BCBS (Blue Cross Blue Shield) AI Use Policy

1) Purpose

This policy will outline the standards and expectations regarding the Blue Cross Blue Shield (BCBS) AI in order to ensure secure database management. The implementation of AI at Blue Cross will allow for employees to increase productivity, improve patient services, and aid in decision making, while safeguarding protected health information (PHI). By enforcing constraints according to user type and establishing security boundaries, BCBS will improve operations while minimizing the likelihood of cybersecurity incidents.

2) Scope

The BCBS_AI serves as a secure information and decision-support system that enforces role-based access controls to ensure sensitive healthcare and insurance data is only accessible to authorized users and will deny or escalate any requests out of a user's authorized scope. Patients access the AI through authenticated accounts with required multi-factor authentication, while employee access is restricted to authorized BCBS-managed devices.

Insurance provider:

- Claims
- Coverage
- Billing info
- Patient identifiers
- Plan details
- Limited to assigned claims only

Doctors:

- Current patient records
- View and update patient medical records
- Updates are logged and auditable

IT/Admin:

- Logs
- system health
- security controls
- **NO PHI**

Patients:

- Access their own medical info
- Their own Billing info
- Submit Update requests (no direct record edits)

3) Definitions

Authorized User

BCBS employees that have been formally approved access to AI systems and databases based on user type

BCBS_AI

The approved artificial intelligence system authorized by Blue Cross Blue Shield for internal use.

HIPAA

The Health Insurance Portability and Accountability Act, which governs the protection of patient health information**.**

Patient Identifiers

Information that can identify a patient, including policy number, date of birth, or member ID.

PHI (Protected Health Information)

Individually identifiable health information related to a patient's care, condition, or payment for healthcare services.

PII (Personally Identifiable Information)

Information that can identify an individual, such as name, address, email, or phone number.

Insurance Claim

A request submitted to BCBS for payment or reimbursement of healthcare services provided to a member.

Documentation

Clinical, administrative, or operational records related to patient care, insurance processing, or internal business function**s.**

Role-Based Access Control (RBAC)

A security method that restricts system access based on a user's role and authorized scope.

Human Review

The required evaluation of AI-generated output by an authorized individual before use or distribution.

4) Policy Position

BCBS authorizes the use of BCBS AI for supporting business, administration, and healthcare related operations.

The use of BCBS data in other unauthorized AI tools or sites is forbidden in order to secure PHI under HIPAA regulations

Authorized users are responsible for the content generated through approved AI systems

5) SAFE LANE Rule (Quick Decision Test)

AI use is permitted only when all three conditions are met:

- Approved Tool — BCBS_Ai is used. No other AI tools are permitted for BCBSwork.
- Approved Data — No prohibited or non-public BCBS information is entered.
- Appropriate Review — Outputs are reviewed when required before use or sharing.
- Role-based approval — is this input appropriate for the user
- Role_base retrieval — what role does the user have

If any condition is not met, Authorized Users MUST sanitize inputs, use an approved non-AI workflow or avoid AI for that task

6) Prohibited Inputs

General (all users regardless of role):

- Large-scale data extraction
- Attempts to manipulate the AI
- Requests to bypass MFA,security controls, or authentications
- Requests to act on behalf of another user
- Requests for login credentials outside of users

Insurance provider:

- Requests for any medical/clinical records
- Requests to view full patient history
- Requests for anything outside information within assigned claim
- Requests to approve/deny claims outside assigned workload

User:

- Requests for patients data outside users scope
- Requests to access other patients medical or billing information
- Requests Bulk data requests or any attempts to bulk export large data
- Requests to export data outside user scope
- Requests for system configurations, credentials, or internal logs
- Any requests to try and bypass security controls put into place
- Requests to change records directly instead of submitting requests
- Requests to view internal notes or provider comments

Doctor:

- Request for patients info outside their current patients

- Requests for patient billing information
- Requests to export any patient medical info
- Requests to gain access to other users login credentials
- Requests to access historical patients without an active relationship
- Requests to perform bulk searches across patients

IT/Admin:

- Requests for any patient medical information
- Requests for Doctor login credentials
- Requests for Billing information
- Requests to alter access logs
- Requests to grant themselves elevated data access

Authorized users must not enter the following into BCBS_AI

Patient or Personal Identifiers (PHI/PII) (Exception for doctors)

• Patient names, dates of birth, and medical record numbers
• Identifiable clinical notes, lab results, or patient portal communications
• Employee or customer identifying information

Security or Internal System Information (Exception for It/admin)

• Passwords, MFA codes, encryption keys, access tokens
• Network diagrams, server names, or system configurations
• Security logs, audit reports, and incident investigations

7) Permitted Uses

Permitted uses of BCBS_AI vary based on the role of the user. The system will only allow actions and requests explicitly listed in this section and will deny any use outside an individual's authorized role.

Insurance provider:

- Access patient claims
- Insurance provider accepts or denies claims
- Send billing information
- Look at account info
- Manage account credentials(MFA required)
- Review claim details and identify missing documentation
- Interpret coverage and eligibility rules

- Draft explanations of benefits (EOBs) for members
- Process claims
-

Doctors:

- Access their own patient medical records
- Review and approve/reject update requests
- Document care
- Submit clinical information
- Send in claim requests for patients for care
- Manage account credentials(MFA required)

It/admin:

- Monitor system care
- Monitor AI logs and audit trails
- Manage user roles and permissions
- Incident response and compliance reviews
- Implement security controls
- Review Security controls
- Manage account credentials(MFA required)

Patient:

- View their own medical records
- View claim status and billing information
- Requests updates or coverage explanations
- Manage account credentials(MFA required)

8) Required Human Review

All high-risk or sensitive BCBS_AI outputs require review before use in cases where the content involves:

Insurance provider:

- Review billing information
- Review claims

Doctor:

- Review medical records of their own patients
- Review update requests
- Review documentations

It/admin:

- Review logs
- Review Security breach attempts
- Review malicious attempts to manipulate AI

Patient:

- Review their own account information
- Ask questions about their coverage
- Patient should not be able to review anything else

9) System Safeguards

When using BCBS_AI, users must authenticate with a valid username and password, followed by multi‑factor authentication (MFA) prior to accessing the system. Upon successful authentication, BCBS_AI verifies the user's scope and enforces role‑based permissions to ensure access is limited to authorized functions and data. All AI interactions are logged for audit and monitoring purposes, and the system actively flags unusual or potentially malicious requests for review by the IT department. User sessions automatically terminate after 15 minutes of inactivity to reduce unauthorized access risk. Encryption is enforced at all stages of data handling, including data in transit, at rest, and during use.

10) Incident Reporting:

Any suspected or confirmed malicious attempts to manipulate, misuse, or compromise BCBS_AI must be promptly investigated to protect the security and integrity of the system. All AI activity logs are retained to support incident analysis and are made available to the IT/Admin team for review. During incident reporting and investigation, logs and reports will be handled in a manner that prevents the exposure of personally identifiable information (PII) or protected health information (PHI) to unauthorized personnel. Appropriate corrective actions will be taken to mitigate risk, prevent recurrence, and ensure the continued protection of user data.

11) Monitoring

BCBS_AI is continuously monitored to detect the entry or attempted entry of prohibited information, including unauthorized PHI, PII, or system-restricted data. If prohibited information is entered or suspected to have been entered into BCBS_AI, authorized users must immediately cease further interaction with the system, notify the Information Security and Privacy/Compliance teams, and follow all containment and remediation instructions provided. Monitoring mechanisms include automated alerts, audit log reviews, and anomaly detection to identify potential misuse, policy violations, or security incidents.

12) Consequences of Noncompliance

Failure to comply with this policy may result in corrective actions, up to and including access suspension, mandatory retraining, disciplinary action, or termination of access to BCBS_AI. Violations involving the misuse of AI, unauthorized access to data, or exposure of protected health information (PHI) or personally identifiable information (PII) may also result in escalation to Information Security, Privacy/Compliance, or Human Resources for further investigation.

BCBS reserves the right to take additional action as required to protect system integrity, data security, and regulatory compliance.

13) Acknowledgment

All authorized users of BCBS_AI are required to acknowledge that they have read, understood, and agree to comply with this policy prior to being granted access to the system. Continued use of BCBS_AI constitutes ongoing acceptance of the terms and responsibilities outlined in this policy. Failure to acknowledge or adhere to this policy may result in revocation of access.