

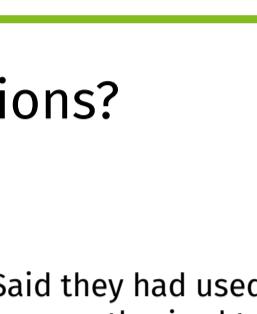
# How are shadow AI tools used in healthcare?

A Wolters Kluwer Health survey of healthcare providers and administrators assessed the usage and perceived risks of shadow AI tools in the workplace.

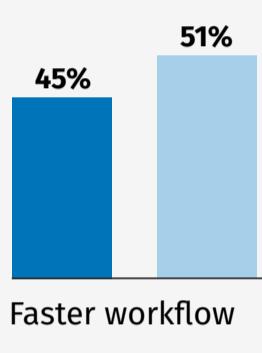
**What is “shadow AI”?** Shadow AI occurs when employees use unapproved AI-powered tools across an organization. As a result, leaders lack insight into usage, increasing risks to security, data breaches, and—in healthcare—patient safety.

## \$7.42M USD –

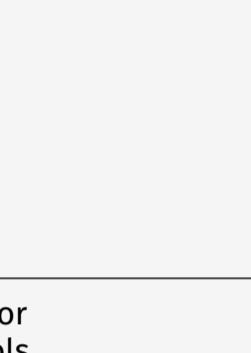
Average cost of AI security breaches for the healthcare industry in 2025<sup>1</sup>



## How are unapproved AI tools used in organizations?



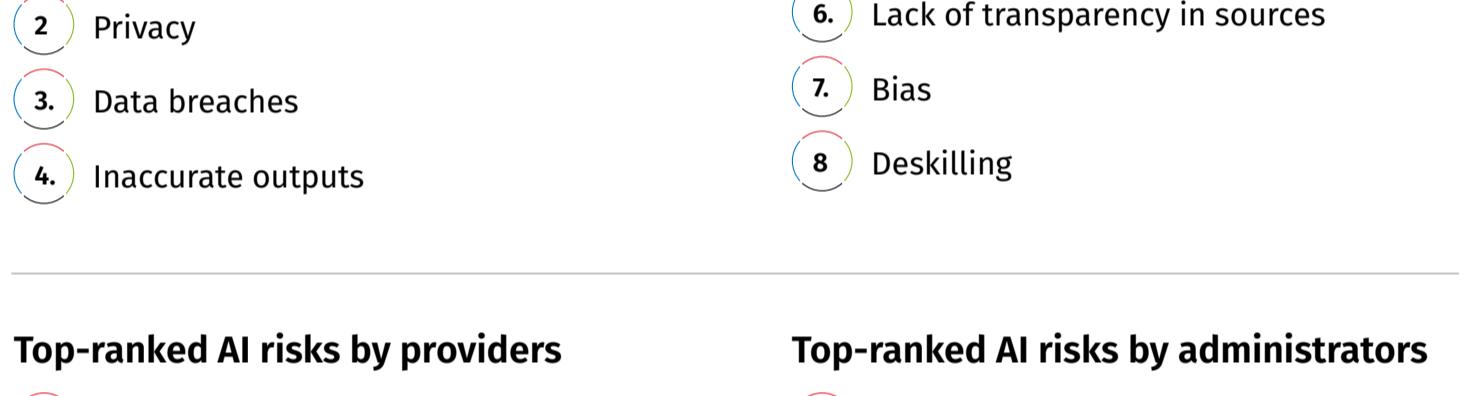
Respondents who were aware of colleagues using unauthorized AI tools



Said they had used an unauthorized tool

### Reasons for using unauthorized AI tools

■ Provider ■ Administrator



## What are some of the top risks posed by AI?

### Overall AI risks, ranked

1. Patient safety
2. Privacy
3. Data breaches
4. Inaccurate outputs

5. Regulatory compliance
6. Lack of transparency in sources
7. Bias
8. Deskilling

### Top-ranked AI risks by providers

1. Patient safety
2. Inaccurate outputs
3. Privacy

### Top-ranked AI risks by administrators

1. Patient safety
2. Privacy
3. Data breaches



Concern about bias in AI tools, top 3 rankings

⇒ Less than 5 years of practice: 21%



Concern about deskilling, top 3 rankings

⇒ Less than 5 years of practice: 34%

⇒ 5-19 years of practice: 27%

⇒ 5-19 years of practice: 22%

⇒ 20+ years of practice: 42%

⇒ 20+ years of practice: 27%

Providers who responded: “I never use AI tools”

⇒ Less than 5 years of practice: 16%

Providers who used AI for clinical decision support

⇒ 5-19 years of practice: 3%

⇒ Less than 5 years of practice: 31%

⇒ 20+ years of practice: 5%

⇒ 5-19 years of practice: 46%

⇒ 20+ years of practice: 45%

UpToDate® Expert AI can support consistent clinical decision-making across your enterprise.

Learn more →