Executive Summary:

The five participants in this proposal will use the HEART implementation specifications to create a solution that gives consumers the ability to conveniently access and share their own health records on demand, on a national scale. This prototype will incorporate the complete suite of HEART profiles, and will demonstrate a unique nationwide capability for consumers to conveniently verify their identity, locate and electronically request their records, and deliver them to a secure cloud-based personal storage service. The patient record queries will incorporate digitally signed patient record requests that satisfy the requirements for triggering the HIPAA patient mandate.

Each participant brings a robust set of complementary capabilities that, when combined, overcomes each of the key barriers to low-friction patient-directed health record access. Resilient has successfully deployed OpenID Connect and OAuth 2.0 in production deployments, and developed a low-friction and robust cross-organizational access management and policy enforcement model. WebShield has developed a privacy network and unified trust model that makes it possible to pool, link and analyze privacy sensitive, regulated and proprietary data from disparate parties that don't agree upon policies or trust each other. This in turn makes it possible to authenticate and verify the identities of consumers on a national scale, locate and match records about them from disparate sources, and accurately link disparate sources of data and the online user – all without jeopardizing their privacy. This is being rolled out on a national scale with the support of several national healthcare payers, pharma, technology vendors and identity providers.

This unique nationwide privacy preserving identity verification and record linking capability will be integrated with the digital identity and digital signature capabilities of SAFE BioPharma Association to enable a legally robust mechanism capable of satisfying the diverse regulatory requirements in healthcare. It will also incorporate the healthcare data interoperability, querying, and messaging capabilities of InterSystems HealthShare, and the HIPAA compliant patient-directed record storage, access and sharing capabilities of Carebox, and support for UMA (User Managed Access).

The team offers proven and robust capabilities in their respective domains. Carebox is an active member of NATE (National Associate for Trusted Exchange) and part of the NATE Blue Button for Consumers (NBB4C) Direct Messaging trust bundle that makes it easy for any doctor or hospital with a Certified Electronic Health Record (CEHRT) that meets the US Government requirements of "Meaningful Use" to send anyone their clinical summary, discharge summary, and other medical records directly into Carebox. Carebox has deployed patient-centered exchange solutions as a FHIR Server and FHIR client, incorporating user-managed access design patterns based on OAuth 2.0.

The most unique and compelling aspect of this demonstration is that it offers a comprehensive approach that promises to overcome all of the barriers to information sharing that still inhibit data liquidity even after the latest interoperability standards have been widely adopted. The fundamental barrier to sharing is the lack of a mutually trusted way for disparate organizations and systems to agree when the are talking about the same person, and the resulting inability of the consumer to enforce their legal right to access and share their own health records. This system was designed from the ground up to consider all factors that drive or inhibit data sharing, including but not limited to privacy, security, discoverability, regulatory compliance, technical compatibility and enforcement of commercial terms. The collaboration presented here of healthcare providers, technology vendors, and security and privacy experts has been incubating for years and is ready for rollout to patients in the next 3-6 months. This Challenge could be an excellent vehicle to showcase its potential to improve health data sharing and to promote the HEART standards. The attached presentation will explain how it works in greater detail.

Proposed Technologies:

Resilient Access™ is a network-centric real-time workflow engine that interrogates multiple internal/external authoritative sources (e.g., identities, attributes, multifactor authorizations, entitlements, biometrics, roles, access privileges, environmental contexts, etc.) to establish a level of trust between two parties to resolve the requesting user's access rights based on the defined policies of each involved party. Privacy and confidentiality is maintained to whatever level is desired.

For the critical identity syndication and regulatory compliance steps, the solution will utilize Webshield's Privacy Network & Unified Trust Model in order to overcome legal, regulatory and commercial barriers to access a diverse network existing nationwide identity and data sources capable of authoritatively verifying patient identities and discovering and matching patient records.

SAFE Biopharma will be digitally signing the patient record requests in order to assure a high standard of trust and security as data moves via the HEART protocols, and to ensure that the patient record requests can be trusted and relied upon by providers that receive them. Specifically, the solution will generate a digitally signed document (signed with the patient's digital signature) that verifies not only the patient's identity, but also their patient ID at the provider, their direct address, and the fact that they have requested that a copy of their health records be sent to their direct address.

This digitally signed document (including verified attributes from a FICAM-certified signing authority accepted by the FDA, DEA, EMA and the Federal PKI bridge) removes any reasonable uncertainty as to whether HIPAA covered entities (payers, providers, labs, pharmacies, etc.) are authorized and obligated to send the requested records in accordance with the patient's request, pursuant to the HIPAA patient mandate.

In addition to delivering the digitally signed patient request, the solution will use InterSystems Healthshare to actually query patient records sources, transform the resulting response into standard interoperable formats, and then send the document as an encrypted Direct message to the specified Direct address.

Finally, the solution will utilize Carebox's HIPAA-compliant cloud infrastructure to receive and store the patient records, support patient access, and to implement user managed access and sharing via Direct, FHIR, email and other sharing mechanisms.

Target Population:

The target consumer population is open ended, with the ability to authenticate and verify on demand the identities of the vast majority of US residents. The launch of the eP^3 (Empowering People with Privacy and Personalization) Network and related ecosystem initiatives is being conducted in parallel and on a similar schedule for the Moving Health Data Forward Challenge, and offers numerous opportunities to demonstrate the ability of the HEART WG-based APIs to empower consumers with access to and control of their data in clinical research and personalized care management for payers, providers, pharma and in research settings.

HIPAA-Compliance:

The proposed solution will empower individuals with the ability to exercise their right under HIPAA to access and share protected health information about them, as specified in **45 CFR 164.524,** “Access of individuals to protected health information”.

The key is the ability to tap into a diverse network of regulated and proprietary data sources to authoritatively verify the identity of an individual and authenticate them online on demand, and to locate and verify an accurate match with that person’s healthcare records stored in different systems that don’t necessarily have consistent identity attributes or patient IDs. This, combined with SAFE BioPharma’s universally accepted FICAM-compliant identity credential and digital signature trust framework makes it possible for an individual to independently prove to record holders they are in fact the subject of their health records, and to properly document that a legitimate request has been received.

In addition, the solution will rely upon the HIPAA-compliant Carebox platform as the consumer records repository, using open standards such as FHIR, Direct Messaging, etc.

Financial Matters and Use of Funds:

All five companies are financially self-sufficient, but the challenge award will allow the teams to dedicate resources to this topic, and also offer an opportunity to recruit their members, ecosystem customers and partners to participate in pilot deployments that demonstrate the real world capabilities of the technology. All of the funds will be used to pay the personnel and subject matter experts on the teams. No funds will be needed for overhead, computers, offices, product development R&D or testing, etc. Resilient and WebShield are orchestrating a number of well funded (millions of dollars) commercial projects that have significant overlap in technical requirements, ecosystem participation, target user populations, regulatory compliance requirements and operations. To maximize efficiency, Resilient and WebShield will split the project management responsibility and budget authority equally. The challenge funding will be split between implementing and validating a HEART WG Profile compatible solution and recruiting and managing deployments of the HEART challenge solution to prove the real world ability to empower consumers. InterSystems, SAFE BioPharma Association and Carebox are already working with Resilient, WebShield and the broader eP^3 Network to prepare for the commercial launch. They will assist in integrating their technologies and deployments and adapting them where necessary to align with HEART profiles, recruiting their members, customers and partners for a broad-based technology showcase.

Business Model for the Offering:

These companies would like to see true data liquidity happen and therefore this service will be offered for free to all Americans. During the consent process, the patient will determine what use of this data is approved and acceptable. The provenance and usage rights of the data will be captured when the data is encrypted and safely stored. Only the consumer has the legal right to authorize access to and use of their records from all sources, and who can interact with them online, and for what purposes. Thus, empowering consumers with direct control over their records on a global scale, and the ability to use them for personalization and process optimization, makes data much more valuable and much more useful. The network creates a free exchange and solution app store that allows individuals and organizations to pool their resources and create value, without fear that their privacy or commercial rights will be compromised. This allows the network overall to be free and open to all participants, yet be self-funding via revenue share from value-added services such as clinical research, value-based payments, fraud prevention, etc. The solution will first be deployed as an email and social media campaign that directs towards a public website. If phase 3 is awarded, the team will also move the solution on to mobile with the help of an existing partner, Parallel6. The use of funds throughout the phases will be 50% engineering and test, 20% project management and 30% ecosystem development, the gap between the overall cost and the covered by working capital.

Development plan and timeline for Phase 1:

- Phase 1 (3 months) – The team will use the time to complete the design, begin the prototype, and lock down pilots sites for phase 2. Based on the significant demand and complementary deployments and strategic initiatives of the members, customers and partners of the SAFE BioPharma, InterSystems, Carebox, WebShield and Resilient, we feel confident that one or more of the following companies will participate in phase two and publically support a technology show-case, including a nationwide insurer, multiple major global pharma, multiple patient-powered research networks, a nationwide provider network, etc.

Success Metrics: The key success metrics for this challenge are the number of organizations adopting the solution to empower patients with access to their data, the number of users supported and health records retrieved, the number and diversity of data sources connected, and the diversity of overall patient populations empowered. In addition, the convenience and usability of the solution are a key success metric, measured by the amount of effort and expertise it takes for a person to successfully request and receive their health records, and what percentage of people that attempt to request their records succeed in getting through all of the steps necessary to create and send the requests.

Risk metrics: A key risk of the Moving Health Data Forward Challenge is motivating awardees to stay focused on the deliverables given the relatively small size of the grant compared to ambitious scope of work. That risk is mitigated because the team members have long been actively collaborating on the necessary product development, regulatory compliance and ecosystem adoption tasks in support of very substantial existing projects, the eP^3 network launch, and a pipeline of other opportunities. The timing of the Challenge aligns perfectly with the culmination of a years-long effort, and offers an opportunity to show-case the disruptive innovation of a nationwide privacy-preserving identity network that magnifies the ability of HEART WG API standards to empower patients. Another risk is rallying showcase participants to prove the ability to empower patients in a real world environment. This risk is mitigated by the fact that eP^3 Network participants and their respective members and customer/partner ecosystems reach a majority of the overall healthcare ecosystem, the fact that there is significant unmet need for patient-centered data sharing, and the fact that the solution can empower patient using only existing standard-based data sharing standards interfaces.

Use of HEART Implementation Specifications

The team has evaluated the UMA specifications and we have deep knowledge and experience with OAuth2 and OpenID, and are confident that the additional UMA profiles are aligned with our existing architecture and implementation, and can be accommodated with a manageable incremental effort. For the pure security step, Resilient will use OpenID for patient authentication. As it relates to the more granular permissions included in the UMA standard, Carebox will handle some of the messaging steps inside their application.

Team:

Resilient Network Systems is a privately held, venture-backed company based in San Francisco. Our expertise is solving complex multi-organizational access management problems with our distributed, network-based software. Our 2 technical leaders (one a former Chief Engineer of Sun and the other a co-author of J2EE) designed our systems to work at Internet scale. We are experts in all modern techniques related to identity, access and policy enforcement. The engineering team that will complete this API service is the same team the executed the successful “Patient Centered Care” National Strategy for Trust Identity in Cyberspace - NSTIC grant in 2013-14. Ethan Ayer, CEO, will be the point of contact, (415) 291-9600 x103.

WebShield Inc. is a privately held company that has pioneered the development and launch of the Privacy Network and Unified Trust Model, recruiting a broad-based ecosystem team made of dozens of partners and customers, including non-profit consortia, major national payers and pharma, global identity firms, technology vendors, etc. These organizations (many of whom are in the eP^3 Network) are in the midst of a nationwide roll-out of the network. Jonathan Hare, CEO, will be the point of contact, (415) 265-3250.

InterSystems is the leading health data management and interoperability vendor, whose technology manages 67% of patient records in the US. It has over half a billion in annual revenues, and supports all the major data interoperability and messaging standards. Ron Sullivan, Vice President & General Manager of Public Sector, will be the point of contact.

Carebox is a digital health company that makes it easier for patients to collect, organize, and re-use their clinical data from medical records that patients can access. Carebox partners with a range of healthcare, life sciences, and related organizations that want to make patient-centric healthcare data part of their solutions. Brian Weiss, CEO, will be the point of contact.

SAFE-BioPharma Association, and SAFE-BioPharma Bridge CA (SBCA) SAFE-BioPharma Association (www.safe-biopharma.org) is the non-profit industry coalition responsible for the SAFE-BioPharma® digital identity and signature standard used in the global biopharmaceutical and healthcare sectors. The SAFE-BioPharma Bridge Certification Authority (SBCA) satisfies legal requirements for online trust in the US, the EU and elsewhere, and is accepted by the FDA, DEA and EMA, and is cross-certified with the US Federal PKI Bridge. Mollie Shields-Uehling, CEO, will be the point of contact.