Grokker GrokkyAi™ Safety & Security FAQ

Data Collection and Usage:

1. What personal information will it collect?

Grokky is designed to minimize the collection of personal information. It will not collect a member's name, age, health conditions, location, or benefit enrollment details.

While Grokky won't directly collect this information, the chatbot may leverage anonymized user conversations, app usage data, and member benefits eligibility data.

2. How will this information be used?

The information collected is used to enhance the member experience. Grokky leverages anonymized conversations and app usage data to improve the overall quality of the responses. Grokky also leverages member benefits eligibility data to provide more personalized member benefits guidance.

3. Will this information be shared with any third parties?

Grokker may share aggregated and anonymized data about Grokky usage with our partners to help improve the overall experience. However, Grokker never shares any personally identifiable information or data that could be considered sensitive.

In the case of enterprise users, Grokker adheres strictly to the data retention and deletion requirements outlined in the contracts with their customers. This ensures that member information is handled securely and follows the customer's company policies.

The information collected may be shared with third parties in an anonymized and aggregated format for purposes such as analytics, technical support, and research, but never in a way that could identify or compromise any individual user.

4. How long will this information be retained?

Grokker retains chatbot conversations for a limited time to improve user experience but never uses personally identifiable or sensitive information. Benefit eligibility data (for enterprise members) is stored securely and is not used for AI training, but rather as context for active chat sessions.

5. What measures are in place to ensure the accuracy and integrity of the data collected?

Grokker ensures data accuracy and integrity through anonymization, secure storage, strict data handling procedures, and regular monitoring and audits, safeguarding both member privacy and the quality of the data collected.

6. How will Grokky handle sensitive health information or mental health concerns?

Grokky is not designed to handle sensitive health information or mental health concerns. If you share such information, it will not be stored or used to train the AI model. We strongly encourage you to seek help from qualified healthcare professionals for any sensitive health or mental health issues.

7. What measures are in place to ensure Grokky provides accurate and safe information and recommendations?

Grokky prioritizes providing accurate and safe information by curating its responses from Grokker's trusted content library, actively monitoring its performance, encouraging user feedback, and continuously improving its capabilities.

8. Will Grokky be able to connect users with human support or resources if needed?

While Grokky is designed to be a helpful and informative resource, it cannot directly connect users with human support or resources at present. However, if you require further assistance or have concerns that Grokky is unable to address, you can always reach out to Grokker's designated support channels.

9. How will Grokky maintain user privacy and confidentiality when recommending benefits or connecting users with resources?

Grokky prioritizes user privacy and confidentiality by anonymizing all interactions, and by providing general benefits guidance. Grokky does not send any specific member information to external resources but rather will guide members so that they may access these resources themselves.

Data Security:

1. How is the data collected by Grokky stored and protected? (e.g., encryption, access controls, secure servers)

Grokker employs robust security measures to protect the data collected by Grokky. All data is encrypted both during transmission and at rest, safeguarding it from unauthorized access. Strict access controls limit data handling to authorized personnel only.

Data is stored on secure servers hosted by Amazon Web Services (AWS), adhering to top-tier security standards. When data is no longer needed, it is destroyed securely. These combined efforts ensure the confidentiality and protection of member information.

2. What measures are in place to prevent unauthorized access, use, or disclosure of the data?

Grokker employs robust security measures to prevent unauthorized access, use, or disclosure of member data. Grokker begins by storing all data on secure servers hosted by Amazon Web Services (AWS), which implements industry-leading physical and technical safeguards to protect against unauthorized access.

In addition to secure storage, Grokker utilizes encryption both in transit and at rest. This ensures that even if data were to be intercepted or accessed without authorization, it would remain unreadable and unusable. Grokker further minimizes the risk of internal breaches through strict access controls, limiting data access to authorized personnel only.

To proactively identify and address any potential vulnerabilities, Grokker conducts periodic security audits and employs continuous monitoring of its systems. Grokker also prioritizes employee training on data security best practices and our specific information security policies, fostering a culture of security throughout the organization.

Finally, Grokker maintains a comprehensive incident response plan to ensure a swift and effective response to any potential data breaches, minimizing any potential impact. These measures collectively create a robust security framework that safeguards your data against unauthorized access, use, or disclosure, ensuring member privacy and maintaining the confidentiality of member information.

GrokkyAI Safety & Security FAQ

(continued)

3. **What is the incident response plan in the event of a data breach or security incident?**

   Grokker has a comprehensive incident response plan to address any data breaches or security incidents. Grokker's dedicated Computer Incident Response Team (CIRT) is trained to handle such events, following a well-defined process to contain, assess, eradicate, and recover from any security threats.

   The plan includes procedures for each phase of the response, from identifying the breach to implementing preventative measures for the future. Grokker prioritizes transparency and compliance by notifying impacted parties, including card brands, banks, and legal authorities, when necessary. We also conduct regular reviews and tests of our plan to ensure its effectiveness.

   Grokker is committed to protecting member data and takes proactive measures to safeguard member privacy. In the unlikely event of a breach, Grokker has a robust plan in place to respond swiftly and effectively, minimizing any potential impact.

4. **Is Grokky HIPAA Compliant?**

   Grokky is not designed to handle Protected Health Information (PHI) as defined by HIPAA and is therefore not subject to HIPAA compliance. However, Grokker's security measures already prioritize general data security and confidentiality and are on track to formally establish HIPAA compliance in the near term.

User Control and Transparency:

1. **Can users access, review, and correct their personal information?**

   Grokker prioritizes member privacy and allows members to access, review, and edit some of their personal information directly through the platform. However, certain enterprise member information might be managed by their employer and not be accessible to them through Grokker.

2. **Can users delete their personal information and account?**

   Yes, members have the right to delete their personal information and account. Members can submit a request through the Grokker platform or contact Grokker's support team directly.

   Please note that deleting a member account will permanently remove member data, including any personalized settings or preferences.

   For enterprise members, some data may be retained by their employer per their data retention policies and contractual agreements with Grokker.

3. **How will users be notified of changes to the privacy policy or data practices?**

   Members will be notified of any changes to the privacy policy or data practices through prominent notifications within the Grokker platform and via email. The updated policy will also be readily available on the Grokker website for review at any time.

4. **Will users be able to opt-out of certain data collection or usage practices?**

   Grokker prioritizes member privacy and offers options to control data practices. While Grokker doesn't share personally identifiable information, members can request anonymization of their chatbot conversations.

AI and Algorithm Transparency:

1. **How does Grokky's AI algorithm work? (in a way that is understandable to the average user)**

   Grokky uses a blend of AI-powered decision-making and a vast knowledge base of curated Grokker wellness content training data to provide members with a uniquely sophisticated chat experience. When a member asks a question, Grokky first determines if the member needs a video recommendation, information about benefits, or both. Then, Grokky searches its library for the most relevant content to match the member's query. Finally, Grokky uses advanced generative language capability to present the information clearly and helpfully.

   Grokky is designed to act as a knowledgeable assistant who understands the individual member's needs and quickly finds the right resources to support their well-being.

2. **What factors does the algorithm consider when recommending benefits or content?**

   Grokky's algorithm considers the semantic meaning of a user input AND benefits available to the user, then maps that to the best benefit. In the case of videos, it considers the semantic meaning of the user input AND tries to convert this semantic meaning into specified filters (such as topics) to search through content.

3. **How can users provide feedback on Grokky's recommendations?**

   Users can rate a response as helpful via the thumbs-up and thumbs-down features on the chat UI. We can incorporate a 'report answer' option, for users to provide in-depth feedback about a particular response.

4. **What measures are in place to prevent bias or discrimination in Grokky's responses or recommendations?**

   Our AI team monitors the results for accuracy and bias. We've established a process where designated team members review a sample of interactions weekly and we encourage users to provide feedback directly through the chatbot interface. This helps us identify any inaccuracies and make improvements in real-time. Our team is composed of individuals with diverse backgrounds and experiences. We believe this diversity of perspectives helps us identify and mitigate potential biases in the chatbot's responses. We provide regular training to our team on recognizing and addressing bias in AI. This helps us maintain a high level of awareness and sensitivity to potential issues. Our team monitors the chatbot's performance to some degree. We all share a responsibility for ensuring the chatbot is fair, accurate, and helpful. We conduct periodic reviews of a sample of interactions.