Ballad Health
Guidelines for Use of Public or Personal AI Platforms

These Guidelines govern the use of publicly available or personal artificial intelligence (AI) platforms by team members when conducting company business. These Guidelines apply in all circumstances where the organization's approved internal AI platform is not utilized and are intended to safeguard Protected Health Information (PHI), confidential information, and other sensitive or regulated data.

- Public and personal AI platforms shall be treated as unsecured, external third-party environments.
- No information entered into such platforms shall be presumed confidential, private or compliant with applicable healthcare privacy and security laws.
- Team members are strictly prohibited from entering, uploading, transmitting or otherwise disclosing any of the following information into public or personal AI platforms:
  - Protected Health Information (PHI), as defined under HIPAA
  - Individually identifiable health information in any form
  - Patient, member or beneficiary data
  - Confidential or proprietary organizational information
  - Trade secrets, clinical protocols or internal methodologies
  - Nonpublic financial, strategic or operational information
  - Vendor, payer or contractual information
  - Attorney-client privileged or work product materials
  - Internal reports, communications or documentation not approved for external disclosure
- Public or personal AI platforms may be used solely for low-risk, nonsensitive purposes, including:
  - Drafting generic, nonconfidential content
  - Summarizing publicly available information
  - Ideation or general productivity assistance

  Such use is permissible only where no PHI, confidential or proprietary information is included or reasonably inferable.

- Team members remain solely responsible for all content generated, utilized or disseminated, regardless of source or AI involvement.
- The following activities are expressly prohibited:
  - Use of AI tools to process or analyze PHI outside approved systems
  - Reliance on AI outputs for clinical decision-making without appropriate professional validation
  - Use in connection with patient diagnosis, treatment or care coordination via public platforms
  - Inputting organizational data for testing, experimentation or training purposes
  - Circumventing established privacy, security or IT controls
  - Generating or disseminating inaccurate, misleading or noncompliant content
- Use of AI tools must comply with all applicable information security policies. Workforce members shall not:
  - Use personal accounts in a manner that stores or transmits organizational data externally
  - Enable integrations, plugins or extensions that introduce unauthorized data sharing
- Any actual or suspected disclosure of PHI or confidential information to a public or personal AI platform must be:
  - Reported immediately to Compliance, Privacy and Information Security
  - Treated as a potential security incident and evaluated under breach notification requirements

  Failure to timely report an incident may result in disciplinary action and regulatory exposure.
- The organization reserves the right to monitor, audit and review usage of AI tools on organizational systems and devices. Adherence to Ballad Health policies applies and failure to adhere to these Guidelines and Ballad Health policies may result in disciplinary action, up to and including termination of employment, and may subject the individual and the organization to civil and criminal penalties under applicable healthcare laws and regulations.
- Any exceptions to these Guidelines must be approved by Corporate Compliance and Legal.