HITAP
Health Intervention and Technology Assessment Program
FOUNDATION

AI Standard Practices

Purpose and Scope

Purpose

Provide clear practices for the use of Artificial Intelligence (AI) in HITAP's work, ensuring that AI is used appropriately, securely, responsibly, and in line with the HITAP AI Policy.

Scope

Applies to HITAP personnel, interns, research assistants, consultants, contractors, and collaborating researchers who use AI in HITAP-related work or have access to HITAP data or outputs, whether using personal or organizational devices and accounts.

The Standard Practices may be updated more frequently than the AI Policy to keep pace with developments in AI

Roles and Responsibilities

The AI Policy assigns joint responsibility to the Information Technology (IT) team, Administration Unit, and management team for overseeing AI use and developing and reviewing the AI Standard Practices to ensure alignment with the policy.

Before Recording	**Inform participants that the meeting will be recorded and AI will be used, including the purpose, who will have access, and the data retention period. Obtain authorization or consent as required.**
Choose the Tool and Account	Use only tools and accounts authorized by HITAP for the data level involved in the meeting, and seek approval when confidential data is involved.
Check the Data before Uploading	Do not enter prohibited data into AI. If the audio file contains such data, remove that segment before uploading. Deleting data from the transcript afterward does not count as masking it before submission.
Review the Output	Check speaker names, figures, decisions, and assigned tasks before using the transcript or meeting summary.
Unit/Team Representatives	Provide use cases · Workflows · Risk points · Quality criteria · Practical examples
HITAPer	Follow the Standard Practices · Review AI outputs · Report incidents



Central Standard + Unit Practice - Apply the organisation-wide standards alongside unit-specific practices to support practical implementation suited to each unit's work, under a shared organisational AI Policy

From AI Policy to AI Standard Practices

AI Policy

Sets the framework and principles

- Ethical, transparent & fair use
- Accountability & ownership
- Accuracy & reliability
- Data protection & confidentiality
- Research & academic activities
- Incident reporting & governance

AI Standard Practices

- Turns the Policy into practical guidance for day-to-day work
- What AI can be used for
- What data is prohibited or requires approval
- What must be checked before using AI outputs
- When AI use must be disclosed
- Who approves or provides guidance
- Where to report AI-related incidents

Unit Practice

- Adds work-specific context
- Use cases relevant to each team
- Workflows & control points
- Commonly used data & documents
- Examples of safe prompts
- Work-specific risks
- Quality & review criteria

Policy = What / Why → Standard Practice = How → Unit Practice = How for my work

Standard Practices Structure

Framework & Roles
Purpose & Scope
Roles & responsibilities
From Policy to Practice

Core Principles
7 principles and checks before using AI

AI Use Across Work Functions
General & operational activities · Research & academic activities

AI Risk Levels
4 AI risk levels and a decision tree for guidance

Data & Confidentiality
What data can/cannot be used · Data classification · Data Masking/Anonymization

Recommended AI Tools
AI Types and Example Uses
Privacy and Security Settings

Quality & Transparency
Human review
AI disclosure
Prompting

Incident & Support
Report any AI-related incidents or concerns as soon as they are identified

Core Principles & Pre-Use Checks

7 principles from the AI Policy that apply to everyone, with key questions to ask before using AI.(Principle 7 is on the next page)

1. Use AI as a Support Tool
AI supports research, analysis, summarisation, translation, and drafting.

Pre-use check: Is it being used only to support the organisation's mission, with a clear purpose?

2. Use Organisation-Recommended Tools
Choose tools and plans that match the data classification level.

Pre-use check:
Are this tool and account recommended?

3. Protect Confidentiality and Personal Data
Do not enter confidential, personal, or sensitive data into unauthorised AI tools.

Pre-use check:
What classification level is the data, and can it be reduced or de-identified?

4. Check Before Use; Humans Remain Accountable
The user is responsible for the output, decisions, and resulting impacts.

Pre-use check:
Who will review the output before it is used?

5. Be Transparent and Respect Intellectual Property
Do not present AI-generated work as entirely your own.

Pre-use check:
Must AI use be disclosed under the policy, funder, or journal requirements?

6. Report Risks Promptly
Report incidents or concerns as soon as they are identified.

Pre-use check:
Do you know the reporting channel?
Notify your head of unit and cc IT.

Stop and consult before use when:
• Personal, confidential, or sensitive data is involved • The output will inform an important decision • Funder requirements are unclear •
• The tool is not recommended •

7. Ownership and Copyright

Practices

- Work created by personnel using organisational AI accounts in the course of their duties shall be treated as HITAP's work, with copyright held by HITAP under a written agreement.
- Organisational AI accounts must not be used for personal work, external freelance work, or activities unrelated to HITAP's mission.
- When employment or a project ends, all work-related conversations, files, and prompts must be handed over to the relevant unit before the organisation closes the account.
- Outputs generated entirely by AI without human creative input may not qualify for copyright protection. Substantial human rewriting and editing are therefore required before such outputs are used as organisational work.
- Before publication, check that outputs do not reproduce others' work without attribution, as AI may generate text closely resembling existing material.
- Agreements or Terms of Reference (TOR) for non-employees, including interns, consultants, contractors, and collaborating researchers, must include provisions assigning rights in work created using organisational AI accounts to HITAP.

Legal Basis

Copyright Act B.E. 2537 (1994)

- Section 9: Copyright in work created by an employee belongs to the employee unless otherwise agreed in writing. The employer is entitled to communicate the work to the public in accordance with the purpose of the employment.
- Section 10: Copyright in commissioned work belongs to the commissioning party unless otherwise agreed.
- Accordingly, copyright in work created by employees does not automatically belong to the organisation without a written agreement.

AI Use Across Work Functions

Type of Work	What to Check
Conversations and information searches	Factual accuracy, currency, relevance, and sources
Drafting letters and emails	Names, dates, times, figures, substance, and completeness; language, format, and formality appropriate to the recipient
Translation and language editing	Preservation of the original meaning, technical terminology, job titles, and strength of conclusions
Transcription and meeting summaries	Consent before recording; accuracy of meeting decisions
Creating media and presentations	Accuracy and clarity; content must not mislead the audience

Type of Work	What to Check
Research and literature reviews	Read original sources, verify references, and check that no key points have been omitted
Data Analysis and Coding	Test with synthetic data first. Check the logic, assumptions, and calculations against reliable methods.
AI Agents and System Integrations	Use only approved connections, limit permissions, and require human confirmation before sending, deleting, or modifying important data.

Type of Work	What to Check
Creating and editing images	Rights to source materials; permission to use a person's likeness within the agreed scope; accuracy, appropriateness, and bias. Do not present generated or altered images as authentic evidence. Check output quality and disclose AI use as required.
Creating animations and videos	
Creating synthetic speech and music	Rights to source audio and music; consent for voice imitation; accuracy, quality, and appropriateness. Ensure the content is not misleading and disclose AI use as required

Using AI with Research Data

Before entering research data into an AI tool, check all four areas.

1 Research Protocol

Confirm that the approved research protocol covers the intended purpose, methods, and types of data to be entered into AI.

2 Informed Consent

Use data only within the scope of the informed consent provided by research participants.

3 Ethics Approval

Check the conditions approved by the Institutional Review Board or Ethics Committee (IRB/EC), including restrictions on data use and disclosure.

4 Agreements and Organisational Requirements

Comply with data-sharing or data-use agreements, the data owner's requirements, and HITAP's AI guidelines.

Once all four checks are satisfied → Use data within the approved scope, document AI use, and review outputs before use.

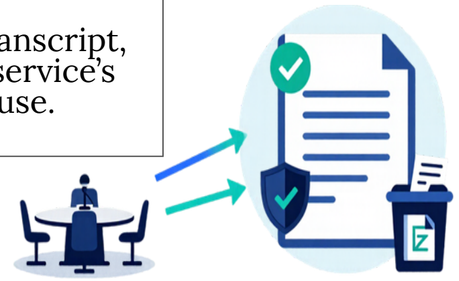
If any requirement is unmet or unclear:



Do not enter the data into AI. Consult the relevant team, your head of unit, or management team before proceeding.

Meeting Transcription

Before Recording	Inform participants that the meeting will be recorded and AI will be used, including the purpose, who will have access, and the data retention period. Obtain authorization or consent as required.
Choose the Tool and Account	Use only tools and accounts authorized by HITAP for the data level involved in the meeting, and seek approval when confidential data is involved.
Check the Data before Uploading	Do not enter prohibited data into AI. If the audio file contains such data, remove that segment before uploading. Deleting data from the transcript afterward does not count as masking it before submission.
Review the Output	Check speaker names, figures, decisions, and assigned tasks before using the transcript or meeting summary.
File Storage	After transcription is complete, download the transcript and store it on SharePoint or a computer, restricting access to relevant personnel and setting an appropriate retention period.
Delete Files from AI	Once the files have been stored and transcription is complete, delete the audio file, transcript, and summary from the AI service, including the trash or recycle bin according to the service's procedures. For shared team or department accounts, delete them immediately after use.



AI Risks

Example Uses and Tools	What Could Go Wrong?
1 **General Conversational Assistants** ChatGPT - Claude - Gemini	AI-invented figures or facts may enter reports. Text pasted into prompts may be outside our control when using a personal account.
2 **Search and Information Synthesis** NotebookL.M - Perplexity - Elicit	Citations may be fabricated, or real citations may not support the claim.
3 **Data Analysis and Code** Code Interpreter - GitHub Copilot	Code may run successfully while producing incorrect numbers without an obvious error. An entire file containing personal data may be uploaded acidentally for analysis.
4 **Transcription and Meeting Summaries** Teams - Zoom - Otter - Whisper	Meetings may be recorded without everyone's consent. Unpublished information may be stored on an external service.
5 **Translation and Language Refinement** DeepL. - Grammar - Gemini	HTA terminology and government job titles may be mistranslated. AI may change the strength or meaning of a conclusion without the user noticing.
6 **Image, Media, and Slide Creation** Canva - Gamma - Image Generators	The output may resemble copyrighted work, or commercial rights may not cover the intended use. Images resembling real people may be created without consent.
7 **AI Agents / System Integration** Agents with access to email, files, or calendars	An agent may open files or send emails without step-by-step human confirmation. Connecting to organizational systems may unintentionally pull data across projects.

Not recommended (red lines)

Research and academia

✗ Do not let AI screen the literature alone. Studies suggest it may miss around 1 in 5 eligible studies.
✗ Do not use AI-generated citations without checking the original source.
✗ Do not let AI interpret results or summarise findings on behalf of the researcher.
✗ Do not list AI as an author or conceal its use.

Systems and decision-making

✗ Do not activate an AI note-taker before obtaining everyone's consent.
✗ Do not install AI extensions outside approved accounts.
✗ Do not connect AI to organisational email or files without approval.
✗ Do not let AI make decisions about people or money.

Mitigate these risks with 3 practices: Choose HTAP-recommended tools - Do not enter sensitive data - Always verify before use

AI Risk Levels

AI Risk Level

The more sensitive the data, the greater the potential impact, or the more important the decision, the stronger the approval and review required.

Low Risk

Routine AI-assisted tasks using public or authorized information, with no significant impact on individuals, the organization, or important decisions.

Examples: Brainstorming, language editing, drafting emails, document summaries, creating PPTs

Practice: Use HITAP-recommended AI tools + review outputs before use + human review is always required

Moderate Risk

AI outputs may affect work quality or communication, but a responsible person reviews, corrects, and makes the final decision before use.

Examples: Analysing non-sensitive internal information, summarising reports, assisting with presentations

Practice: Verify data and context + identify any limitations where appropriate + human review

High Risk

AI use that may significantly affect rights, privacy, safety, research or organizational credibility, or important decisions, requiring stronger controls and human oversight.

Examples: Research data analysis, interpretation of findings, content supporting important decisions

Practice: Use only HITAP-recommended AI tools + systematic verification + consult the responsible person/Head of Unit as appropriate

Prohibited

AI use that violates the AI Policy, applicable laws, or ethical requirements.

Examples: Uploading confidential, personal, or sensitive data to unauthorized AI tools; creating intentionally false or misleading information; infringing rights or applicable requirements; automated decisions affecting individual rights without human review

Practice: Do not proceed. Report any incident or concern through the appropriate organizational channel.

Data & Confidentiality

Data & Confidentiality: Which Data Can and Cannot Be Entered into AI

Each data classification informs the risk assessment and decision tree. Identifying the data classification helps determine the required safeguards and approval steps.

Level 1
Public data

Low Risk

Generally allowed

Published reports · Public communications · Published materials

May be used with AI. Review outputs before use.

Level 2
Internal Only Data

Moderate Risk

Use only with HITAP-recommended tools

General drafts · Internal meeting notes · Internal manuals/guidelines · Work plans
Contains no personal data or confidential information.

Use only AI tools recommended by HITAP

Level 3
Confidential Data

High Risk

Prior approval required

Unpublished research data · Budgets · Personnel information · General personal data · MOUs/NDAs containing confidential information

Prior approval is required before entering the data. Use only enterprise AI tools (Enterprise GenAI) recommended by HITAP.

Level 4
Restricted data

Prohibited

Do not use with AI

Identifiable health data · Genetic data · Biological data · Racial origin · Religion · Other sensitive data that can identify individuals directly or indirectly · Passwords and API keys · Data that the data owner or IRB/EC prohibits from being entered into AI

Note: If a data/file contains multiple data classifications, apply the requirements of the highest classification

Examples of data classification

Level 1: Public Data

- Organisational information: Content on websites and social media, partner and joint project information, including HITAP and GEAR projects
- Finance and accounting: Published financial statements, income and expenditure, and financial, accounting, and tax rules issued by government agencies
- Procurement and HR: Procurement announcements, job postings, and publicly disclosed benefits information
- Funding and research guidance: Funding announcements, research topics, manuals, and publicly released evaluation results
- Publicly authorised policy briefs, infographics, posters, and presentation slides

- Open-access academic articles and published research reports
- Abstracts, bibliographic information, and article metadata made publicly available
- Open datasets without personal or sensitive information that can be linked to individuals, including data dictionaries and sample data released for use by their owners
- Published aggregated health data and statistics, such as population statistics, number of service recipients, disease rates, and health indicators, where individuals cannot be identified
- Code and models made publicly available and licensed for use under stated conditions

Considerations Before Using Data with AI:

- Being accessible or downloadable does not always mean data may be used with AI. Check usage rights and the source's terms, especially for articles accessed through an organisation's subscription.
- Use only published versions. Do not attach internal comments, personal notes, unpublished analyses, or data from additional projects.
- Public data containing personal information must be assessed under personal-data criteria; it is not Tier 1 simply because it can be found on the internet.
- Even for Tier 1 data, verify accuracy, sources, and the suitability of AI-generated outputs before use.
- Free AI accounts: Turn off the use of your data for AI model training.

Level 2: Internal-Only Data

- Internal regulations, operating manuals, blank forms, draft correspondence, and work schedules
- General meeting agendas and minutes, follow-up task lists, activity plans, and internal draft slides
- Project submission procedures, report templates, draft workplans, and ToR sections without confidential details
- Reimbursement procedures, blank forms, document checklists, account-closing calendars, and budget templates without real data
- Employee manuals, training plans, orientation materials, and blank evaluation forms

- General research-operation manuals, work schedules, manuscript-preparation guides, blank peer-review forms, and pre-submission checklists
- Media-production plans, publicity templates, and draft knowledge-sharing materials using public data or published work

Considerations Before Using Data with AI

- Use only AI tools recommended by HITAP

Level 3: Confidential Data

- Confidential meeting minutes, undisclosed strategic plans, draft project proposals, draft contracts, and details of negotiations with partners
- Unpublished budgets and financial reports, cash flow, transaction details, and disbursement documents containing payee names or account numbers
- Quotations with specific terms, price comparison results, bidder evaluation scores, and undisclosed negotiation information
- Job applicant records, employment contracts, salaries, and performance evaluations
- Information or documents subject to confidentiality obligations or usage restrictions
- Individual personnel data, salaries, performance evaluations, and applicant information
- Files containing comments or Track Changes: review and remove information that should not be disclosed, including original text retained in the revision history
- Confidential MOU, NDA, DSA, and budget documents, provided that their use does not conflict with the requirements of the contracting parties or data owners

- Research-related information
- Our own unpublished manuscripts, subject to journal or funder requirements. If Level 4 data is included, apply the Level 4 requirements
- Research participant names and contact information
- De-identified datasets that have not yet been made publicly available
- Draft policy proposals, research findings pending publication, and confidential partner feedback

Considerations before entering data into AI

- Prior approval is required. Use only enterprise-grade AI tools (Enterprise GenAI) recommended by HITAP

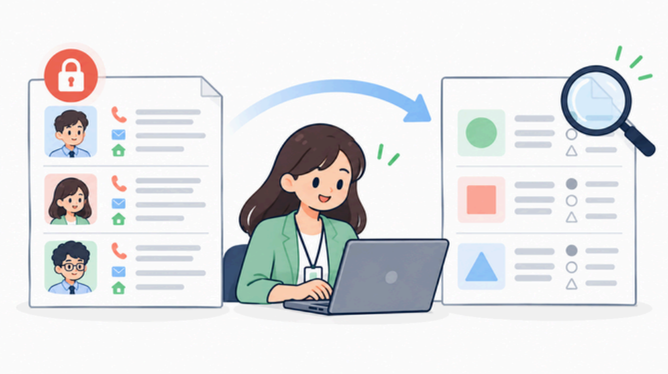
Level 4: Restricted Data

- Personal data or research participant data that directly identifies an individual or can be linked back to them
- Identity information at risk of impersonation, national ID numbers, passport numbers, and copies of identity documents
- Race, religion, political opinions, sexual behaviour, and criminal records that can be linked to an individual
- Online banking passwords, PINs, OTPs, and authentication information for transactions
- Medical certificates, health records, disability information, criminal records, and fingerprints or facial data used for identity verification
- Supporting documents containing identifiable health or sensitive information
- Highly sensitive data subject to legal, ethical, or contractual restrictions

- Identifiable health data
- Questionnaires or interviews containing identifiable health or sensitive information
- Case studies or interviews that disclose identifiable sensitive information
- Individual medical records and genetic data that can be linked to an individual
- Passwords or keys used to access databases
- Data that the data owner or Research Ethics Committee (IRB/EC) prohibits from disclosure and/or entering into AI
- Manuscripts under Peer Review: must never be entered into AI in any circumstance, to preserve the confidentiality of the peer-review process
- Restricted-access articles

What should you do if the task involves data that must not be entered into AI?

1. Choose the Tasks Where AI Can Help
   - Consider what you want AI to help with, and use only the information necessary for that task. Do not send the entire document.
2. Prepare the Data before Entering It into AI
   - Delete, mask, remove, or replace prohibited data (Data Masking/Anonymization)
   - Remove unnecessary data, mask or replace identifying information, and reduce details that could be used to identify a person, such as [Person A] and [Organization B].
   - Check the file before sending it, including Comments, Track Changes, and hidden sheets.
3. Have Someone Else Review It
   - Ask a team member or supervisor who is authorized to access the data to check that no prohibited data remains, especially in complex datasets.
4. Reassess the data after preparing the data/file, and verify that the tool, account, and purpose of use comply with the requirements before entering it into AI.
   - Once all requirements are met, no approval request is needed.
5. If it is still necessary to use restricted data, consult and seek approval from the head of unit for guidance, together with IT team.



Data Masking/Anonymization: Masking and Replacing Data before Entering It into AI

Mask or remove real data that should not be disclosed, and replace it with text or fictional values. Retain only the details necessary for the task.

1. Original Data

Start with the actual file stored in the organization's system.

→

2. Replace with Codes

Change names, numbers, and identifying information into placeholders.

→

3. Let AI Work from the Context

AI analyzes the structure and reasoning without needing to know who anyone is.

→

4. Reinsert the Real Data

The person responsible for the task puts the real values back into the output in the organization's file.

Do Not Enter Data This Way:
Risk of Violating the PDPA and Confidentiality

"Summarize the medical history of Mr. Somchai, national ID number 1-xxxx-xxxxx-xx-x, who is HIV-positive and has an outstanding balance of THB 45,000 at Hospital A."

This contains a real name, national ID number, sensitive health information, and the name of an organization.

Text after Data Masking

"Summarize the case of [Patient-A], in the [Chronic Disease-01] group, with an outstanding balance of [Amount-X] baht. What management approach should be taken?"

AI can still provide an equally relevant answer because it needs the structure of the problem, not the patient's identity.

Store the table linking replacement codes to real identities in a separate file on the organisation's system, with access restricted to authorised personnel. Never upload or paste it into AI.

Full name
→ [Patient-A] · [Respondent-1]

National ID number
→ Delete it; do not replace it

Date of birth
→ Age range, e.g., 45–49 years

Disease or health condition
→ [Disease Group-01]

Amount of money and budget
→ [Amount-X] or a percentage

Organization and healthcare facility name
→ [Organization-1]

Data Masking/Anonymization: Masking and Replacing Data before Entering It into AI

After masking, check the risk of re-identification 

Details that could identify someone indirectly

- Check age, sex, occupation, location, service dates, and specific events. Combined, these details may reveal someone's identity.

Individuals or groups with distinctive characteristics

- Take care with rare diseases, publicly reported events, or small groups. Even without names, the data may identify individuals or reveal sensitive information about them.

Reduce detail to what the task requires

- Use age ranges, replace village names with provinces, use less precise dates, or remove high-risk records.

Reassess risk after modifying the data

- Check whether individuals could still be identified and whether the modified data remain suitable for the intended task.

Have another person review the data

- Ask an authorised colleague, principal investigator (PI), or head of unit to help assess the remaining risks.

Data Masking/Anonymization: Masking and Replacing Data before Entering It into AI

Even after replacing names with codes, a person may still be identifiable.

- Even if a name is changed to “Participant A,” other details may reveal the person’s identity, such as “a 47-year-old woman who is the only school director in the subdistrict and received treatment on a specified date.” People with relevant knowledge or other information may be able to link the details back to her.
- Do not send the code-to-identity mapping table to AI. If the table showing “who Participant A is” is also sent to AI, replacing names does not protect identity. Keep the mapping table separate and restrict access.

Therefore

- Create a new file containing only the necessary data. Do not use the original file with hidden columns or a hidden sheet containing the mapping table.
- Remove details that could be linked to an individual, such as the school name, specific position, detailed address, and service date, if they are not necessary for the task.
- Store the mapping table separately from the file to be sent, in an organization-controlled area with access limited to relevant personnel. Do not attach it, copy it into the conversation, or connect AI to that area.



Data Masking/Anonymization: Masking and Replacing Data before Entering It into AI

Covering text with a coloured box or hiding rows in a table is not the same as deleting the data.
Covering or hiding content only conceals it from view. The original data may still remain in the file, for example:

- Word or PDF: placing a black rectangle over a name may leave the text underneath selectable, copyable, or extractable.
- Excel: hidden rows, columns, or sheets can be unhidden by the recipient, and software may still read the hidden data.

Therefore

- Delete the data from the copy that will actually be sent, or use permanent redaction that removes the original content, then check the file again. For tables, create a new file containing only data permitted for entry into AI.
- Create a new document containing only the necessary content, delete or replace prohibited data, and have an assistant review it before entering it into AI. If you cannot prepare the file with confidence, consult IT.



Approval Process for Using Data with AI Within HITAP

Use this process when entering Level 3 data into AI or using an AI tool outside the recommended list. Every step must be documented in writing so it can be reviewed later who approved what and when.

When is approval required to use AI?

No approval is required for each use

- Level 1 data, with human review at all times
- Level 2 data, using only the tools and accounts recommended by HITAP

Prior approval is always required

- Using Level 3 data with AI (confidential data)
- Using Level 2 data (internal data) with an AI tool not recommended by HITAP
- Connecting AI to email, file storage, or organizational systems
- Using AI to assess, rank, or make recommendations for decisions affecting individual rights, employment, or financial approvals

Approval cannot be granted: do not enter into AI

- Level 4 data
- Data or documents subject to requirements prohibiting their use with AI

How to submit a request

- Channel: Email the Head of Unit and copy IT team.
- Subject: [Request to Use Data with AI] Name of task or project
- Request details: Specify what data will be entered into AI, its data level, the purpose, why the data is necessary, the tool, account type, users, output reviewers, and the required period of use.
- Supporting information: Describe the nature and fields of the data to be used. Do not attach the complete original data file.
- While awaiting a decision: Do not enter the requested data into AI until written approval has been received.
- Evidence: Keep the approval email, including its scope and conditions, for reference.

Approval Process for Using Data with AI Within HITAP

1 **User - Prepare a complete request before submitting**

- Follow the Decision Tree on page 3 and clearly identify the data tier according to page 9.
- Reduce data detail as much as the task allows: anonymize / redact.
- State all required details: purpose; what data and which tier, which tool;
- who will review the output; and how long it will be used.

2 **Head of Unit - Screen necessity**

- Is real data necessary, or can reduced-detail data be used instead?
- Is the use within the research project, I&R requirements, and any MOU / NDA / DSA?
- If approved, forward to IT. If not approved, return the request with written reasons.

3 **IT Team - Check the tool and settings**

- Is the tool on the approved list? Is an organizational or personal account being used?
- Has data use for training been disabled, and how long does the system retain data?
- Check the provider's terms, data location, and user access permissions.

4 **Head of Unit with IT -** Review and approve

- Three possible outcomes: approved, approved with conditions; or not approved, with reasons.
- Clearly define the scope: which dataset, which tool, and the permitted end date.
- Notify the requester in writing and record the decision in the approval register.

5 **After approval - Use, review, and revoke access**

- Use only within the approved scope, with Human Review every time
- Changing the tool, dataset, or scope requires a new approval.
- When the project ends or the approval expires, notify IT to revoke access.

Approval applies only to the specific dataset, tool, and time period stated.
Users remain responsible for the results. When uncertain, stop and ask the Head of Unit first.

Recommended AI Tools

Using Free AI Tools through Personal Accounts

Only Level 1 data may be used, in accordance with HITAP guidelines. Check each service's data-use terms and settings before starting.

Tool	Example Uses	Checks Before Use
ChatGPT	General assistant for writing, summarizing, and analysis	Disable model training in settings
Claude	Reads long documents, analyzes, and rewrites	Disable model training in settings
Gemini	General assistant; summarizes and answers questions about our own documents	Turn off Gemini Apps Activity
Canva · CapCut	Graphics, slides, infographics, and video editing	Check media rights before publishing
V2md	Converts documents into text for further use	Check where data are processed
AISysRev	Screens titles and abstracts for literature reviews	Check data transfers to external APIs
Grammarly	Polishes academic English	Turn off text collection
DeepL	Thai–English translation	Do not paste an entire document
Perplexity	Searches for information with links; use as a source-finding aid	Open and verify source links every time

Rules for Personal Accounts

Permitted Use

- Use only with Level 1 data, meaning information already publicly available
- Never use with Level 2 data or above, even if it does not confidential

Before Every Use

- Turn off the use of data for model training in the tool's settings, and check again when the provider updates its service
- Do not share conversation links containing content related to the organization's work

Common Misconceptions

- Creating a free account with an organization email does not make it an organizational account. The permissions and contract remain those of a personal account.
- Work created with a personal account while performing official duties is still considered the organization's work.

HITAP Recommended AI Tools

Permitted for use with Level 1-2 data only

Core — Enterprise Accounts

Tool	Example Uses	Data Level
Microsoft 365 Copilot	Works with files, email, and meetings within the organization's existing systems	1–2
ChatGPT Team	General assistant for writing, summarizing, and analysis	1–2
Claude Team	Long documents, analysis, and coding assistance	1–2
Canva Pro · CapCut Pro	Graphics, slides, infographics, and video	1–2
ChatPDF	Reads, answers questions about, and summarizes PDF documents	1–2
Mentimeter	Creates interactive presentations, polls, and quizzes	1
Zotero · EndNote	Manages and verifies references	1–2

Meeting Transcription and Summarization

Tool	Example Uses	Data Level
Otter.ai	Transcribes meetings, creates transcripts, and summarizes meetings	1–2
Transkriptor	Transcribes meetings, creates transcripts, and summarizes meetings	1–2

Usage Guidelines

How are enterprise accounts different from free accounts?
• The provider has a contract with the organization not to use the data for model training, so Level 2 data may be used. However, the data is still transferred to the provider's systems.

Meeting transcription
• Avoid uploading sensitive personal data or confidential research data.
• If necessary, mask identifying information before uploading.
• After transcription is complete, download the transcript to SharePoint and delete the file from the AI system.
• For accounts shared by multiple people, delete both the audio file and the transcript after each use.

Pending review for HITAP recommendation.
• NotebookLM · V2md · AISysRev — Some units have reported using these tools, but they are not yet on HITAP's register. Before use, check whether they send data outside the organisation.
• New AI features added to recommended software should not be assumed safe. Notify IT before using them with Level 2 data or above.

Settings: Turn Off Model Training

- **ChatGPT:** Settings → Data controls → Turn off “Improve the model for everyone”
- **Claude:** Settings → Privacy → Turn off “Help Improve our AI models”
- **Gemini:** Gemini Apps Activity → Turn off “Keep Activity” (Data may still be retained for 72 hours)
- **Free Copilot: Does not provide enterprise-level assurances. Under HITAP’s Standard Practices, do not use it with Level 2 data or above.**
- **Turning off training is not enough: For Level 2 data or above, use only tools and organisational accounts recommended/authorised by HITAP for that data classification, and obtain approval where required.**

Configure settings before first use and check them periodically.

Menu names may vary by version. If you cannot find a setting or are unsure, contact IT.

Account settings help reduce risk, but do not authorise the use of restricted data. Users remain responsible for the information they enter into AI.

Training disabled ≠ no data retention. It does not change the data’s confidentiality classification.

Safe Use of AI Tools

Do not allow AI tools to access all data on your device.

Limit access to only the folders being used.



To protect data, please follow the AI Policy.

1. Separate the AI Workspace from OneDrive-Synced Folders



Create a dedicated folder separate from folders synced with OneDrive,
such as D:\ai-workspace.
If you are unsure, consult IT.

2 Copy only the files you need into the workspace, and move the results out when finished.

Mask Confidential Data before Entering It into AI



3 Specify the Target Folder Clearly Every Time You Ask AI to Search for or Access Files

Avoid commands such as “search the entire computer” or “find everything.”

Specify the target folder clearly

Search the entire computer /Allow all access

Please follow these requirements strictly.

Quality & Transparency

Quality & Human Review

AI output is considered a “draft” until it has been reviewed for accuracy and appropriateness by the responsible person before use or publication.

1	**Accuracy**	Numerical facts are accurate, references actually exist, and the information is current.
2	**Evidence and References**	References exist, support the claims made, and are sufficient for the conclusions.
3	**Objectivity and Logic**	No bias or stereotyping related to gender, culture, or values. Presents conflicting issues based on evidence and does not take sides without supporting reasons. Clearly separates facts from opinions.
4	**Completeness**	Covers relevant conditions, exceptions, and limitations. Provides enough detail for use or decision-making. Does not oversimplify to the point of losing essential information.
5	**Readiness before Sharing**	Contains no information that is not permitted to be disclosed. Check content-use rights and disclose AI use as required.

Quality & Human Review

Factual Accuracy

• Every number matches the original source — always open and compare with the original file.
• Names of people, organizations, medicines, and diseases are spelled correctly and actually exist.
• Units and currencies are correct (baht / USD, per year / per occurrence).
• Check whether the results are consistent with the Thai and organizational context.
• Check completeness — did AI omit anything without saying so?
• Be cautious of answers that sound confident but have no supporting evidence.
• Different answers to the same question mean the information cannot yet be trusted.

References

• Open every original document — never trust references generated by AI.
• Check that the DOI / PMID actually opens and matches the cited topic.
• Check that the author, year, and journal match the real publication.
• Check that the cited text actually appears in the document and has not been over-summarized.
• Watch for citations that seem plausible but do not actually exist (hallucinations).
• Use reliable software or real databases to verify every reference.
• Report the actual search strategy used, not one drafted by AI.

Checking Information and References That AI May Fabricate (Hallucinations)

AI may provide information that appears credible but is incorrect. It may also generate author names, article titles, publication years, journal names, DOIs, or URLs that do not exist. Users must therefore verify information against the original sources before using it.



Warning Signs That Require Further Verification

1. Unsupported figures: for example, percentages of effectiveness or budget savings without citing the source, calculation method, or conditions.
2. Incomplete references to laws or regulations: the law's name, version, year, or section is not specified for verification.
3. Unverifiable references: links cannot be opened, documents cannot be found, or the DOI leads to an article on a different topic.
4. Current information without a source or date: for example, news, policies, or recent situations that have not been checked against current sources. Broad claims: for example, "research has found" or "experts agree" without specifying which research or which experts.



Recommended Practice

- Verify facts and figures against the original document or a reliable source.
- Check that the reference exists, the details match, and the content supports the cited claim.
- Check changeable information against the current official source, even if AI has used web search.
- If the information cannot yet be verified, leave it out of the work and send it to the responsible person or an expert for review before use.
- If incorrect information has already been used, follow HITAP's incident-reporting procedures.

Cross-Examination and Re-Verification Technique (Cross-Examination Prompting)



Use AI to review the draft from a reviewer's perspective. Instead of simply asking, "Is this answer correct?", ask it to identify errors, unsupported assumptions, missing information, and counterarguments worth considering. Consider starting a new chat to separate the review from the original drafting process.

Ex 1:
Adopting the Role of a Strict Accounting/Fact Checker (The Strict Auditor Role)
[Role]: You are an internal auditor (Internal Auditor) with extremely high rigor, adamant about 100% data accuracy.
[Task]: Please review the following draft report in detail:
[Insert the text/report obtained from AI]

[Instructions]:
1. Find at least 3 points of weakness, logical loopholes, or points with floating citations
2. Point out any points that may contain incorrect numbers or calculations
3. Identify any points where this report is overly optimistic (Overly Optimistic), and suggest a worst-case-scenario risk outlook

Ex 2:
Adopting the Role of an Academic Critic (Devil's Advocate Reviewer)
[Role]: You are an academic who specializes in critical thinking (Devil's Advocate), responsible for finding fault and questioning every recommendation.

[Task]: Read the policy recommendation below, then answer 3 questions:
1. If there were an expert reading this report, which point would they most likely disagree with?
2. Are there any assumptions in this text that would not hold true in the Thai social context?
3. Please write 3 counter-arguments with supporting reasons to challenge this report
[Attached: insert the policy recommendation]

Source: AI Literacy Handbook, Prof. Suthep Suantai

The Triangulation Method with Primary Sources



A convincing answer may still contain errors, even if AI confirms it repeatedly or several tools give the same response. Use triangulation: compare the answer with evidence from original sources, then cross-check it against independent sources or seek expert review before use.

Step Triangulation Workflow

Step 1: Separate Out the "Units of Data That Need to Be Verified" (Extract Claim Units)
Instruct the AI to break its own answer down into Atomized Claims, or small units of individual facts, to prepare them for checking against real sources.

- [Prompt for extracting facts for verification]: "Please extract all the facts, numbers, names of people, names of laws, and statistics from the text below and list them as bullet points, without summarizing the content, so I can use them to fact-check against official sources."

Step 2: Compare Against Primary Sources (Primary Source Cross-Check)
Take each fact and verify it against an official primary source (Primary Official Sources), for example:

- Laws/articles: Check against the Royal Gazette (Ratchakitcha) or the Council of State (Krisadika)
- Economic/public-health figures: Check against the National Statistical Office, the Ministry of Public Health, or the World Health Organization (WHO)
- Organizational regulations: Check against the agency's official Standard Operating Procedures (SOP) manual

Step 3: Assess Conflicts (Conflict Resolution)

- If the AI's output does not match the primary source, always treat the primary source as the highest ground truth (Ground Truth), and immediately discard the portion the AI fabricated.

Source: AI Literacy Handbook, Prof. Suthep Suantai

Human Review 
Responsible person must always review before use.

- AI output is considered a “draft” until it has been reviewed by the responsible person.
- It must be possible to identify “who” reviewed the work and is responsible for it.
- Review every item before use or sharing: check accuracy, completeness, references, bias, and suitability for the task.
- Review using evidence and expertise: do not rely solely on the confidence of the answer or on asking AI to confirm itself. If the matter exceeds your expertise, involve someone with relevant knowledge.
- Increase review according to risk: work affecting research conclusions, policy recommendations, individual rights, or budgets must be reviewed according to the relevant work procedures.
- Correct or stop using it when necessary: if key points cannot yet be verified, revise or delay use. Do not endorse an output simply because it was generated by AI.
- Do not let AI make personnel, financial, or individual-rights decisions on its own. An authorized person must review and confirm them before action is taken.
- Keep evidence of the review according to the risk of the work, identifying the reviewer, the issues checked, and the review results so they can be audited later.

AI supports decision-making but does not replace human decision-making.
Humans must review, exercise judgment, and take responsibility for every decision.

Transparency and Disclosure

Disclose AI use when it contributes to the substance of the work. Disclosure is not required for routine tasks that do not affect the substance.

When to Disclose

- AI makes a substantial contribution to the content.
- AI plays a significant role in the workflow, such as literature screening or data extraction.
- **Disclosure is required by a funder, journal, conference, research ethics committee, project agreement, or external organisation.**
- AI's involvement could affect the credibility or transparency of the work.
- AI is used to generate images, media, or videos for public dissemination.

When Disclosure Is Generally Not Required

- Spell-checking, grammar checking, or minor wording adjustments.
- Translating short text and helping with formatting.
- Initial brainstorming.
- Summarizing information for internal working notes.
- Removing an image background.
- However, if the AI output becomes the main content of the work, disclosure is required even if it began as a routine task.

Examples of disclosure text

- Under an image or video: "AI-generated image" "This video contains AI-generated content" "Created with AI assistance"
- In acknowledgments: "AI was used to assist with language editing. The content was reviewed and verified by the authors."
- In the methods section: State the tool name, developer, version, period of use, scope of use, and how the output was checked.
- Always follow the requirements of the funder or journal first.

If AI affects the substance of the work, disclose it. If it affects only the format, disclosure is not required.
When unsure, disclose first, and never conceal AI use when asked.

Disclosure

Where AI is substantively used in the conduct of research, researchers should maintain appropriate documentation of the AI use, including:

- AI tool used;
- model or version, where available;
- purpose of use;
- relevant prompts, where applicable;
- method used to review or verify the AI-generated output; and
- date or period of use, where relevant.

Researchers must be able to explain how AI-generated outputs were reviewed or verified before being used for analysis, interpretation, reporting, or publication.

*Always follow journal, funder, or recipient requirements.

Disclosure Template

"During the preparation of this work, the author(s) used [Specify tool name, e.g., ChatGPT-4o] in order to [Specify reason, e.g., improve readability and language editing of the manuscript]. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication."

Where to Disclose: Acknowledgements for drafting and language editing · Methods for AI-assisted screening, data extraction, or analysis · Figure captions for AI-generated or AI-assisted images.

Five Required Elements

- Tool and model/version: Specify the tool and model used, such as ChatGPT (GPT-4o), rather than simply "AI".
- Period of use: State the month and year.
- Purpose and scope: Identify the specific stages or tasks supported by AI.
- Human verification: Describe what the authors checked after receiving the outputs.
- Responsibility: Confirm that the authors take full responsibility for all content.

Important Considerations

- Always check the target journal's requirements for disclosure wording and placement.
- Do not list AI as an author or co-author. AI cannot take responsibility for the work.
- Before using AI to review another author's manuscript, check the journal's policy. Many journals prohibit such use. HITAP's own restrictions must also be followed.

Disclosure Template

- AI-generated image/This video contains AI-generated content/ Created with AI assistance
- AI was used to assist with language editing. The content was reviewed and verified by the authors.

Acknowledgements

I gratefully acknowledge the valuable comments and suggestions received from participants at the Professor Donal O'Donoghue Global Kidney Policy Forum during the World Congress of Nephrology 2025, where an earlier version of this work was presented. Large language models, including ChatGPT (OpenAI) and DeepSeek, were used solely to enhance the clarity and readability of the submitted version of this manuscript; they did not contribute to the intellectual content, analysis or conclusions of the article. The Health Intervention and Technology Assessment Program Foundation (HITAP) is a research unit in Thailand and supports evidence-informed priority-setting and decision-making for health. HITAP is

- Acknowledgements: AI assistance with drafting, editing, translating, or formatting the manuscript.
  - “The authors acknowledge the use of Microsoft Copilot (accessed August 2024) to generate a first draft of the Acknowledgments section and translate the Methods section from Spanish to English. All AI-assisted text was reviewed and revised by the authors to ensure accuracy and clarity of meaning.”

- Methods: AI assistance with research methods, data analysis, or literature reviews.
  - “Literature screening was assisted by GPT-4 (accessed March 2024) to categorize 500+ abstracts by predefined relevance criteria. AI-assisted outputs were reviewed and validated by the authors, who confirmed the final inclusion and exclusion decisions.”

- Figure caption: AI used to create or modify images, graphs, or diagrams.
  - “Figure 1. Conceptual diagram of treatment pathway. Diagram created using DALL·E 3 (accessed March 2024) to generate an initial draft, with subsequent modifications by the authors in Canva. All content was reviewed for accuracy by the clinical team.”

- Peer review: AI assistance with wording or structuring reviewer comments.
  - “GPT-5 was used to prioritize and polish review feedback. All original review feedback was provided by the peer reviewer, and all AI-generated content was reviewed, revised, and approved by the peer reviewer prior to sending this review.”



Learn more : Wiley — Using AI tools in your research www.wiley.com/en-us/publish/article/ai-guidelines

Incident & Support

7 REPORTABLE INCIDENTS

1 **Suspected Security or Trustworthiness Issues with an AI Tool or Account**
Uploaded files become accessible to others unintentionally, the tool asks you to enter your email password in the chat, or files are downloaded or extensions installed without your instruction.
Immediate action: Stop using the tool or account · Securely preserve evidence and details of any data shared or permissions granted · Notify Head of Unit and IT.

2 **Confidential or Personal Data Entered into AI**
Patient data or confidential documents entered into a tool or account not authorised to process that data.
Immediate action: Stop the affected activity · Securely capture screenshots as evidence · Notify Head of Unit and IT.

3 **Suspected AI Data Leakage**
Internal or confidential information becomes accessible to unauthorised individuals, or chat links are shared beyond the authorised scope.
Immediate action: Stop the affected activity · Disable shared links or restrict access · Securely preserve evidence · Notify Head of Unit and IT.

4 **AI-Generated Misinformation Distributed**
Materially incorrect figures, facts, or references generated by AI have been shared, published, or used to inform decisions.
Immediate actions: Stop further distribution · Notify Head of Unit and IT · Coordinate with recipients or relevant parties to correct or withdraw the information.

5 **Suspicious AI Behaviour**
AI provides internal information that was never submitted, or an Agent acts autonomously.
Immediate actions: Screenshot and save the prompt used; stop using the tool; notify Head of Unit and IT for investigation.

6 **Account Compromise**
Unrecognized chat history or access from an unfamiliar device.
Immediate actions: Change the password; enable MFA; log out from all devices; notify Head of Unit and IT.

7 **Copyright Concern**
Reason to suspect that AI-generated images or text reproduce or adapt someone else's work without the necessary rights or permission.
Immediate actions: Suspend use or publication of the material · Notify Head of Unit and IT · Check usage rights · If already published, coordinate corrections or removal as appropriate.

Incident & Support

REPORTING INSTRUCTIONS

Email Your Head of Unit and CC IT

- Send the report within 24 hours of becoming aware of the incident.
- Include: what happened · when · the tool or account involved · the data classification · actions already taken.
- If personal data are involved, also CC management.



What Happens After an Incident Is Reported?

In Parallel with the Initial Assessment
Management, head of unit, and IT assess whether the personal data breach requires notification to the relevant authorities or affected individuals under the PDPA, and ensure any required notifications are made within the statutory timeframes

Immediately upon Discovery, Within 24 Hours
Person identifying the incident: Stop the affected activity, notify the head of unit and IT, and securely preserve evidence.

Within 1 Working Day
Head of unit and IT: Conduct an initial assessment, contain or reduce the impact, and coordinate with management or relevant personnel.

Within 5 Working Days
Assigned personnel: Investigate the cause and develop initial corrective measures.

Within 30 Days
Assigned personnel: Summarise lessons learned and a plan to prevent recurrence. Share findings without identifying the individuals involved.

Early Reporting Helps Reduce Harm: HITAP encourages staff to report AI-related errors, incidents, risks, or concerns as soon as they are identified, so we can address them together and reduce their impact. Those who report in good faith will be treated fairly. Lessons learned will be shared without identifying the individuals involved to help prevent recurrence.

Support
If you have questions or need help using AI, contact your head of unit and/or IT, as appropriate to the issue.

Incident Types and Reporting Criteria

Incidents are divided into two types because they require different solutions. Clearly identify which incidents must be reported and which only need to be recorded.

Type 1: User-Caused Incidents
Addressed through training and account controls

- Entering Level 3 or 4 data into a tool
- Using a personal account for organizational work
- Sharing a conversation link containing organizational data
- Using an unapproved tool without requesting approval

Type 2: AI System Incidents
Addressed through human review and tool selection

- Generating information or references that do not exist
- Biased or discriminatory outputs
- An AI agent acting beyond its instructions
- Outputs that infringe another person's copyright
- Data leakage between users caused by the service

When Must an Incident Be Reported, and When Should It Simply Be Recorded?

Notify the head of unit and IT as soon as possible, within 24 hours of becoming aware of the incident.

- Level 3–4 data — confidential or personal data — is sent to AI or disclosed outside the permitted scope, including suspected data leaks, regardless of whether the output was used.
- When an incorrect output has already been used, published, shared with an external party, or used to support a decision.

Record Only — No Incident Report Required

- AI provides information or references that do not exist; the user detects the issue, identifies the error before use, and corrects it or stops using it, with no data leakage, unauthorized action, or impact on others.

Data shared outside the authorised scope or AI acting beyond its permissions = Always report
Materially incorrect output already used = Report
Errors caught and corrected before use, with no impact = Record only

Examples of Problems Caused by AI System Performance

- Provides incorrect or nonexistent references
- Gives a confident-sounding answer, but the facts are inaccurate
- Misinterprets the user's context or needs

All three are Type 2 incidents.

Response: Focus on building fact-checking and reference-verification skills, using a checklist first. Finding an AI error does not mean the user did something wrong.

Why Separate Incident Types?
To analyze causes and apply targeted fixes across tools, usage, and review procedures. One incident may involve multiple contributing factors.

AI Do’s and Don’ts

Do’s & Don’ts

Quick Reference

DO’s

- Check the data level and choose the appropriate tool and account.
- Use only the data you need and check files before uploading.
- Check facts, figures, and references before use.
- Have someone else review before entering data into AI, making a decision, or submitting work.
- If you notice an abnormality or suspect an AI-related incident, notify Head of Unit and IT immediately.
- Check prompts, attachments, and data-access permissions every time before using AI, and do not connect AI tools to organizational data sources such as SharePoint.

DON’Ts

- Enter confidential, personal, or sensitive data into AI.
- Trust AI output without verification.
- Conceal the use of AI when it must be disclosed.
- Use AI to create or distribute false, misleading, or deceptive information.
- Let AI make decisions on behalf of humans in matters with significant impact.
- Ignore requirements from laws, funders, journals, or regulatory bodies.
- Wait until damage occurs or the issue has been fixed before reporting it.
- Send an entire document without checking the information it contains.

AI Can Be Used, But “THINK” Before You Use It

T

Trust but Verify

Check the answer before using it.

- Open the original source and compare numbers and references.
- If asking again produces different answers, it is not reliable yet.

H

Handle Data Carefully

Do not enter confidential or personal information.

- Patient data and sensitive information are prohibited.
- Level 2 data and above must be used with an organizational account only.

I

Intellectual Property

Respect copyright and intellectual property.

- Check copyright before uploading full-text materials.
- Do not claim AI-generated work as your own.

N

No Sensitive Decisions Alone

Do not let AI make important decisions instead of people.

- Decisions involving people, money, or rights require human decision-making.
- Interpretation of research findings belongs to the researcher.

K

Keep Responsibility

The user remains responsible.

- AI output is always a "draft".
- It must be possible to identify who reviewed the work and is responsible for it.

Unsure? Pause and consult Head of Unit and/or IT - If you wouldn’t share it outside HITAP, don’t share it with AI.