ATTACHMENT C

AGENCY TERMS

SOLICITATION NO. 0900000477

C.1. Project Description/Scope

C.1.1. The objective of this RFP is to obtain a Supplier to provide a user-friendly healthcare fraud analytics system that Compliance Analysts can utilize to identify potential FWA in HealthChoice claims, which includes case tracking, ability to query by patient, provider and service, offer customizable dashboards to fit our needs and provide support services.

C.1.2. Supplier's system should have capability to identify and analyze improper claims for purposes of fraud detection and prevention across the HealthChoice medical, dental and pharmacy claims data through preprogrammed analytic models.

C.1.3. Supplier's system shall identify inconsistencies and "rule-breaking" behaviors by providers and patients, learn from fraudulent patterns and scenarios and adapt predictive algorithms against emerging schemes as industry patterns are discovered.

C.1.4. Supplier's system should identify behavior changes in an individual patient or provider, identify normal "spikes" (e.g. a provider seeing more patients during the flu season or the COVID pandemic) as well as "abnormal spikes", include provider risk scoring based on claims, billing and other pertinent data, flagging high risk providers for analyst reviews.

C.1.5. Supplier's system should include a user-friendly dashboard to manage workloads and predefined work queues.

C.1.6. Supplier's system should allow for customizable edits and include provider peer comparisons and risk scores, and capability to identify the following: duplicate claims, procedure bundling, irregularities between coding combinations; procedures to diagnosis mismatches, Excluded Individuals and Entities, invalid or deactivated NPI numbers, charges significantly above or below geographic and/or national norms, incorporate National Correct Coding Initiative (NCCI) data rules, geospatial data visualization, link analysis .

C.2. Training and Support Services

C.2.1. The Supplier shall provide user training prior to implementation and offer ongoing support.

C.2.2. The Supplier shall provide access for a minimum of 8-10 users.

C.2.3. The system should have permission-based access for users.

C.3. Reliability and Stability

C.3.1. System downtime for routine maintenance should be performed with little to no disruption of system availability to users (e.g. weekends, holidays, etc.).

C.4. Backup and Disaster Recovery

C.4.1. Supplier shall have processes for backing up and a disaster recovery plan with policies and procedures in place to control, limit or prevent the transportation and storage of client data on laptop computers, compact discs, flash memory drives or any other portable device.

C.5. Security Encryption

C.5.1. Supplier shall use Pretty Good Privacy (PGP) as its standard encryption application and any encrypted files shall be transmitted over Secure File Transfer Protocol (SFTP). EGID policy dictates that all files at rest must be encrypted.

C.5.2. Email communications shall be sent over Transport Layer Security (TLS) connections.

C.5.3. Supplier shall utilize multi-factor authentication.

C.5.4. Supplier shall complete and sign the Standard Business Associate Agreement (Exhibit 1).

C.6. Quality Assurance

C.6.1. Supplier shall have a quality assurance process the software is run through to ensure the least number of bugs and issues are found in the product in a production environment.