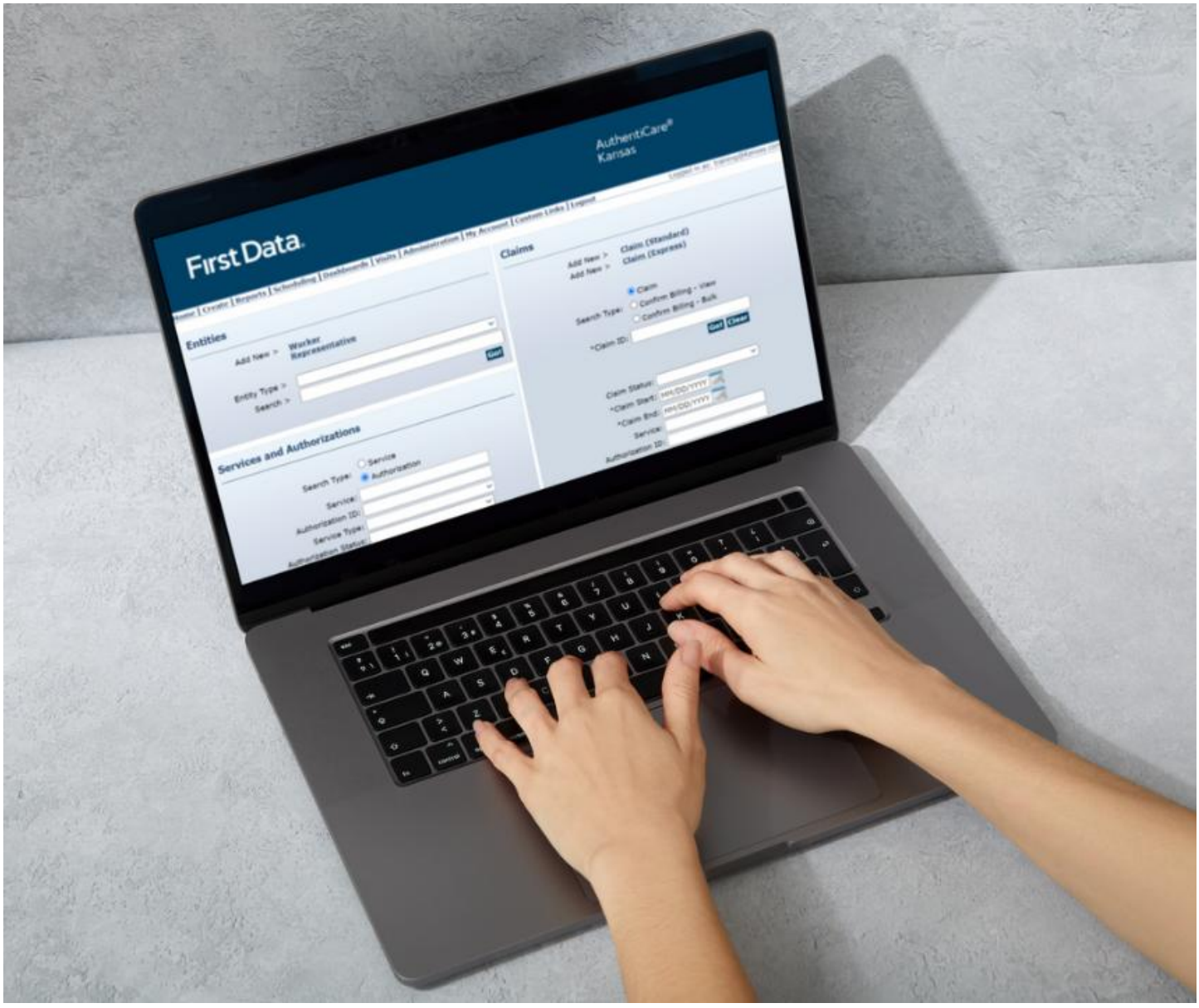

Mobile Security

AuthentiCare® 3.0

Last Updated: 3/16/2026

Welcome to AuthentiCare 3.0!

1.0 Executive Security Overview

AuthentiCare Mobile 3.0 employs layered security controls, “defense in depth”, designed to protect application access, data, and system integrity following the NIST 800-53 R5 standard.

These controls include encrypted communications, secure application development practices, authenticated access, device binding, vulnerability management, and formal governance processes.

The application has been developed and maintained in alignment with industry standards, including HITRUST, HIPAA, OWASP and NIST.

Secure code best practice, security testing, change management, and audit logging are embedded throughout the application lifecycle to ensure ongoing protection, traceability, and compliance.

Fiserv, performs annual, independent third-party audits for AuthentiCare and related systems to demonstrate our commitment, due diligence and dedication to security, compliance and privacy.

Our annual independent third-party audits include but are not limited to: SSAE18 (SOC 2), and our HITRUST R2 certification, current until 2027.

1.1 Secure Development & Vulnerability Management

AuthentiCare Mobile 3.0 has been developed and maintained using the Fiserv Secure Application Development process, which aligns with HITRUST, HIPAA, OWASP and NIST standards.

For AuthentiCare Mobile 3.0, security testing was performed by trained Fiserv personnel and approved third-party assessors prior to production release and at least annually thereafter.

Security reviews, peer code reviews, and vulnerability testing are embedded throughout the software development lifecycle and combine automated scanning tools with manual analysis.

Fiserv utilizes a comprehensive, risk-based, information security risk assessment tool and process. The application certification and approval process is required to assess information risk for all applications across the globe, including internal applications and those that are exposed to the internet.

Assessments are performed prior to production, when changes in the application or

infrastructure are required, and/or on a periodic basis that is determined by the residual risk of the application.

Industry-standard testing methodologies were performed for Mobile 3.0, including Static (SAST), Dynamic (DAST), Interactive (IAST), and Mobile Application Security Testing (MAST), which are used to identify and remediate vulnerabilities.

No critical and high-severity findings were found prior to deployment.

1.2 Transport & Communication Security

AuthentiCare Mobile 3.0, enforces secure communications through the use of Transport Layer Security (TLS) encryption to protect data in transit and HTTPS. Certificate pinning has been implemented to prevent man-in-the-middle attacks and ensure communications are established only with trusted endpoints.

These controls are consistently applied across supported platforms, including iOS, Android, and MAUI, to maintain secure and encrypted transport for all application communications.

1.3 Authentication, Access Control & Device Security

Access to AuthentiCare Mobile 3.0 requires MFA, authenticated user credentials and is restricted to authorized workers only.

The application enforces device binding through unique device identifiers to limit access to registered devices.

Additional access controls include environment separation, NIST password requirements, and mandatory acceptance of an End User License Agreement (EULA) prior to use.

These measures help ensure that only approved users on trusted devices can access application functionality and data.

1.4 Data Protection & Offline Controls

AuthentiCare Mobile 3.0 supports controlled offline data capture to accommodate field operations while maintaining data security.

Data collected while offline is securely stored on the device and transmitted using encrypted communications once network connectivity is restored.

Store-and-forward controls ensure data integrity and confidentiality during temporary loss of connectivity.

Data in transit is encrypted with TLS 1.2 and Data at rest is encrypted with AES 256 bit encryption.

1.5 Governance, Change Management & Auditability

All security-related changes to AuthentiCare Mobile 3.0 have been managed through the Fiserv Change Management processes. Approved source code changes were formally submitted, reviewed, and authorized prior to deployment.

Changes were logged in accordance with Cyber Security Logging and Monitoring Standards to support traceability, accountability, and audit readiness.

Fiserv information resources (for example, networks, applications, systems and others) followed formal change control procedures to ensure that only authorized changes are committed to production.

Change control procedures include:

- Identification and recording of significant changes
- Planning and testing of changes
- Assessment of the potential impacts, including security impacts, of such changes
- Approvals for proposed changes from application, system or business owners
- Communication of change details to all relevant persons
- Implementation and Backup procedures

1.6 Client-Facing Security Communication

AuthentiCare Mobile 3.0 communications to state and client stakeholders are through annual independent 3rd party audit reports, the plan of action/milestone (POAM), and security documentation.

These materials are provided as part of release, conversion, and governance activities to support transparency, assurance, and informed decision-making regarding application security controls and practices.