AMA | Center for Digital Health & AI

AI-Generated Deepfakes: Key Policy Principles and Proposed Protections

Advances in generative augmented intelligence (AI) now allow realistic impersonation of physicians through synthetic images, audio and video ("deepfakes"). When used maliciously or without consent, these tools can spread medical misinformation, damage physicians' reputations and careers, and undermine patient trust in evidence-based care. Existing privacy, employment and intellectual property laws do not adequately address these risks in clinical contexts.

The AMA has identified key policy principles applicable to AI-generated deepfakes that establish clear, enforceable protection for physicians against unauthorized AI-generated impersonation, while safeguarding patient safety, professional integrity and public trust in medicine. This policy framework seeks to modernize identity protections for physicians in the AI era and close critical legal gaps, recognizing identity misuse as both a patient safety and professional integrity issue.

1. Physician Identity Is a Protected Right

- A physician's name, image, likeness, voice and digital replicas are protected interests.

- Health institutions, health technology vendors, third-party applications and affiliated service providers must explicitly acknowledge that a clinician's name, image, likeness, voice or digital representation is not a transferable, sublicensable or implied asset of employment, credentialing, contracting, data integration or technology deployment, and may not be used beyond the scope of the clinician's informed, affirmative consent.

2. Prohibition on Deceptive Medical Impersonation

- Absent informed, affirmative consent, the use of a physician's identity in AI-generated or materially altered content that falsely conveys the physician's endorsement, authorship or medical judgment and is likely to mislead a reasonable patient in a health-related decision must be prohibited and should be treated as a deceptive practice. Failure to provide a clear and conspicuous disclosure of synthetic content should weigh in favor of a finding of deception.

3. Informed, Opt-In and Revocable Consent

- Use of a physician's identity in AI-generated or manipulated content requires affirmative, informed opt-in consent. Consent may not be implied, inferred or obtained through general terms of service, employment agreements or blanket media releases. Consent must be separate, explicit and specific to AI-generated or synthetically manipulated uses, and must identify:

  a. How the identity is used (image, voice, avatar)
  b. Where it appears (patient-facing, internal, public)
  c. The purpose and duration of use

- Advertisers and digital health companies have a duty to verify authorization before using a physician's identity in health-related marketing.

- Consent must be revocable if risks change or the physician's role changes.

Continued on next page ...

4. Mandatory Labeling and Transparency

- AI-generated or materially altered content depicting a physician must be clearly and conspicuously labeled in plain language and include a "digital watermark."

- Patients interacting with an AI-generated health professional must be alerted prior to the interaction and disclosed immediately.

5. Shared Responsibility for Preventing Impersonation

- Platforms, hospitals, health systems and AI vendors share responsibility for preventing misuse.

- Required safeguards include:
  a. Clear and conspicuous labeling of AI-generated or manipulated content
  b. Rapid reporting and takedown mechanisms for health-related deepfakes
  c. Prohibiting the use of health professional titles by AI-generated content

6. Enforcement and Practical Remedies

- Physicians must have access to clear, workable processes to:
  a. Document identity misuse
  b. Trigger takedown and escalation procedures
  c. Seek institutional remedies or legal relief when necessary

- Institutions and platforms must:
  a. Preserve audit logs noting how the AI-generated content was created, modified, distributed or interacted with
  b. Cooperate with investigations
  c. Provide transparent escalation pathways with defined timelines

Enforcement and Practical Remedies *continued ...*

- A designated federal agency with explicit authority to enforce protections against deceptive medical impersonation and unauthorized use of a physician's identity in AI-generated or manipulated content should be required to:

  a. investigate violations;
  b. require preservation of relevant records and audit logs;
  c. compel cooperation;
  d. seek injunctive relief and civil penalties;
  e. mandate corrective disclosures; and
  f. produce an annual public report on health-related impersonation incidents, takedown performance and enforcement actions

7. Minimizing Administrative Burden

- Any mandatory requirements seeking to protect physicians against unauthorized use of their identities must not create an undue administrative burden on clinicians.

- Identity protection is the default; physicians should not bear ongoing monitoring or enforcement responsibilities.

- Consent mechanisms should be standardized, reusable and supported by institutions and platforms.

26-1635000:pdf:3/26