tool before it goes live.

Step 1. Ask three questions

1. Do we know what patient information it touches, and where and how it is stored, processed and deleted?

Ask each of these separately. One answer never covers the others.

- ☐ **Patient Information.** Does the solution need to access patient information to work? Can we configure it so it doesn't access patient information?
- ☐ **Data storage.** Where is the data stored? Where is each database located?
- ☐ **Data processing.** Where is it processed?
- ☐ **Sent elsewhere.** Is it encrypted in transit and at rest?
- ☐ **Data Encryption.** Does it get sent anywhere else? Think model providers, training databases and sub-processors.
- ☐ **Copies and deletion.** Can we get a copy of the data held by the vendor? Can we have our data permanently deleted upon request?sub-processors.

2. Do we know, in writing, whether the vendor uses our data for AI training, and is there a clear breach process in both directions?

- ☐ **What is your position on using our data for training? Get this in writing.**
- ☐ **How do we get notified in the event of a data breach?**
- ☐ **Who do we call if we have a problem with our account or notice suspicious activity?**

3. Does a clinician review and own every output before it is used?

If it writes a note, letter or summary, a named clinician must be able to review it and be accountable for it.

Step 2. Sort it and write it down

Yes to all three	Any no, or not sure
Add it to the **approved register.** Record the answers and the conditions of use. Done.	Add it to the **requires IT input** register. Not banned. It waits for the right skills to look before anyone relies on it.

Either way, it goes on a register before it goes live. Not stated counts as no until the vendor tells you otherwise in writing. Ask for answers in writing.

This is a method, not legal advice. Check the rules that apply to your practice, including the Privacy Act, My Health Record, and the RACGP Standards.

Best Practice

One-page tool register

One row per tool. Start with whatever you can list today. A register with eight tools beats a perfect one next year. Each tool has one named owner, not a team.

Tool and vendor	Used for	Roles that can use it	Owner (one name)	Triage Q1 Q2 Q3 (Y/N)	Data Stored where (City, Country)	Processed where (City, Country)	Encrypted (transit & at rest)	Data Sent elsewhere?	Exit rights (copy / delete)	Status	Conditions of use	Dates (Approved)	Date (Next Review)

Status is one of approved, requires IT input, or not approved. Conditions of use are, for example, 'clinician reviews every output'.

Keep on file. One folder per tool

- ☐ Completed triage record
- ☐ Vendor privacy policy, terms, and written breach and no-training commitments
- ☐ Evidence of encryption and data location
- ☐ How to export and permanently delete our data, with the vendor's confirmation
- ☐ Approval decision, who made it and when
- ☐ IT review outcome for anything marked requires IT input
- ☐ Staff guidance and who to call if something goes wrong