Electronic Validation of Consumer Consent

Quick Reference Guide

United Healthcare®

Electronic Validation of Consumer Consent

To protect consumers and meet regulatory expectations, UnitedHealthcare requires specific evidence any time consumer consent is captured electronically ("e-consent"). Please review the recommendations below and confirm your systems and processes align before assisting consumers or transmitting data to us.

The following key elements are recommended to be electronically captured to support validation of consumer consent and confirmation of eligibility application documentation.

1. Audit Trail

Your logs should show the following to demonstrate valid consent:

- **Who** gave consent (consumer identifier/account), and who administered any related configuration
- **What** happened (event type like consent given), including the exact consent text version
- **When** it happened (server generated UTC date-stamp)
- **Where** it occurred (hosting environment/service name and consumer IP)
- **How** it was processed (the consent pathway and relevant service calls)

Audit trails must be **tampered evident**, protected from modification, and included in routine backups/archives so they can be produced on request.

2. Exact date-stamp (UTC)

Use a standardized format (UTC with offset or epoch). Date-stamps must be created by your server and consistent across services.

3. Originating IP address

Record the consumer's IP at the time consent is given. If available, also record the device or host name.

4. User identity & session context

Save the authenticated user ID (if applicable), session ID, and whether multifactor/One-Time Passcode (OTP) was used.

United Healthcare®

5. Device/browser details

Capture the user agent string (browser/app, OS, version) sufficient to distinguish the client environment.

6. Consent interaction details

Log the specific action (e.g., “checkbox checked,” “Agree clicked,” name typed, OTP entered), including the page/view and the UI element or event name.

7. Consent text & version

Store the exact wording shown to the consumer (version number) and, preferably, a cryptographic hash (e.g. digital fingerprint or unique identifier) to prove the content has not been altered.

8. Unique transaction ID

Assign a unique identifier that ties all evidence to the single consent event and appears on confirmations/receipts.

9. Consumer visible receipt

Provide a receipt (PDF/HTML) or confirmation email that references the unique transaction ID. Do not expose internal routing or system details to consumers.

Retention, security, and access

- **Retention:** Agents, brokers, and web-brokers operating in the Federally-Facilitated Marketplace (FFM) and State-Based Exchanges on the Federal Platform (SBE-FPs) or assisting an individual with applying for advance premium tax credit (APTC) or cost-sharing reduction (CSR) are required to retain and maintain consumer consent documentation for at least 10 years, and made available upon request in response to monitoring, audit and enforcement activities. Archived audit logs must remain searchable and retrievable

- **Access controls:** Limit access to authorized personnel only; maintain separation of duties (operations vs. review)

- **PII protection:** Encrypt in transit and at rest; share on a strict “need-to- know” basis; never send PII in unsecured channels. Report suspected incidents promptly per regulatory and contractual obligations. Refer to the Privacy and Security section of our IFP Compliance Page in ***Jarvis***

United Healthcare®

Common pitfalls to avoid

- **Do not** rely on consumer-side time or editable fields for timestamps
- **Do not** store consent evidence only in screenshots or emails—keep structured, searchable logs
- **Do not** commingle consent records with unrelated logs without clear identifiers; ensure easy retrieval
- **Do not** substitute marketing opt-in language for legal/transactional consent—version your consent text and keep hashes to verify that files have not been tampered with or altered

Public references and resources

- **CMS: Frequently Asked Questions: Consumer Consent & Application Review Requirements (June 12, 2024)**
  cms.gov/files/document/frequently-asked-questions-consumer-consent-application-review-requirements.pdf
- **CMS: Statement on System Changes to Stop Unauthorized Agent and Broker Marketplace Activity (July 19, 2024)**
  cms.gov/newsroom/press-releases/cms-statement-system-changes-stop-unauthorized-agent-and-broker-marketplace-activity
- **CMS: FAQs for Marketplace Agents and Brokers**
  agentbrokerfaq.cms.gov/s/