CMSS AI TASK FORCE

AI RISK IDENTIFICATION AND MITIGATION CHART

Risk	Examples	Mitigation Strategies
Intellectual property esp. copyright – (1) avoiding infringement and (2) ensuring copyrightability	• Inputting of copyrighted specialty society materials into LLMs	• Inform membership of requirement to obtain permission prior to inputting material into LLM; send cease-and-desist letters to anyone (including members) who infringes society materials; ubiquitous banner on website pages
	• General trawling of content on internet by LLMs	• Anti-piracy vendors and metadata warnings may be used • Consider using a strategy (e.g., Robots.txt) to restrict crawling of portions of the website • Evaluate which content should be behind paywall to protect highest value content
	• Use of generated AI to create content for use by specialty societies; efficiency and workflow	• Ensure that high-value material is originally authored by humans – quantum of human input to maintain copyrightability is still unclear • Evaluate IP strategy to determine high value areas for copyright
Reputation and integrity – ensuring	• Use of generative AI to create programmatic or	• Set specific guidelines on acceptable use by staff (e.g.,

accuracy and limiting bias	other content for use by specialty societies • Use of generative AI for web-based and social media content to keep specialty societies' online presence constantly updated • Use of AI in hiring processes (differentiate between creating job descriptions and selecting candidates)	use of AI to simply review or edit material, versus original generation) • Require human review of ***all*** content exported by LLMs to ensure accuracy and avoid bias • Ensure any AI tool used by HR in hiring processes is fully vetted by IT and Legal.
IT security and privacy	• Any use of AI tools, especially unauthorized use, or use of tools not examined by IT and Legal departments • Data and document retention by AI tools • Private data input into LLMs	• Take proactive steps to ensure that all staff know that only reviewed and authorized AI tools may be used. IT and Legal must carefully review terms of service for any product. Products should be used pursuant to paid licenses. • Ensure that all licensed AI products have clearly delimited data/document retention policies consistent with specialty society overall policies for document and data retention and destruction. Especially relevant for meeting transcription tools. • Presumption should be that sensitive data (membership, PHI, etc.) ***never*** is placed into an LLM. Exceptions may be

		granted where IT and Legal have reviewed the proposed use as well as the proposed tool and are assured that TOS are sufficient to protect data and comply with all relevant laws (including but not limited to CAN-SPAM and HIPAA).