



**AMERICAN
PSYCHOLOGICAL
ASSOCIATION**



APA's AI tool guide for practitioners

This step-by-step guide discusses how to decide which AI tools are right for your practice

Artificial intelligence (AI) is evolving rapidly and is increasingly integrated into both everyday life and health care delivery. AI-enabled tools designed for use in health care are expanding beyond administrative functions such as scheduling or documentation to include clinical tools such as clinical decision support, symptom monitoring, and patient engagement tools, among others, to augment traditional therapy delivery. Given the rapid expansion of tools marketed to mental and behavioral health (MBH) professionals, it is important for psychologists to develop a process to assess whether and if so, how AI tools may support their practice and the needs of those that they serve.

Below is a guide that highlights many of the important considerations when evaluating AI-enabled tools for possible inclusion in your practice. To gather this information, review the company website, terms of service, privacy policy, business associate agreement, and any AI specific documentation. Psychologists who work in organizational settings are encouraged to consult any existing internal AI policies before incorporating AI tools into their work and may be required to choose from a list of organizationally vetted or approved tools.

CLARITY ABOUT THE PROBLEM THE AI TOOL IS SOLVING

The first step in exploring a new AI tool for one's practice is to gain clarity on the problem that the AI tool will address and to begin identifying relevant tools.

COMPANY (VENDOR/DEVICE MAKER/ DEVELOPER/INDUSTRY PARTNER)

Once a potential tool is identified, psychologists may consider gathering information regarding the company's reputation and standing within the field. This could include a review of how long the company has been in business and whether they have a strong track record of developing successful mental health products. You may also research whether the company has collaborations with trusted health care organizations, academic institutions, or professional associations. In addition to positive product and user reviews, you can review whether they have conducted research on their product and whether that research has been published in peer-reviewed publications.

It's also important to understand who is on the leadership team of the company. If a tool is designed for use by MBH

professionals: are psychologists or other MBH professionals represented in leadership positions that guide development of and have oversight for the product? For example, MBH professionals may be represented in roles such as chief medical officer, clinical director, director of research, or they may serve on clinical or scientific advisory boards.

FEATURES AND FUNCTIONALITY

Psychologists have unique practice needs; a tool that works well for one practice may not be suited to another practice. Review whether a particular tool offers the function(s) or feature(s) that are important to your practice needs. Additional questions include:

- Which functions or features of the tool use AI?
- Does the tool integrate with software or the electronic health record (EHR) that you may already be using?
- Does it fit easily within your workflow to improve efficiency or enhance care delivery?
- Is it a cost-effective tool for your practice needs?
- Does the tool support accessibility features such as screen readers, resizable text, or captioning?
- Does the company offer demos of their product or a limited free trial?
- What kind of tech support is offered by the company?
- How much time do you estimate it will take you and any employees to learn to use the AI tool?

AI GOVERNANCE

AI governance is the framework of policies, processes, and oversight used to ensure AI systems are safe, effective, ethical, and compliant throughout their lifecycle, from development and deployment to ongoing monitoring and improvement. Companies may have AI specific documentation on their website, sometimes in sections with headings such as “AI safety”, “Responsible AI”, or “Trust center”.

Key considerations include:

- Does the company clearly disclose how the AI tool is intended to be used, its capabilities, and its limitations?
- Does the company provide documentation describing how the tool was developed and evaluated?

- Does the company evaluate the accuracy, reliability, and consistency of AI output?
- Has the company conducted and made available evidence regarding the tool’s safety and effectiveness for its intended use?
- What kind of research has been conducted? (e.g., survey data, a real-world effectiveness study, a randomized controlled trial, etc.)
- What guardrails exist to help ensure the product functions safely and minimize any potential harm or unintended consequences?
- Is the tool subject to regulatory oversight? The FDA regulates software as a medical device, meaning software that is intended to diagnose, cure, mitigate, treat, or prevent a condition. If so, what is its regulatory status?

Bias, equity, and fairness

Algorithmic bias occurs when AI models produce unfair outcomes or systematically disadvantage particular groups. Bias can be introduced in a variety of ways, including unrepresentative or incomplete training data, as well as human judgements made during design, development, or deployment.

It is important to note that there is variability in the degree to which companies publicly share the information below. Companies may disclose some, but not all, of this information. You may wish to reach out to a company directly to inquire about questions that you were unable to answer.

Key considerations include:

- Was the data on which the AI model was trained representative of the intended user base?
- In what settings and with what populations have the tool’s performance been evaluated?
- Are there differential outcomes for specific groups?
- Does the company conduct fairness audits and document the steps taken to minimize bias?

Post-deployment

Post-deployment considerations include the mechanisms for ongoing monitoring of a tool’s performance once it is being used in a real-world clinical setting.

Key considerations include:

- Does the vendor engage in ongoing performance monitoring of the tool? If so, how?

- Is there a process for human oversight of the product's performance over time?
- What are the incident monitoring and escalation protocols? In other words, is there a clear process to identify and respond to any AI errors or safety risks?
- Does the company notify users when significant updates are made to the AI model?

PRIVACY COMPLIANCE

Confirm whether the company attests compliance with applicable laws and regulations, such as HIPAA, GDPR, and/or other applicable privacy and data security standards in the jurisdiction(s) where you practice. Many jurisdictions (including California, Colorado, Nevada, and Virginia), have specific state-based data privacy laws that may apply. Privacy policies often have a separate state-specific section.

If the tool creates, receives, maintains, or transmits protected health information (PHI) on a psychologist's behalf, a signed business associate agreement (BAA) with the company is needed.

DATA GOVERNANCE

AI tools may have access to a wide variety of identifying information both about the clinician who adopted the tool and the patients who either use or whose data are processed by the tool. It is important to understand what data are being collected, how that data can be used, and what happens to the data once you stop using the tool. To find this information, you will begin by reviewing the privacy policy and BAA, but some information may be found in other documents like the terms of service.

- What data are collected and for what purpose?
- Who has access to the data? This may include employees of the company that provides the tool, as well as third parties with whom the company contracts, like AI foundation model providers.
- What is the data retention policy? How long are data retained? Who owns the data and what happens to it when you terminate your contract with the company and/or if the company goes out of business or is acquired?
- Are data used exclusively to provide the service, or can data also be used for additional activities, such as product improvement, employee training, research, marketing, and/or analytics? Can you or your patients

opt out of any secondary uses of data, if you wish to do so?

- Does the vendor sell data? Selling PHI is a violation of HIPAA and possibly other applicable data privacy and security laws. While HIPAA generally permits the use, including the sale, of properly de-identified data, psychologists may consider whether such practices align with their professional expectations. For more information on methods to de-identify PHI that are in accordance with the HIPAA Privacy Rule, see the guidance provided by the U.S. Department of Health and Human Services (HHS).
- Pay particular attention to the collection of sensitive information, such as biometric, voice, and neural data. Because some biometric data are inherently identifiable, additional safeguards may be warranted. See APA's Resolution on the Protection of Neural and Cognitive Data for more information. Additionally, some states may have relevant laws that specifically govern the use of biometric data (such as the Illinois Biometric Information Privacy Act) or states may have consumer data privacy laws that address biometric data within the overarching legislation.

Are user data used to train AI models?

This is an important consideration for AI-enabled tools. Key questions include:

- Is clinician or patient data used to train, fine-tune, or improve AI models?
- Is training enabled by default? Is an opt-out mechanism available?
- HIPAA prohibits using identifiable data without explicit consent. However, properly de-identified data is no longer considered PHI and can be used to train AI models. Companies may indicate in their BAA or privacy policy that they do not use PHI for model training. Confirm whether de-identified data is used for model training or other internal improvements and whether you can opt out, if you wish to do so.

How are data retained, deleted, and controlled?

Review the company's policies (this information is often found in the privacy policy but may be in other documentation like the terms of service or BAA) regarding how long data are retained, where the data are stored, users' rights to access, correct, export, or delete data, and processes for terminating your account.

TECHNICAL SECURITY

The HIPAA Security Rule requires that electronic protected health information (e-PHI) be secured when it is in transit and at rest; however, it generally does not specify which security measures a regulated organization must use.

- National Institute of Standards and Technology (NIST) has developed guidance to assist organizations in complying with the Security Rule. Advanced Encryption Standard (AES) is a widely used and U.S. government-approved algorithm used to encrypt and decrypt data. Products often are listed as using AES-128, AES-192, or AES-256-bit encryption. The numbers (128, 192, 256) refer to the bit length of the encryption/decryption key.

Does the company report additional technical security measures or certifications?

- Does the tool require multifactor authentication (e.g., two or more credentials to login)?
- Does the company report third-party security certifications or attestations? These could include HITRUST certification, SOC 2 attestation, ISO 27001 certification, among others.
- Does the company engage in penetration testing? This generally involves hiring an independent, third-party company to simulate a cyberattack to identify and mitigate any security vulnerabilities.

HUMAN OVERSIGHT

AI tools can support clinical care, but AI tools also can be misleading or wrong, and psychologists remain responsible for clinical decision-making. When using an AI tool, it is important for clinicians to consider how they will maintain oversight; this may vary depending on the functions of the tool. For tools that assist with documentation or clinical recommendations, clinicians review outputs and modify them as needed before incorporating them into the clinical record or care plan. For tools that are patient facing, it is important to understand what information will be available to the treating clinician. For example, some tools may include a clinician dashboard that shares information about a patient's use of the tool, such as sharing symptom monitoring or homework completion. For a tool that has any risk detection features, it is critical to understand how risk is identified, how you will be alerted to any patient safety concerns, and whether any crisis resources are provided directly by the tool.

INFORMED CONSENT

It is important to consider how you will talk with patients about AI tools that may be integrated into care. This may require updating informed consent processes and documentation to include information about the purpose, as well as the potential risks, benefits, and limitations of AI tools. Additionally, psychologists are encouraged to consider whether they feel they have adequate information about the tool to have an informed consent discussion with patients and answer any of the questions that may arise. It also is helpful to have a process to check with patients regarding their experience of any patient-facing AI tools.

Importantly, AI legislation is rapidly evolving, and informed consent requirements may vary by jurisdiction. You are encouraged to review the relevant laws in the jurisdictions in which you practice to ensure compliance.

CONTACT THE COMPANY FOR ADDITIONAL INFORMATION

After reviewing this information, you may contact the company if you have further questions or you are unable to answer any of the above questions. You also may consult with a local attorney if there are provisions in the privacy policy, terms of service, and/or BAA that are unclear.

NEEDS OF YOUR PRACTICE

The decision about incorporating an AI tool into your practice is an individual decision based on one's practice needs and a thoughtful risk-benefit analysis. However, these steps will help you gather the relevant information needed to make an informed decision.

LEGAL AND LIABILITY CONSIDERATIONS

As with any technology-enabled care, you are encouraged to consult with your liability carrier to ensure that your use of technology is covered by your professional liability policy or whether additional policies such as a cyber liability policy would be appropriate.

Legislation regarding the use of AI in health care is rapidly evolving, particularly at the state level. You are encouraged to consult with a local health care attorney familiar with AI and privacy regulations in your practice location(s) to ensure that you are in compliance.

DOCUMENT YOUR REVIEW

You are encouraged to document your initial review of the above information to demonstrate your due diligence in selecting a tool.

REVIEW POLICIES FOR UPDATES

Companies may periodically update their privacy policies and terms of service; you are encouraged to review these updates and consider whether any subsequent changes may be needed to your informed consent process.

ADDITIONAL RESOURCES

[Use of Generative AI Chatbots and Wellness](#)

[Applications for Mental Health](#)

An APA Health Advisory

[APA Labs Digital Badge Program](#)

Independent, evidence-based evaluations of digital mental and behavioral health technologies

[Guidance for the evaluation of AI scribes](#)

Practical considerations for psychologists when integrating AI tools into their practice

[Ethical guidance for AI in professional practice](#)

Practical considerations and recommendations for using AI in real-world clinical settings

This document is provided by APA as a preliminary guide for psychologists considering the integration of tools utilizing AI into their practice. It is intended to serve as a starting point for evaluation and is not exhaustive. Users are encouraged to apply their own professional judgment and seek additional resources and guidance as needed, including legal consultation to ensure compliance with applicable laws and regulations. APA does not endorse any specific AI tools and assumes no responsibility for the outcomes of their use. Always ensure compliance with relevant ethical guidelines and legal requirements.