Responsible Use Policy for Avante AI (Carly)

PURPOSE

This policy establishes guidelines for the responsible use of Avante AI (Carly) to support employees with benefits-related inquiries while ensuring compliance with data privacy, security, confidentiality, and responsible AI use requirements.

SCOPE

This policy applies to all employees who access Carly and to Benefits and Legal personnel who administer, review, audit, monitor, or support the platform. Access rights are role-based and limited to approved business purposes.

POLICY

3.1 Access and Interaction Channels

Employees may access Carly through approved channels including the web application authenticated via SSO and Microsoft Teams. The benefits mailbox is not an employee-facing access point and does not provide direct employee access to Carly.

3.2 Data Protection and Privacy Controls

Carly is trained exclusively on approved benefits plan documents and policies maintained by the Benefits team. All interactions are logged for audit, quality assurance, security, and compliance purposes. Benefits personnel with access to employee inquiries must complete applicable confidentiality and privacy training, including HIPAA-related requirements where applicable.

Employees must not enter: detailed medical diagnoses, treatment records, or clinical notes unless necessary for an authorized benefits inquiry; Social Security Numbers or government-issued identification numbers; bank account, credit card, or other financial account information; or information unrelated to benefits administration or plan interpretation.

3.3 Accuracy and Limitations

Responses are informational only. Carly does not provide medical, legal, tax, financial, investment, or employment advice; does not make eligibility determinations; and cannot modify plan terms. Official plan documents govern in all cases.

3.4 Human-in-the-Loop Workflow

For benefits mailbox inquiries, Carly may generate draft responses. Benefits personnel must review, validate, edit as needed, and approve responses before sending them to employees. AI-generated content must not be sent without appropriate human review.

3.5 Acceptable and Permitted Use

Employees may use Carly to understand company benefit plans, coverage provisions, eligibility rules, and benefits-related policies. Benefits and Legal personnel may use Carly for approved support, quality review, auditing, and compliance activities consistent with their roles.

3.6 Prohibited Uses and Guardrails

Attempting to access, infer, or report another individual's personal, medical, benefits, employment, or sensitive information.
Using Carly to make employment, compensation, eligibility, or benefits determinations.
Using identified employee information for analytics, reporting, or monitoring unless expressly authorized and legally permissible.
Circumventing privacy, security, access, or audit controls.
Requesting aggregate results that could reasonably identify an individual or small group.

Employee Guardrails for Using Carly

Do Not Ask for Clinical or Medical Advice.
Do Not Attempt to Make Plan Changes or Enroll.
Do Not Use Carly for General HR or Payroll Tasks.

Benefits Team Guardrails

Validate AI-generated responses before sharing them with employees.
Do not rely on Carly as the sole source for final eligibility, claim, or coverage determinations.
Use the minimum employee information necessary to address an inquiry.
Do not use Carly outputs to create employee profiles, rankings, monitoring, or workforce decisions.
Report suspected privacy, security, or accuracy issues through established channels.

Legal Team Guardrails

Access identified logs only when required for legal, regulatory, investigative, or compliance purposes.
Use de-identified data whenever feasible for reviews and audits.
Do not use Carly outputs as a substitute for legal analysis or legal advice.
Ensure reviews comply with privacy, retention, litigation hold, and data-governance requirements.
Monitor for misuse, inappropriate access, and potential privacy risks.

3.7 Access to Data

Access is limited to authorized Benefits and Legal personnel. Routine audits should use aggregated or de-identified data where feasible. Identified logs are restricted and available only when required for legitimate legal, compliance, or investigative purposes.

3.8 Governance, Approval Process, and Retention

The Benefits Team is responsible for approving user access to Carly and related administrative functions.
The Benefits Team is responsible for approving, maintaining, and updating the benefits plan documents, policies, and other approved source content used by Carly.
The Benefits Team, in conjunction with the Digital Employee Experience Team and/or the Architecture Review Board, must review and approve material configuration changes, integrations, functionality enhancements, and other changes that may impact system behavior, user experience, privacy, security, or data processing.
The Privacy Legal Team must review and approve any exceptions to this policy.
All records generated through Carly will be managed in accordance with the Company's Data Retention Policy and applicable legal, regulatory, privacy, and information governance requirements.

Subject to applicable retention schedules, Avante and/or the Benefits Team will retain chat logs, audit logs, and mailbox-generated draft responses.
Access to retained records will be restricted to authorized personnel.

4.0 Auditing and Monitoring

Benefits will conduct periodic accuracy audits. Audits will evaluate accuracy, consistency, privacy compliance, access controls, and potential risks. Reporting should be aggregated and de-identified whenever possible.

5.0 Disclaimer

Statements made by Carly do not constitute a formal benefit determination and do not alter the terms of any company policy or benefit plan. In the event of a discrepancy, official company documents govern.

DEFINITIONS

Carly: Avante AI benefits assistant. Policy Owner: Sr Director Global Benefits. EVP Approver: Chief People Officer. Authorized Personnel: Individuals with approved access rights.

RESPONSIBILITIES

Policy Owner: Sr Director Global Benefits. Maintain content, review outputs, approve mailbox responses, conduct audits, and oversee governance. Legal: Oversee compliance, review identified logs when required, and advise on privacy and regulatory obligations. Employees: Comply with all requirements of this policy.

ENFORCEMENT

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Benefits and Legal may monitor compliance and conduct audits.

EXCEPTIONS

Exceptions to this policy are to be avoided. Any exception related to data access, data use, retention, privacy controls, security controls, or governance requirements must be reviewed and approved by the Privacy Legal Team.

DOCUMENT MANAGEMENT

This document is subject to enterprise policy management processes governing approval, communication, acknowledgement, publication, review, and revision. Review frequency: at least every three years. Policy Owner: Sr Director Global Benefits. EVP Approver: Chief People Officer. Policy acknowledgement determination: Required. This policy addresses AI, privacy, confidentiality, and employee benefits risks and employees may be required to acknowledge receipt and compliance.

RELATED POLICIES & PROCESSES

Enterprise AI Policy
Privacy Policy
Data Retention Policy
Code of Conduct

Revision History and Approval

Rev #	Revision Date	Description	Policy Owner	SVP Approver	Approval Date

1	June 23, 2026	Initial Responsible Use Policy	MaryBeth Kramer, Sr Director Global Benefits	Emily Del Toro, SVP, Total Rewards	June 30, 2026