BIOMETRIC CARE CORP

REQUEST FOR HEALTH IT PROPOSALS 2022

ABSTRACT

Biometric Care Corp (BCC) is a development stage business in California, incorporated in Delaware, that improves patient and business outcomes.

Patient matching is defined as the identification and linking of one patient's data within and across health systems in order to obtain a comprehensive view of that patient's health care record. At a minimum, this has been accomplished by linking identifying data fields or credentials such as name, birth date, phone number, and USPS address. Patient matching is a critical component to interoperability and the nation's health information technology infrastructure, but defects still pose risks.

Usually, a patient presents their own data fields to verify themselves. In some cases, however, the patient might need to have passed the whole set of credentials or verifiable attributes to another individual or group of individuals in advance. If the patient, for instance, is ill or incapacitated, a medical first responder would need to enter these fields or identifiers on behalf of the patient to get rapid access to active conditions, allergies, or medication intolerances of the patient to personalize care early.

While few expect to be in the situation of this distressed patient, even fewer would decline safer assurances that rapid identification using biometrics and matching could be performed on their behalf if they are so distressed. Fortunately, new techniques allow the patient's designees to use patient biometrics to close gaps from unknown demographic fields, or otherwise confirm that the patient is not subject to the all-too-common errors of mistaken identity. Improved safety and security enhance patient outcomes, engagement, and business goals by sharply reducing risks and costs.

BCC is selecting a developer to help it deliver on the promise of the new techniques with patient safety, data privacy, and security. BCC will be the first to legitimately

leverage key patented innovations to become the leading Identity Provider with OpenID Connect (OIDC) that supports mobile rapid healthcare using biometric ID.

The solution must also support BCC's provision of database services as an Attribute Provider that performs biometric authentication of patients by requestors for identification with MFA, personalized data exchange, and treatment matching.

The Contractor will assist BCC to design, develop, and implement a reliable platform with functions and features to personalize care services earlier by integrating:
(a) identity, credential, and access management (ICAM) and biometric technologies;
(b) advanced designation capabilities to act when a patient is unable or incapacitated;
(c) mobile and remote access to verifiable patient identities using transformed biometrics at least at an acceptable assurance level (NIST's IAL2, AAL2, and FAL2).

Our services are being developed to help health systems retrieve each patient's essential health data fast, accurately, and securely anywhere in mobile device range.

Whether in an emergency, a pandemic, or a transition care setting, BCC's platform for patient identity and matching will personalize services even in remote places to improve treatment, hasten diagnosis, extend telehealth, customize transport, or match treatment from the first point of care with data privacy.

BCC's RFP for Design, Development, and Installation Capabilities

BCC'S RFP ABSTRACT KEY BIOMRETIC & ICAM ROADMAP

Biometric Patient ID is the new control plane for telehealth thanks to ICAM Management and OpenID Connect (OIDC) IdP software. Even Open-Source Code under MIT License offers pretrained biometric software that seamlessly operates to (a) translates biometric inputs like a face photograph of the patient into the patient's name and password reliably, (b) unlocks a physical authenticator of that patient or a composite persona for AAL2, and (c) enables discovery of the patient's primary care provider [or "home" IdP].

Designated Authority with Data Privacy is the technology, standards, and processes that allow a patient or their parent to designate an authorized person ,representative, proxy, group members, to provide each of them with the credentials to act as patient's trusted referee, a designated party to use the patient's transformed biometrics to verify the patient's digital identity. The solution may use the best designating techniques,

containers, compatible SAML patterns, and/or Network Functions Virtualization (NFVs) to support designee or first medical responder access via mobile device by matching patient attributes or "claims" and using credentials for managed across vis-a-vis multiple health systems to personalize identification or treatment.

Mobile Network Security and Interoperability comprise the set of networks, technologies, and systems that support ICAM functions, activities, FHIR APIs, and outcomes via mobile networks, the Internet, Web Applications, RANs, VPNs, Software Defined Networks (SDNs), and network overlays to aggregate claims needed to identify patients via communicably connectable health systems with the variable content for patient health and safety compatibly under shared principles of limited purpose, data minimization, integrity, and confidentiality. Join BCC's effort to build on advances like SMART on FHIR process for secure authorization of third-party application access to patient data when need its most over the Patient Access API, Provider API, and Provider Directory APIs.

BACKGROUND:

[A] Key Dates: (RFP Schedule)
RFP Publish Date: Wednesday, 2 February 2022 (2-22-22)
Contractors' Question Deadline: Wednesday, February 9, 2022
Contractor Proposals and Bids Due: Friday, 25 February 2022

[B] Work Performance: Performance of the work will be Offsite. The Contractor needs to carry work in their office location. This work could extend to a number of ICAM categories of software and network customization including the sprints for OIDC IdP Provider and ICAM Solution functions, features, and extensions described below. Interested Parties ought to look at BCC's Executive Summary and Preliminary Roadmap next. **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 place "RFP" in the subject line.

[C] Eligibility: CONTRACTOR eligibility is based on Company Nationality and Corporate Headquarter Location either: (i) Onshore (a USA Organization) or (ii) Eligible Offshore (EU Member States, UK, Canada, Switzerland, or Australia Organizations Only); Exceptions upon request and pre-approval. Category: Software, System and Application, Wireless Networks, Apps, SDNs, and NFV, Web Design and Development.

BCC's ODIC IdP Provider and ICAM Sprints

Identity Management is how BCC collects, verifies, and manages attributes to establish, discover, and maintain patient identities consistently as an OIDC Identity Provider at AAL2 & Multi-Factor Authentication (MFA) across health systems and providers, including Emergency Service Providers.

Credential Management is how BCC issues, manages, and evokes credentials bound to patient identities or describes personas that couple patients with pre-authorized caretakers, first medical responders, or other trusted designees.

Access Management is how BCC authenticates patient identities and authorizes appropriate access to protected services by or on behalf of the patient, and compiles the identifying claims needed by external systems for identification with data minimization sufficient for ID, health profiles, and clinical support decisions.

Federation is the technology, policies, standards, and processes that allow an entity to accept digital patient identities, attributes, scopes, and credentials managed by BCC subscribers (active) and other non-subscribing sponsors (passive) using BCC's verification services as a biometric attribute provider.

Governance is the set of practices and systems that guides ICAM functions, activities, and outcomes under safeguards of data privacy. BCC does not use or rely upon the storage or transit of raw biometrics or unencrypted Protected Health Information (PHI).