ODYSSEY SOLUTIONS OPERATOR TOOLKIT

Dental Practice AI Use Policy Template

A practical template for approving AI tools, use cases, data handling, human review, integrations, records, and incident reporting.

Prepared for	[Practice or organization name]
Prepared by	Odyssey Solutions | Houston IT, cybersecurity, and HIPAA guidance

Start here: Customize every bracketed field, assign an accountable owner, and test the finished process with the people who will use it. Keep completed copies in a controlled location.

Important: This template is educational and does not provide legal, insurance, privacy, compliance, or clinical advice. It does not guarantee HIPAA compliance, insurance eligibility, security, or recovery. Confirm requirements with qualified professionals and never enter patient information, passwords, or other sensitive data into an uncontrolled copy.

How to use this template

1. Replace bracketed fields and remove options that do not apply.
2. Inventory every AI-enabled tool already used by staff, vendors, or connected applications.
3. Approve the service, account configuration, information class, and use case separately.
4. Train the workforce on prohibited inputs, required review, and incident reporting.
5. Review this policy after material tool, workflow, vendor, regulatory, or risk changes.

Policy control record

Field	Practice entry
Organization	[Legal practice or organization name]
Policy owner	[Name and role]
Approved by	[Executive or governing role]
Effective date	[YYYY-MM-DD]
Next review date	[YYYY-MM-DD]
Applies to	[Employees, contractors, owners, locations, and vendors]
Related policies	[HIPAA, security, acceptable use, records, incident response]

1. Purpose and scope

[Organization] uses artificial intelligence only when the tool, account, configuration, information, and intended use have been reviewed and approved. This policy applies to standalone AI services, AI features inside existing software, automated agents, transcription tools, chatbots, image generators, coding assistants, and vendor-provided AI capabilities.

AI does not replace professional judgment, clinical responsibility, privacy obligations, security controls, records requirements, or human accountability.

2. Information classification and input rules

Information class	Examples	Default AI rule	Approval required
Restricted	Patient information, ePHI, credentials, payment data, government identifiers	Do not enter unless the exact service and use are formally approved	Privacy, security, legal/compliance, and business owner
Confidential	Contracts, HR records, internal financials, nonpublic operations	Use only in approved business accounts and approved workflows	Information owner and security
Internal	Procedures, drafts, internal communications without restricted data	Use only in approved tools with human review	Department owner

Information class	Examples	Default AI rule	Approval required
Public	Published website content, approved marketing material, public references	May be used in approved tools; verify accuracy and rights	Content owner

Default rule: If a staff member is uncertain about the information class, the tool, or the use case, they must stop and ask the policy owner before submitting the information.

3. Approved AI service register

Tool or feature	Business owner	Approved account/configuration	Information allowed	Review date
[Tool name]	[Owner]	[Business tenant, retention, training controls]	[Public / Internal / Other]	[YYYY-MM-DD]

4. Approved use-case register

Use case	Tool	Permitted inputs	Required reviewer	Output or record location
[Example: draft public FAQ]	[Tool]	[Public source material]	[Marketing owner]	[Approved content system]

5. Prohibited activities

Done	Action
[ ]	Entering patient information, ePHI, credentials, payment data, or restricted records into an unapproved tool.
[ ]	Using a personal account for organization work when a managed business account is required.
[ ]	Letting an AI system make a final clinical, employment, legal, financial, privacy, or security decision without an accountable human reviewer.
[ ]	Publishing or sending AI output without checking accuracy, context, confidentiality, bias, rights, and audience.
[ ]	Connecting an AI tool to email, files, patient systems, identity platforms, or other applications without written approval.
[ ]	Disabling logging, retention, security, or administrative controls that the organization requires.
[ ]	Representing AI-generated content as verified professional advice or guaranteed fact.

6. Meaningful human review

The assigned reviewer must be qualified to evaluate the output and must:

- Check facts, calculations, citations, dates, names, and required context.
- Confirm the output does not reveal restricted or confidential information.
- Evaluate whether the result could mislead a patient, employee, vendor, regulator, insurer, or customer.
- Edit or reject unsuitable output instead of treating AI output as authoritative.
- Record approval when the workflow, policy, contract, or risk decision requires evidence.

7. Accounts, access, and integrations

Done	Action
[ ]	Use organization-managed identities, multifactor authentication, and least-privilege roles.
[ ]	Assign a business owner and a technical owner for every approved service.
[ ]	Review data retention, model-training settings, sharing, plugins, connectors, and administrative logs.

Done	Action
[ ]	Inventory connected applications and remove unused permissions.
[ ]	Disable accounts and revoke integrations promptly during offboarding.
[ ]	Confirm contract terms, security responsibilities, incident contacts, and any required business associate agreement.

8. Records and evidence

The policy owner maintains the approved-tool register, approved-use-case register, review decisions, training records, significant output approvals, vendor records, incident records, and revision history according to the organization's retention requirements.

9. Mistakes and incident reporting

1. Stop the activity and do not delete relevant evidence.
2. Notify [incident contact] using [approved channel] as soon as possible.
3. Record the tool, account, user, time, information involved, output, recipients, and actions already taken.
4. Follow the organization's incident response, privacy, legal, insurance, and notification decision processes.
5. Document corrective actions, owner, due date, retest, and policy or training updates.

10. Training, exceptions, and enforcement

Workforce members receive this policy before using AI for organization work and after material changes. Exceptions require written approval from [roles]. Violations may result in removal of access, corrective action, contract action, or other consequences consistent with organization policy.

Staff acknowledgement

Acknowledgement	Entry
Name	_____
Role	_____
Signature	_____
Date	_____

Make the policy match the real environment

Odyssey Solutions can inventory current AI use, review connected systems and data flows, tailor this policy, train staff, and connect the result to HIPAA, cybersecurity, vendor, and incident-response work.

Book an Odyssey consultation

Official references

- **HHS HIPAA Security Rule guidance:** https://www.hhs.gov/hipaa/for-professionals/security/index.html
- **NIST AI Risk Management Framework:** https://www.nist.gov/itl/ai-risk-management-framework
- **NIST AI RMF Generative AI Profile:** https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence
- **FTC guidance on AI claims and accountability:** https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check

Important: This template is educational and does not provide legal, insurance, privacy, compliance, or clinical advice. It does not guarantee HIPAA compliance, insurance eligibility, security, or recovery. Confirm requirements with qualified professionals and never enter patient information, passwords, or other sensitive data into an uncontrolled copy.