PRELIMINARY ROADMAP

INTRODUCTION

BCC seeks agile software development services under this Request for Proposals and includes by reference the separate RFP Abstract, Executive Summary, and Schedule. The services to be provided will include all aspects of the software development process, including initial planning, design, software development, application integration, integration with networks and third-party systems, security provisioning, and coding, prototyping, documenting, testing, continuous integration, and configuration. BCC intends that the software and technology solutions delivered under this task order will be proprietary as works for hire on behalf of BCC, and they will NOT be committed to the public domain. This software development project will use AGILE development and LEAN principles, with robust documentation, human-centered design, and an extensible infrastructure. BCC expects that the development process will be collaborative and iterative, with open, regular, and frequent communication between BCC and the Contractor.

BCC plans that the development process will consist of weekly sprint cycles, and that the initial phases of the development process will focus on providing identity, credential, and access management (ICAM), OpenID Connect Identity Provider capabilities, biometric patient identification, biometric registration and verification. matching initiation (person, patient, and/or treatment), fee code ascription, financial responsibility management, payment of fees, search functionality, e-signatures, FHIR APIs, patent EHR data and granular requests, physician notes, and content management, as describe below in this preliminary roadmap.

NEXT STEPS: To explore the Deliverables of the RFP, please fill out the following fields, copy, and email them to steve@biometriccare.com under the Subject "RFP Deliverable":

Developer's Name:
Developer's Headquarter Address,
City, State, County:
Developer's email:
Developer's Telephone (Optional):

BCC will send you **a link and access code** for the Deliverables of the RFP and other materials.

Interested Parties ought to look at BCC's RFP Abstract and Executive Summary, if not yet viewed. **BCC's Contact** and Official Website: biometriccare.com Contract Location: California. (8:30 a.m. - 5:30 p.m. PST); email: Steve@biometriccare.com - Please add "RFP" to Subject.

The Contractor will have to obtain BCC permission before delivering software under this task order that incorporates any software that is not free and open source. The Contractor also will have to obtain BCC permission before delivering software under this RFP, Roadmap and Delivery order that incorporates any software that is free and open source, but not licensed under the MIT license. **As this is a preliminary document, like other documents that predate the Agreement under this RFP, it is the Agreement that will govern and control if there is a conflict between any terms arising from earlier published or posted documents, such that conflicts will be interpreted solely under the Agreement.**

The Contractor, not the BCC, will be responsible for the hosting of the deployed System and obtaining any necessary Authority to Operate (ATO). BCC will provide certain written warranties of freedom to operate to the Contractor, with regard to the patent rights that it or its executive management exclusively controls for the purposes of use for BCC under the Agreement.

BCC will also determine what security controls are required and whether they have been satisfied. BCC expects to provide those security controls to the Contractor as either acceptance criteria, Network overlay requirements, or separate user stories. The Contractor is expected to use best practices for security in delivering code.

BCC intends to deploy the new ICAM management operations as soon as the software for the new System has been sufficiently developed to provide the minimal viable functionality required to support an acceptable level of BCC's fundamental biometric patient identification and matching management operations. This minimal viable functionality will include the ability for external users to file documents electronically (including queries, query packaging (i.e., for FHIR APIs, etc.) exchanges, initiation of matching, granular data retrieval and documents), and the ability for internal BCC users to route those filings appropriately, take action on those queries, response, and serve ID and matching results on the parties and their representatives. BCC intends for the software to have been sufficiently developed to allow deployment and conversion by the date for System Deployment in the Schedule. BCC expects that substantial further development of the software and modifications to the System will occur after this deployment and conversion.

General Requirements

System Requirements – The System will be hosted on an agreed upon or certified cloud platform with a storage solution via an account controlled by BCC and its delegated authorities. The System must incorporate an intuitive web-based interface that is accessible from both internal and external platforms, including desktops, laptops, tablets, thin/zero clients, and mobile devices. The System architecture must incorporate Application

Programming Interfaces (APIs) to intermediate major components. The System must have no single point of failure. The System will use elastic, dynamically allocated computing resources that accommodate operations, transactions, and logging along with changing demand in real time. The System must include user authentication and authorization functionality that uses open-source encryption protocols. BCC does not currently have any enterprise authentication/authorization mechanisms that need to be integrated into the new System, but BCC expects these mechanisms to be developed as part of a current System-level user story. The System must be integrated with billing codes, telehealth billing codes, billing, transfers, and payments to enable the receipt of payments or credits/surcredits.

Software Requirements – The software architecture must be extensible to allow for future development. The code base must incorporate analytics, monitoring, continuous integration, and measurement tools. Application design and development must use plain language to the extent practical.

Environments – Contractor as Developer will be responsible for creating, maintaining, and managing an internet-connected staging environment, and an internet connected production environment, on a selected or certified cloud storage solution. The Contractor will be responsible for creating, maintaining, and managing its own internet-connected development environment, which will be a separate environment that the Contractor will deploy to. The Contractor's development environment must mirror its staging and production environments, except that the Contractor's development environment need not be pre-certified beyond best practices for mission critical operations with failover.

User Stories

The set of preliminary user stories set forth below will be the starting point for the development of software to be provided under this task order. These preliminary user stories are provided only for illustrative purposes, and do not comprise the full scope or detail of the project. They have been grouped by topic, but have not been prioritized.

BCC expects that the Contractor will work closely with the Product Owner to perform continuous integration, patient identification, identity verification, patient research, prepare user + group member personas, and to develop and prioritize a full gamut of user stories as the project progresses. BCC also expects that the Contractor will work closely with the Product Owner and BCC-provided end-users to perform usability testing at regular intervals throughout the development process.

Individual user stories may be modified, added, retracted, or reprioritized by BCC at any time, and BCC expects that the user stories will be continuously refined during the development process. Additional user stories will likely cover areas such as patient identification and matching, designations, consent management, delegations, redundancy, network overlays, e-signatures, notes, routing, notifications, calendaring, and reporting and analytics.

The backlog of user stories will be maintained in JIRA or a substitute therefor, a web-based project management application, that will be provided by BCC. The Contractor will be required to manage and update user stories using JIRA.

Current Deliverables and SOWs consist of capabilities, Sprints, Milestones, and diagrams that present the request processing for patient identification and matching workflows that BCC currently expects to eventually be supported by a platform at b-idp.net. The direct and vicarious patient identification and matching process and downstream clinical decision support processing workflows and interoperability with extensibility as set forth below may be revised during the development process.

The sooner BCC's solution gets in the hands of first responders, the sooner our innovation will modernize the high-stakes work of public safety. Created for doctors' and first responders' needs, device usage and rigorous industry expectations, our products will make their communications safer, easier and more direct, even in case of disasters and emergencies.

PATIENT PERSPECTIVE: BCC's RapidVu™ allows me to use myself as my identity solution. I can designate proxies to identify me with biometric if I am unable to do so such as parents, guardians, my health care team members, and medical first responders by name, role, attribute, group, etc. My online biometric telehealth credentials let me to login to my health plan and some third-party websites and apps and to use my health system data for point of care services that require a high level of trust and authenticity. It enables me for EMS to initiate ICE transfers directly via my health system and prove my verified identity to access services that would otherwise require a far slower less elegant verification method,

IDENTITY PROVIDER PERSPCTIVE: The IdP (as OAuth server and OP client) app plays the most fundamental role from the patient's perspective. There is an individual IdP for every health system in the ecosystem of the BCC's RapidVu™ service. The BCC's RapidVu™ service's functionality for the respective patient base will pass-through their own health system's look and feel. The IdP authenticates the patient taking full advantage of existing methods using biometric authentication (or combining biometric authentication and conventional demographic ID) and gathers the patient's consent for any BCC RapidVu™ query or action directly or indirectly, by resolving online telehealth credentials or employing mobile apps capable of receiving messages, alerts, and push notifications.

RP PERSPECTIVE: BCC's RapidVu™ service enables me to easily authenticate and identify our participating patients to share their health or telehealth data set with even new healthcare team members without the need to integrate all health systems separately with my service. RPs include healthcare providers, payers, systems, and qualified intermediaries like QHINs and attribute providers so I get all ONC-mandated services for free, through a single set of FHIR API Specifications and without needing to be certified as a designated data set Information Service Provider (HIPAA ISP for Patient API data), CSP, or Payment Initiation Service Provider (PISP). The same FHIR API Specification allows common means to access health system-verified identity and data sets or subsets even from passive stakeholders that comply with Final Rule API requirements. The RP will typically set up an internal (technical) account to maintain the internal view on the auditable exchange. Moreover, patients can use further BCC's RapidVu™-standardized or third-party services, e.g., to enrich the patient's data by letting my designated representatives identify the patient, access the patient's health records, and sign pre-authorized forms with qualified electronic signatures on behalf of the patient .

SUBCRIBER'S (ACTIVE HEALTH SYSTEM) PERSPECTIVE: BCC's RapidVu™ is deployed over an architecture and framework where, as a subscriber, we keep the patient interface and the ability to authenticate our patients directly to enable supporting the transfer of patient-specific data directly to RPs without the need for third party aggregators, and become the digital master key for our patients. We can share my verified patient and data set data by making it accessible to all RPs and SPs in BCC's RapidVu™ service in compliance with HHS, CMS, and/or ONC mandate using open standards and a well-defined commercial and legal framework provided by BCC.

SP PERSPECTIVE: BCC's RapidVu™ and B-IdP ecosystem comprises a marketplace where I can offer my services that are based on verified patient identities, data and data set data. I can reach a wide range of Relying Parties and other Service Providers and use BCC's RapidVu™ service features as billing partner for my offering.

BCC's RapidVu™ PERSPECTIVE: BCC's RapidVu™ service facilitates the service by managing the trust relationships among IdPs, SPs and RPs. RapidVu™ is BCC's flagship offering and it supports a wide array of interoperable and standards compatible FUNCTIONS AND FEATURES set out in the ROADMAP below. BCC's Federated SSO for B-IdP and Early-Personalized Care determines the FHIR Hub selected and connects RPs and FHIR Hub-presented IdPs (and SPs) on behalf of the patient. The patient determines the health system she wants to use with BCC's RapidVu™ service and this decision is retained in order to provide SSO in subsequent processes even if a strict 3rd party cookie policy is in place. BCC's RapidVu™ service can be used by IdPs and SPs as a gainsharing, billing code provisioning, and clearing platform.

1 ROADMAP: SOLUTION FUNCTIONS AND FEATURES

The BCC has delivered to CONTRACTOR a proprietary "high-level" system description request of BCC to be provisioned as an OpenID Connect Identity Provider with specialized biometric authentication and pre-designated access authorization. BCC's B-IdP.net platform helps healthcare systems personalize healthcare earlier to improve treatment outcomes while reducing improving patient engagement.

RapidVu™ lets providers securely use transformed biometric data for identification at the first point of care (POC) to get summary care records of a patient fast anytime over a scalable mobile or identity-cloud platform (B-IdP.net).

Early-Personalized Care™ informs health professionals earlier via wireless networks of each patient's profile, history, or in-case-of-emergency (ICE) data for targeted treatment (*i.e.,* virtual, on-scene, in-transit, telehealth, transition, or acute care, *etc.*) – anywhere.

Touchless Telehealth™ is the third prong of this internal suite of BCC applications, and it will be provisioned to manage, process, and share confidential or sensitive health-related information for over RapidVu™ and/or Early-Personalized Care™, with security and privacy for regulatory compliance.

By developing Custom Software for BCC, the CONTRACTOR agrees to implement BCC offerings that authenticate patients with transformed biometrics remotely, authorize access critical patient health data by designated proxies acting on behalf of the patient, and match treatments with patient profiles via mobile networks securely across different IT systems. These systems are compatible with BCC software services, including Application Software, Custom Software, Hosted Software, OpenID Connect Identity Provider applications and a set of Identity and Governance Administration (IGA) software or operational modules, as described below, with "(IGA)" designations.

CONTRACTOR has committed to help specify, develop, test, implement, and support BCC's network, firmware, hardware, services, and software that includes without limitation the B-IdP.net platform, key services under trademark, biometric attribute provider capabilities, patient authentication using certain OpenID Connect Identity Provider services using Custom Software and solutions, Designated Proxies acting on behalf of patients, OAuth 2.0 authorizations, as well as IGA modules. Also, CONTRACTOR has agreed to evaluate all third-party equipment interfaces to be compatible in order to ensure that BCC's network would be functional, available 99.99% of the time, and highly scalable like state-of-the-art web services, best of breed mobile networks, extensible distributed databases, and worldwide search engines.

Because the B-IdP.net platform is intended to scale dynamically to support subscribers *as though* BCC's services have been mandated for use by 10,000 health providers or payers, and their patients, by Medicare, it should be configured for dynamic scalability with similarly required or substitutable services. Based on the agreed understanding of the scope of the above, BCC and CONTRACTOR shall further define the specifications, and once defined, CONTRACTOR shall design, develop, test, and implement the Software in accordance with the above Specifications and reconfirm and finally determine "The Deliverables". CONTRACTOR shall use reasonable efforts to deliver the Software to BCC, at the milestone dates as mutually agreed as outlined below in further detail or following the actions the Implementation Schedule below.

The Parties have agreed to hold progress review meetings every two weeks and to adjust staffing as deemed needed by BCC's development manager, based on dialogue with CONTRACTOR's chief engineer.

The CONTRACTOR agrees to design, develop, and implement a solution for BCC, and its exclusive control and use, that comprises certain modules and components that satisfy the following criteria:

A. DESIGN OF COMPUTER SOFTWARE AND NETWORK SOLUTIONS TO SUPPORT BCC'S BRANDED APPLICATIONS

1. The CONTRACTOR will design the solution including without limitations the computer software, network, and service architecture under the following bases:
a. Computer Language. The CONTRACTOR shall design and produce the software using one of the following languages: Java, C#, JavaScript, Python, Ruby or Go. If the

CONTRACTOR recommends the use of any other language, it may request the permission of the Contracting Officer.

b. Open-Source Software Components. To the extent that the CONTRACTOR intends to incorporate open-source content into the computer software, it may use open-source content subject to an open source license that either requires only acknowledgement of the source or the source and a disclaimer of liability. Prior to incorporating open-source content subject to any other license conditions, the CONTRACTOR must request and receive the prior written approval of the Contracting Officer.

c. Commercial or Proprietary Software Components. The CONTRACTOR shall not incorporate into the computer software content that is subject to either commercial or proprietary license conditions without the prior approval of the Contracting Officer.

d. Server Compatibility. To the extent that the computer software is to be designed for loading on a server, the CONTRACTOR shall design the computer software to be operated on at least one of the following server operating systems: Linux (Kernel version 4+), Microsoft Windows (version 2012+ for server software, version 10+ for client software), or Unix-based operating systems (e.g., AIX).

2. Computer Software Deliverables. Upon conclusion of contract performance and at any times specified by the contract during contract performance, the CONTRACTOR shall provide the following deliverables associated with that computer software.

a. Operable Source Code. The CONTRACTOR shall deliver at the conclusion of contract performance one computer disc containing the complete, compilable, and operable source code in the BCC approved language.

b. Executable Code. The CONTRACTOR will deliver at the conclusion of contract performance one
computer disc containing the complete and operable executable code.

c. Software Documentation. The CONTRACTOR shall create and deliver software documentation, containing any programmer notes and describing the software, its operation, its organization, and any significant characteristics of its design so that a computer programmer skilled in the art of programming according to the approved language may operate, maintain, update, modify, and perform all operations necessary to perpetuate
the utility of the computer software.

d. Description of Third-Party Licenses Used. To the extent that the CONTRACTOR has included in the computer software either BCC-approved open-source content or software content subject to proprietary licenses, the CONTRACTOR shall provide each of those licenses and incorporate those licenses in a text file in the discs delivered.

3. Independence of Cloud Based Software. The CONTRACTOR must ensure that cloud-based software is capable of running on non-CONTRACTOR based servers. Any cloud-based software must be capable of running on equivalent BCC or third-party servers. This attribute must be an aspect of the software's underling design.

4. Interoperability of Related Data. Data derived from the created software must be capable of being transferred to other software in a machine legible format with a minimal level of

outside intervention when consistent with standard industry practice. This attribute must be part of the software's underlying design. The CONTRACTOR shall not develop software or use COTS that store or transmit raw biometric data or Protected Health Information data using methods and/or data structures that are wholly proprietary or that otherwise would require BCC's biometric identification system to exert undue effort or expense to extract/re-use its own data.

B. DEVELOPMENT AND IMPLEMENTATION OF COMPUTER SOFTWARE AND NETWORK SOLUTIONS TO SUPPORT BCC'S BRANDED APPLICATIONS

1.1 Patient Identification and All FHIR APIs (Application Programming Interfaces) (Mandatory):

(a) The solution will be built in a way that is accessible by other clients and servers via a secure Application Programming Interface (API).
(b) The API must be RESTful and must utilize JSON for all data communications between the API end points and consuming applications / services.
(c) The API must support and utilize multiple authentication methods including:

- Client Server Keys and Shared Secrets (Similar to how Amazon Web Services and Microsoft Azure allow access to their APIs).
- OpenID Connect (OIDC) and Oath2 against our Biometric Identity Provider (IdP)

(d) CONTRACTOR needs to provide OIDC IdP functionalities using at least one of the following FAPI, CIBA, or BCC-approved alternative server functionality under an OSI-approved open-source license, preferably the MIT License.
(f) Support SAML-based clients and assertion attributes for pre-delegated authority to patient's designee, trusted representatives or groups,[1] in addition to OIDC Relying Parties
(g) Has a user-facing interface (registration, login, self-service account management) capable of being updated to match the user interface guidelines,.
(h) Capable of being integrated with FHIR Hubs and SMART on FHIR, plus retrieve data in real-time as well as store and forward modes.
(e) The system will support API that provide authorization and authentication based secured endpoints, including but not limited to, user account creation and administration, content creation, reporting, patient profiles, consents, roles, user profiles, setting changes, and all other portions of the solution.
(f) The solution supports header-based applications (i.e., encoded group, encryption, biometric algorithms, etc.)
(f) Identity life cycle management for patients and requestors/devices or client IDs (IGA);

[1] See, e.g., SAML V2.0 Condition for Delegation Restriction Version 1.0, Feb. 2009) at ¶2.2.1 https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-delegation.html
A wide array of alternatives has evolved.

(g) Demonstration of OIDC software for Patient ID, with endpoint discovery, account management and audits of data exchanges, which is horizontally scalable and interoperable with FHIR hubs using IdP discovery and/or RADIUS Authentication (IGA);
(g) Fulfillment of Virtual Private Cloud or similar environment for Virtual IdP under BCC-preapproved FOSS, COTs, or Custom Software Solution.
(h) Installation and Implementation of the ICAM platform that is configured to auto-populate all FHIR API inputs as needed (e.g., with Patient Name & Password or translated Biometric ID outputs, or Requestor-specific data, etc.) and other inputs for exchange of patient health data, or treatment matching.
(i) Risk-Management identification of requestors, patients, and administrators (IGA).
(j) Conditional and branching logic without code, including without limitations, protocols to support (A) confidential mobile apps (e.g., for active subscribers) and (B) IWA (e.g., or passive non-subscribers like certain Trusted Third Parties (Schedule X) compatibly with UDAP.
(k) Solution supports Cross-Domain Identity Mgmt (SCIM) with tracking for audits of FHIR API use, content management by patient data set, file(s), source(s), date(s), or field(s) (e.g., full, In Case of Emergency (ICE) profile, International Patient Summary, etc.)
(k) Identity analytics and reporting (IGA)

1.2 Patient Biometrics-based Authentications (Mandatory):
(a) CONTRACTOR will integrate remote biometric authentication software by configuring specialized software, custom software, and conventional hardware, servers, databases, networks, and directories for BCC's SaaS/PaaS/hosted platforms and branded offerings to support patient ID and patient's pre-delegated (and concurrent) authorization services.
(b) Provision the Biometric Identity Provider (IdP) (Custom Identity Server Implementation - OpenID Connect and Oath2) at NIST IAL2, AAL2, and FAL2 or higher ((IGA);
(c) Optimization modeling (hosted/SaaS/PaaS, or NVF, etc.) for substitutable identification algorithms including configuring a pre-tested and pretrained biometric identification (1:N and 1:1) that is template-free or with a compatible store, if needed, suitable for recognition even of an unconscious patient (IGA);
(d) Deployment of OIDC IdP software with customized physical authenticators for AAL2 (e.g., using containers and virtualization, fobs, FIDO, Yubikeys, etc.) with extensibility for remote use (IGA);
(e) Interoperability with FHIR Provider API, Provider Directory API, SMART on FHIR, UDAP, Argonaut IG, Carequality Cert, and Final Rule APIs, Inbound Federation with support from external providers, and modifications (IGA);
(f) Cloud Single Sign-on (SSO) and Outbound Federation to other OIDC/SAML Apps (IGA);
(g) Application choreography, and data and process mediation, and alternative flow sequences pivoting on initial self-identification capacity or not (IGA);
(h) Decentralized ID, personas, and/or Solid pods, (IGA);
(i) The solution supports a logical network overlay of SDNs to provide Biometric Attribute Provider Services for IdPs of RPs, which can require different sets of claims. Schedule 3.

(j) The solution supports Multi-Factor Authentication (MFA) of (a) patients with biometrics, and (b) healthcare providers with access to PHI (e.g. patient history, physician notes, and diagnostic results, etc.); including, unless exception taken, extensibility for (i) Third party multi-factor support; (ii) Policies based on Users, Roles/Attributes, Groups, Applications, & Network Zones; (iii) Risked-based Authentication via Biometric Factors (Template-free or secure); (iv) Second Factors using OTP, Possession (TouchID) or Knowledge Factor (shared secret); and (f) Location Context, Contextual Access Mgmt (w/scopes), & Push Notifications, as needed.

1.3 Requestor Authorizations, Scopes, Permissions, Consents (Mandatory):

(a) Configure BCC's Software to use identity as a control plane within a network overlay architecture and to handle consent management, scopes, and permissions for fine grained data and to perform polymorphic roles across the ecosystem mainly for BCC subscribers but also for passive users (non-subscribers) under sponsor (e.g., local Medicare carriers, etc.).

(b) All permissions must follow the "least privilege" model and must be inherited from their parent containers.

(c) User accounts must be able to be members of multiple roles and groups.

(d) Object (content, data, features, etc.) permissions must be granular and flexible so that individual objects, groups of objects, features, etc. can have permissions assigned and revoked from them.

(e) Access requests and requestor verification (IGA);

(f) Access certification functions wherein permissions must be flexible enough to be assigned to patients, their designees, trusted representatives, roles, groups, attributes and individual users. (IGA)

(g) Entitlements management and Role management, provisioning with RBCP and ABCP and deprovisioning under designations, delegations, revocations, & group membership rules (IGA)

(h) Delegated Authorization, Patient-Designated authority, Patient Proxies, and Policy (IGA);

(i) Unlimited Cloud directory integration, unlimited attributes and fields subject to varied and dynamic data minimization policies, Custom Mapping Cloud based LDAP association, and, if needed, AD-like functionality

1.4. Point of Care Services and NFV Supported by Hosted Environment via Mobile Networks with Security (Mandatory):

(a) The solution must follow all information security best practices and guidelines.

(b) The solution and its development must be OWASP compliant.

(c) The solution must be compliant with all BCC's mutli-level security principles, and all Federal security and risk mitigation guidelines and requirements.

(d) The solution must support Internet Protocol Version 4 and Internet Protocol Version 6.

(e) Mobile Network, Network Overlays for External Exchanges, Secure Transport and Encryption (IGA);
(f) Reserved
(g) Reserved
(h) Mobile Network that support bidirectional exchanges of Data, Images, and Video with Mobility, Roaming, Data Security, Data Privacy, and Access Gateway Servers (IGA);
(i) All solution code, services, servers, gateway, network nodes, and systems must be available for audit at any point by the personnel of BCC or its designee(s).
(j) The public facing internet portion of the solution must be able to be hosted from a single on-premises server (with one (1) IP Address) or network host/data center.
(k) All servers that host/serve the solution must be running the most recent Ubuntu Server LTS OS release, or other OS pre-approved by BCC in advance.
(l) If the solution must be hosted in a cloud environment, the solution must support all three major Cloud providers (Microsoft Azure, Amazon Web Services, and Google Cloud Platform). In addition, the solution must be able to be run from inside cloud space/accounts controlled/operated/provided by BCC.
(m) All third-party resources (including all cloud resources, products, and services) must be compliant with HIPAA/HITECH, HITRUST, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27001, FERPA, COPPA, ADA, state privacy (i.e., CCPA, CCPR, etc.) med info and biometric laws, GDPR, and others as necessary.
(o) All solution mobile applications must be available to(be compiled by BCC staff and upon request, must be available in APK, XPAK, and IPA package file formats (where applicable) for use through a BCC-approved and accepted Mobile Device Management (MDM) system.

1. Confidential Client, and Separate Web Browser Support; Mobile Device Management (Mandatory):

(a) The solution must support all four major Electronic Medical Record (EMRSs) system providers (Epic, Cerner, Allscripts, Med Tech, etc.)
(b) The solution must support all Edge, Chrome, Firefox, and Safari browser versions released during the last 2 calendar years, as well as support for Internet Explorer unless degraded to "desired" rather than "mandatory" in writing by BCC.
(c) All solution will provide mobile applications that must support both Android and iOS operating systems, with wireframes and GUIs for building identity and matching processes.
(d) Support for BCC's Active Subscribers over Client Application(s) and/or Network Overlay, via Cellular, RAN, SDN, VPN, Zero-Trust Network Access (ZTNA) architecture, and Mobile networks; as well as support for Passive requests by non-subscribers subject to sponsors' eligibility via Web Applications, Browser, using security stronger than implicit grants.
(e) All solution mobile applications must be able to be signed and hosted through BCC controlled/operated/provided signing certificates and Epic, Apple iTunes and Google Play storefronts, as well as FirstNet eligible for Certified listing as needed by BCC.
(f) All Apple iOS versions 10 and newer and all Android versions 7 and newer (API Level 24 and newer) must be supported on all devices with and without a screen “notch”.

1.6 SDN, Network Access, Secure Network Overlay, and Mission Critical Partner Extensions

(a) Mission Critical Partner extensions (MCX), data exchanges, multi-hop request handling and tracking, IP Multimedia Subsystem (IMS) services, and auto-loading updates & upgrades (IGA);
(b) MCX Configuration, key management, session management, group management, group roles, directory capabilities, and data migration
(c) A method for application clients to securely receive updates to (a) programs even in mission critical contexts, (b) functions (queries, workflow), and (c) content like a patient's or user's profile (webhooks or other)
(d) Allow zero-downtime upgrades, including security patches, with disaster recovery as well as full backup and restore capabilities.
(e) (connectivity via 3GPP, 4G/5G, gateways, LTE, LMR, RAN, IMS, MCPTT, Software Defined Networks (SDNs), Virtual Private Networks (VPNs) configurations, bidirectional exchange capabilities Single sign-on, federation, and all associated software (IGA).
(f) To support BCC as a Biometric Attribute Provider, one solution supports an "Overlay Network" unless degraded to "desired" rather than "mandatory" in writing by BCC.

Developers will also include in proposals with Milestones, the dates and schedules for the Agreement on implementing the array of recommended software and other integrated building blocks with links to their performance specifications. These plans will provide links to applicable software licenses that correspond to all components, software, and network technologies. These software applications include but not limited to Developer's recommended Biometric Software for Identification, Authentication, Verification, Enrollment, and Attribute Provision Software; as well as --

OpenID Connect Identity Provider Server Software;
OAuth 2.0 Software;
ICAM Software;
MFA Software;
Credential Software:
Consent Management Software;
Patient Designation Software;
SAML and/or Designation Coding better than legitimate impersonation of patient
Mobile Apps (confidential or otherwise);
Web Apps;
UDAP Interfaces and Demarcs;
OS, Server, Client Software;
Hosted Environments;
PaaS;
SaaS;
Prototyping Software;

FHIR APIs - Patient, Provider, Directory, etc.
Authenticators for Biometric ID at AAL2;
Mobility Networks software; and hardware;
Middleware;,
AAA Software;
Gateways;
Network Overlay(s);
SDN Controllers;
Network Function Virtualization (NFV);
Container Software;
Hypervisors;
Modeling software;
Mobile App Design Software;
IP Multimedia Subsystem (IMS);
Mission Critical Provisioning;
Recovery resources, and Testing software;
Billing software; and

Web and Hybrid Applications; External Attribute Provider compatibility	Versioning software and archival Documentation of Function Chaining.

Developer should note performance advantages and benefits of choices and software selections, especially ones that deprecate open-source alternative (see Appendix O) by noting performance-based value added assertions. Developers will also provide guidance on *performance specifications* of platforms, software, network configurations, security, components, modules and applications to elucidate their merits and advantages as discussed below.

1.7 Other Identity and Governance Administration Modules for Access, Workflow, Interoperability, Mediation, Testing, Billing and Auditing (Mandatory if Not Modified to Desired):

A subset of other IGA modules with functions or features that are implemented to support:
(a) Workflow orchestration for all functions and features described herein including without limitation, workflow controller, and workflow connectors for modules BCC's biometric identification/recognition modules, its OIDC authentication modules, its OAuth 2.0 modules, its FHIR modules including all FHIR data exchange capabilities available or required for healthcare, telehealth, or payer compatibility, application programable interfaces (APIs), including all FHIR APIs (i.e., FHIR Patient API, FHIR Provider API, FHIR Provider Directory API, etc.), documentation, and other related instructions (IGA);
(b) Provisioning for Biometric Registration of Patients, MFA, and, as needed, linkage of patient's primary care provider(s) and or preferred IdP (IGA);
(c) Protecting security and privacy of Raw Biometrics and Protected Health Information in rest or transit, while performing Patient Identification, Person Matching, Treatment Matching, Clinical Diagnostic Support (IGA)
(d) Telehealth capabilities with bidirectional exchanges, multi-hop query handling and roaming (IGA);
(e) Management plane with network function virtualization, and tool(s) to model the required infrastructure (e.g., servers, databases, storage) using infrastructure-as-code, preferably with Open Source under the MIT License, to substitute for HashiCorp Terraform, Infrastructure-as-the Code tool capabilities
(f) Support Biometric Attribute Provider services with extensible OIDC Identity Provider software.
(g) Monitoring, Notifications, Open-Source Code vetting, and Auditing, (IGA) and
(h) Testing performance and measure key metrics of remote biometric authentication to replicate pre-integration results in a Virtual Private Cloud (VPC) with QoS metrics and thresholds, and update to reduce any degradation of performance (IGA).
(i) Testing of Software.

(A) Software Testing Required. Any software created under interagency agreement or contract prior to delivery must undergo software testing. Software testing must be conducted using industry standard tools.
(B) Timing of Software Testing. Software testing should occur once executable software has been created.
(C) Software Testing Requirements. Software testing should determine the following:
(1) That the software is capable of serving the purpose of its creation and meets the requirements.
(2) That the software is stable and performs correctly to all inputted information.
(3) The software is usable and performs its functions within a time frame appropriate for the nature of the operation.
(D) Installation Testing. Installation testing that identifies what will be necessary for a user to install and successfully run the software will be required prior to delivery

The Application Software shall also be delivered to BCC in machine readable object code form, and in source code form, and updated upon promptly upon request.

Performance Standards for Deliverables

The following chart sets forth examples of the performance standards and quality levels the code and documentation provided by the Contractor must meet, and the methods BCC will use to assess the standard and quality levels of that code and documentation.

Deliverable(s)	**Performance Standard(s)**	**Acceptable Quality Level**	**Method of Testing**
Tested Code	Code delivered under the order must have substantial test code coverage and a clean code base Version controlled BCC or BCC-specified third-party repository of code that comprises product that will remain in the BCC domain	Minimum of 90% test coverage of all code	Combination of automatic and manual testing

Properly Styled Code for Biometric ID for ICAM for OIDC IdP Server Designated Authority modules, Authentication Consent Mgmt OAuth 2.0 Authz Credentials, Access, etc.	GSA 18F Front End Guide	0 linting errors and 0 warnings	Combination of automatic and manual testing
Accessible	Web Content Accessibility Guidelines 2.1 AA (WCAG 2.1 AA) standards	0 errors reported for WCAG 2.1 AA standards using an automated scanner and 0 errors reported in manual	http://squizlabs.github.io/HTML_CodeSniffer/ or https://github.com/
Deployed	Code must successfully build and deploy into staging environment.	Successful build with a single command	Combination of manual review and automated testing
Documentation	All dependencies are listed and the licenses are documented. Major functionality in the software/source code is documented. Individual methods are documented inline using comments that permit the use tools such as JsDoc. System	Combination of manual review and automated testing, if available	Manual review

	diagram is provided.		
Secure	OWASP Application Security Verification	Code submitted must be free of medium and high level static	Clean tests from a static testing SaaS (such as Gemnasium) and from OWASP ZAP, along with documentation explaining any false positives
Biometric ICAM and OIDC Provider SaaS/PaaS/Network			
Designation and Consent Mgmt w Data Privacy			
Platform, SSO, Federation, and Mobile App and Network Security			

OTHER USER STORIES

SPONSOR'S (NON-SUBSCRIBER'S and UDAP SYSTEM OPERATOR'S) PERSPECTIVE: BCC’s RapidVu™ will be configured solely to interface with certain Non-Subscribing Affiliates on special terms with very limited functions and features, that exclude full service provided to other subscribers. BCC's must be especially careful with those Subscribers and Non-Subscribers that rely upon UDAP by configuring o interface with such entities, *without* merging or contributing to the code of UDAP into BCC's Software, Work Product or Solutions in a way that dedicates certain patented technologies BCC relies upon into the public domain. UDAP may triggers patent retaliation as it is licensed under Apache 2.0. As such, BCC will be relying upon the CONTRACTOR to develop a suite of solutions that support BCC and its subscribers, and separately support certain non-subscribers that are authorized third parties like Trusted Third Parties (TTPs). This is the active and passive dichotomy. Passive health systems like those of Sponsors do not have a contractual relationship with BCC’s and do not provide a BCC’s B-IdP.net platform access or BCC services *directly* for their patients. Passive health systems, instead, may form a part of the BCC ecosystem only implicitly without their advanced direct subscriptions in many instances via sponsors (provided, however, that all uses are secure and accounted for and subject to audits). Any passive health systems may usually only use the BCC B-IdP services for their patients, under a sponsoring affiliate's commercial licenses and/or future subscriptions from BCC, if the sponsoring affiliate has become and active service bureau, subscriber, or gains temporary passive use privileges.

As such, BCC's IdP and other services as well as mobile or web apps must be designed to be extensible with compatibility for sponsoring affiliates that may function as service bureau by relying upon Unified Data Access Profiles or UDAP [Apache 2.0 at github]. The suite of UDAP protocols comprises UDAP JWT-Based Authorization Assertions, UDAP Dynamic Client Registration, UDAP JWT-based Client Authentication, and UDAP Tiered OAuth (i.e., for other IdPs etc.). UDAP proposes to revise the conventional precondition that the Resource Server trust the IdP, by making the IdP selection based on the User's home OIDC Provider, even though it may not be a BCC subscriber. However, BCC's RapidVu™ service may be conditionally available to patients of these health systems through entities like TTPs that provide reciprocal IdP services for passive health system with the BCC's RapidVu™ ecosystem. These non-subscribing IdPs share FHIR Access to data sets via Patient or Provider API. Passive health systems may participate indirectly to form a part of the BCC's extended service ecosystem via a sponsor, even without separate subscription. Passive entities may not have full access to all BCC resources and services that are available to BCC's active subscribers, however. Any passive health system that becomes a subscriber may thereafter directly participate in the BCC's RapidVu™ service and use its B-IdP platform for their patients as an active health system. See also, Appendix A

Interested Parties ought to look at BCC's Executive Summary which is included by reference here. It and other materials may be updated from time to time before the Effective Date of the Agreement, along with a revised list of Deliverables under the RFP and the updated content will be included subsequently at least by reference in the Agreement.

Schedule A

Many eligible sponsors will be granted passive user privileges based upon enhanced exchange of services, rights or privileges valuable to BCC, beyond basic FHIR APIs. See, e.g., QHINS, Azuba, Verato, etc. In turn, these entities and their entrusted external IdPs may interoperate via their respective health system's public APIs (e.g., for FHIR Access to Data Sets, etc.) such as Patient APIs or Provider APIs. BCC's network has demarcations that do not permit it to directly use software or sets of protocols that may undermines its patent or other intellectual property rights.

Cautionary note: UDAP uses an Apache 2.0 license with patent retaliation clause, so BCC does not use UDAP for Active Health Systems, but instead allows passive FHIR hubs, that use UDAP, to exchange data only as a service via common APIs as needed by BCC. As such, UDAP is not a built-in component of any BCC software or part of its basic solution. It is to be described as an optional compatible resource or add-on in proposals aimed for passive entities insofar as the requisite interfaces are possible without abridging proper demarcs however.

Some other kinds of Third-Party Service Providers will enrich the architecture by providing additional services, like third factors, risk-based identity management services, electronic signatures or enhanced matching scores based on the health system-compatible authentication capabilities and verified data. To this end, BCC's platform should be flexible enough to extend using (a) single sign-on mobile app software that provides third-party apps the ability to federate their native mobile application with BCC Identity, Credential, and Access Management (ICAM) (b) single sign-on browser app software that provides third-party apps the ability to federate their native mobile application with BCC Identity, Credential, and Access Management (ICAM); (c) an API Suite that is a set of Web-based plugin APIs that developers of Mission Critical applications may integrate MCX/MCPCC Data into their cellular, radio, IMS, and mobile solutions; and (d) Multimedia Incident Retrieval API allows your internet-aware cell phone apps, desktop or web applications to conduct a single session with mobile devices be in order to retrieve MMS/S

NEXT STEPS: To explore the Deliverables of the RFP please fill out the following fields and email them to steve@biometriccare.com under the Subject "RFP Deliverable":

Developer's Name:
Developer's Headquarter Address,
City, State, County:
Developer's email:
Developer's Telephone (Optional):

Preferred Deal Terms: Looking for Proposals (Open): Bids assessed in view of exchanged value.

Bidders are welcome to present bids for full payment in cash or cash equivalents.

BCC's selection criteria may, however, extend weight to bidder proposals based on reciprocal benefits in kind. Some may help defray part of full cash payment in favor of extending a Developer-branded product lines or of licensing some of BCC patent rights. Some Developers may see a way clear to do so for valuable or exclusive prospects like cross-sales of complementary services, offerings, products, or equipment. Similarly, development teams of health systems, EHR providers, or payers (public or private) may gain benefits in patient engagement, gainsharing, savings, leadership advantages, promotions, reputational capital, enhanced subscription packages, or related to healthcare, transport, insurance (i.e., premium EMS coverage, etc.), well-ness, or professional services.

As such, BCC's selection criteria may favor a payment formula with non-cash aspects for some portion of the project. A bidding developer in related segments, for instance, may also gain an option to license some limited BCC's IPRs a distinct field of use (*i.e.,* specialized mobile devices, security provisioning, gateways, transport services, or certain planned health services (i.e., for mental health transitions, postdischarge acute care, SNF care, hospital-at-home service [e.g., for patients to ill for ICU], etc.). Although Developers usually might be obliged to pay a lump-sum royalty fee to obtain such a biometric ID license for that purpose, BCC's management may favor a proposed reciprocal benefits arrangement.