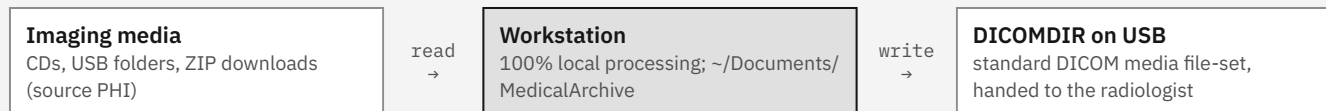


# Security One-Pager

| DOCUMENT           | VERSION | DATE       | LANGUAGE                           | PAGES |
|--------------------|---------|------------|------------------------------------|-------|
| Security One-Pager | 1.0     | 2026-10-20 | English (United States, Singapore) | 1     |

For compliance and information-security review. MIA Toolkit is a free, open-source (MIT) **offline** desktop application that consolidates a patient's imaging media (CDs, USB folders, ZIP downloads) into one DICOMDIR archive (the standard DICOM media file-set) on a USB drive.

## Data flow



No server · No PHI egress · No telemetry · Only network call: the user-clicked update check (version.json)

## Architecture

- **100% local processing.** All work happens on the workstation. Imaging media is read from source media, processed locally, and written to local disk and a destination USB drive.
- **No server component.** There is no MIA Toolkit backend, API, or cloud service. The vendor operates no servers that receive application data.
- **No PHI egress.** Patient health information never leaves the workstation or the USB drive the user writes to. The vendor never sees, receives, or stores PHI.
- **No telemetry, no analytics, no account.** The app's only network call is the user-initiated **Check for Updates**: a single HTTPS GET of a static file (<https://miatools.tech/version.json>), made only when a user clicks it, with a generic versionless User-Agent, no query parameters and no identifiers. Nothing is sent in the background, ever, and the app never downloads or installs anything itself. It works fully on an air-gapped machine (the update check then simply reports that it couldn't check).

## Open source (auditable)

The software is licensed under the **MIT License** and the full source is public and reviewable at <https://github.com/Fritanga-Collective/mia-toolkit> (linked from <https://miatools.tech>). Your security team can inspect exactly what the application does; the update check lives in `mia/gui/updates.py`.

## Code signing status

- **macOS:** signed with an Apple **Developer ID** certificate and **notarized** by Apple (stapled) since v0.1.5. Verify with `spectl --assess --type execute -vv "MIA Toolkit.app"`.
- **Windows: not yet signed.** The installer is unsigned, so SmartScreen may show "Unknown publisher" (choose More info → Run anyway). An Authenticode code-signing certificate (Certum Open Source Code Signing) is planned; this line will be updated when signed installers ship.
- **Checksums:** each release's SHA-256 per installer is published in <https://miatools.tech/version.json>.

Verify signature status and checksum on the build you deploy before rollout.

## Privacy and regulatory framing

- **Privacy policy:** <https://miatools.tech> (Privacy Policy) — the app is built so the vendor *cannot* see your data: offline, no account, no telemetry, no cookies or tracking in the app.
- **Local processing under your controls:** MIA Toolkit processes PHI **locally, under the institution's existing controls** (endpoint security, access control, USB policy, physical security). Because the vendor never touches PHI and operates no servers, there is no third-party data-processing relationship to assess for the application's data handling — PHI stays within the institution's own environment. This document does not constitute legal or compliance advice; confirm against your jurisdiction's requirements.
- **Intended purpose (all markets):** MIA Toolkit is a file-management tool: it copies, organizes and converts DICOM studies from CDs into a DICOMDIR archive on USB. It does not interpret or measure images, and it does not replace a PACS or a diagnostic workstation.

## BY MARKET

### United States

**Not a medical device:** software solely to transfer, store, convert or display images (FDA MDDS/MISD/MICD guidance, Sept 2022; FD&C §520(o)(1)(D)); never interprets. **No BAA needed:** vendor never receives or accesses PHI (HHS HIPAA FAQ 256); support takes de-identified material only.

### Singapore

PDPA: the app collects and transmits nothing. HSA GL-04-R4 (Dec 2025): store/convert/transfer software is not a medical device.

## Support and patient data

We never need patient data. Send de-identified screenshots or logs only — never studies, DICOM files or PHI. Support is best-effort by email at [support@miatools.tech](mailto:support@miatools.tech), with a target first response within **2 business days**.

## Responsible disclosure

Report suspected security issues privately to [support@miatools.tech](mailto:support@miatools.tech) (or via GitHub private vulnerability reporting on the repository; policy in `SECURITY.md`). Please include the affected version, OS and steps to reproduce, and never include real PHI in reports.