FREE RESOURCE · FOR HEALTHCARE STAFF

The De-Identification Checklist

A practical way to spot patient information that must stay out of AI tools your organization has not authorized — especially when you are busy and the shortcut is tempting.

> **Removing a name is not de-identification.** Many other details — and combinations of ordinary details — can identify a patient.
>
> **This checklist does not certify HIPAA compliance** and does not make any tool approved. Your organization's policy, its approved tools and its privacy, security and compliance staff decide.

Step 0 — Before you start

Is this AI tool authorized by your organization for patient information? If yes, follow its rules. If no, the safest default is simple: **no patient information goes in at all.** Use the checklist below to recognize what that includes.

Two kinds of rule

What HIPAA says. HIPAA's Safe Harbor method (45 CFR 164.514(b)) lists 18 identifier types that must be removed, plus a condition that you have no actual knowledge the rest could identify the person. Expert Determination is the other method. Your organization, not this page, decides when information is de-identified.

Cautious workplace practice. Everything else on this page is a careful habit for busy moments. It is not a legal test, and your organization's rules come first.

1 · HIPAA Safe Harbor identifier types

These apply to the patient — and to the patient's relatives, employers and household members.

- [ ] Names
- [ ] Geographic details smaller than a state: street, city, county, ZIP code
- [ ] All parts of dates tied to the person except the year — birth, admission, discharge, death; and ages over 89
- [ ] Phone numbers
- [ ] Fax numbers
- [ ] Email addresses
- [ ] Social Security numbers
- [ ] Medical record numbers
- [ ] Health plan beneficiary numbers
- [ ] Account numbers
- [ ] Certificate or license numbers
- [ ] Vehicle identifiers and serial numbers, including plates
- [ ] Device identifiers and serial numbers
- [ ] Web addresses (URLs)
- [ ] IP addresses
- [ ] Biometric identifiers, such as finger and voice prints
- [ ] Full-face photos and comparable images
- [ ] Any other unique identifying number, characteristic or code

Also keep out — workplace precaution

- Room or bed numbers, wristband details, appointment or order numbers.
- Names of staff caring for the patient, if they could point back to them.

2 · Identifying combinations

No single detail is a name, but together they point to one person.

- A rare condition plus a small town plus an age range.
- An unusual job — "the high school's only chemistry teacher."
- A date of an event that made the news — an accident, a fire, a birth.
- Family details — "her twin sister works in our lab."

3 · Free text

Notes, messages and summaries hide identifiers in ordinary sentences. Read every line before anything leaves the record.

- Relatives' and visitors' names, and who they are.
- Places — "lives above the bakery on Main."
- Quotes that sound like the patient.
- Copied headers and signatures at the top or bottom.

4 · Dates

- Any part of a date tied to the patient, other than the year, can identify them.
- Relative timing can too: "two days after the hurricane."
- Very old ages are uncommon enough to point to a person.

5 · Images

- Faces, tattoos, birthmarks, distinctive jewelry.
- Wristbands, labels and charts in the frame.
- Screens, whiteboards or paperwork in the background.
- Text burned into scans and x-rays.

6 · Metadata

- File names: "Smith_J_MRI_0412.pdf."
- Document properties: author, comments, tracked changes.
- Photo data: location, date and device.
- Screenshots that show browser tabs, the record header or other patients.

7 · Unusual cases — stop and consult

- Well-known patients, or anyone who has been in the news.
- A colleague, their family, or someone you know.
- Small populations, rare diseases, rare procedures.
- Children, behavioral health, substance use, reproductive or genetic information.
- Anything that makes you hesitate.

A synthetic example

Everything below is invented. No real patient is described.

BEFORE — KEEP OUT	WHY IT IDENTIFIES
“Maria Alvarez, 47, Room 312, admitted 3/14 after the Route 9 bus crash.”	Name, room number, admission date and a news event.
“Retired fire chief from Millbrook with a rare liver condition.”	Unusual role, small town and rare condition together.
A photo of a wound showing a tattoo and a hospital wristband.	Distinctive mark and label in the frame.

Even after removing all of these, whether information is de-identified under HIPAA is decided by your organization using HIPAA’s methods — not at the keyboard.

Stop and consult

> **When in doubt, don’t type it.** Ask your privacy officer, information security team or compliance office before using any patient-related information in an AI tool — and report it promptly if something has already been entered where it shouldn’t have been.

Privacy officer · how to reach them

Information security · how to reach them

Approved AI tools at my organization

General education only — not legal advice and not a compliance certification. Sources: HHS guidance and 45 CFR 164.514, in the References Companion · calmgrindco.com · info@calmgrindco.com