Bitr, Inc
Christian Mate Jr.
chrischain98@gmail.com

Move Health Data Forward Challenge | *Business Case*

The proposed solution, termed “MeshEHR”, establishes a unified, interoperable platform in which patients control the sharing and provisioning of their Electronic Health Records. The solution manages health data by associating records with Cryptographic Key Pairs on a secure distributed ledger commonly referred to as a “blockchain”. Within the system, records received by the patient are encrypted so that only they, the owner of the key pair, may view their records. Subsequently, the owner, or Patient, may then provision another, such as a specialist, to view their health records by encrypting select records to that key-pair. This model enables doctors to interact with and exchange data with the patient directly, in a peer-to-peer system.

The vast implications of Blockchain Technology are currently being explored by NIST, The National Coordinator for Healthcare Information Technology, and several others within both public and private sectors. Blockchain Technology stands to improve data integrity, and enable cross-platform interoperability for information exchange, identity issuance, and patient tracking within future and pre-existing healthcare systems.

Currently, Patient Health Records are fragmented across multiple centralized, isolated databases tasked with independently securing and maintaining information. This has led to an ecosystem that lacks efficiency, integrity,and fails to provide sufficient interoperability/availability of health information. This is largely due to the lack of consensus between multiple data-bases, formats, and protocols. These implementations are not only vulnerable, but experience large amounts of friction when processing transactions.

With the MeshEHR API, users may directly interact with their health data.

Doctors, hospitals, and patients may access, share, and exchange health data through a Consumer-Facing Graphical User Interface. The MeshEHR Framework represents an interoperable information layer available to end users, and existing health information systems. Through an API Framework, existing Healthcare providers may then further develop Consumer-Facing graphical interfaces in on-premise, mobile, or web applications that implement MeshEHR API on the back-end of the application. By promoting interoperability, ensuring security, and streamlining regulatory compliance, the MeshEHR API represents a significant value proposition to the Healthcare Sector and to the patients it serves.

The end-user Market Focus includes individuals seeking easier access, understanding, and use of their health records. Target Healthcare providers include small to medium-size entities seeking to improve the efficiency and security of legacy implementations.

Because the MeshEHR Framework seeks to secure interoperability (and subsequent availability/scalability) of health records, the design focuses on a universal syntax API that all network participants manipulate to exchange Health Information. This focus provides a patient-centric model, wherein patient data is attributed by verified, authoritative participants. Independent of servers, hacks, or identity theft.

Bitr, Inc
Christian Mate Jr.
chrischain98@gmail.com

With Patients at the center, each possessing their own sovereign health profile, the efficiency and security of sharing information, and validating claims such as insurance, is significantly increased. Additionally, The HEART WG implementation specification standards ensure secure tokenized access to protected health information.

At the foundation of MeshEHR is a shared database accessible by Mesh network participants. This database, commonly referred to as a blockchain, is distributed, and hosted by a network of nodes geographically distributed. This network maintains consensus by validating each transaction with the entirety of the network (i.e. Doctor A diagnosing Patient C). By leveraging universal consensus across the network, network participants are able to directly transact secure health information by manipulating the API, maintaining interoperability and data integrity. Through the API, doctors are able to attribute data to patient records, patients are able to make claims to their health information, and entities are able to request information; including doctors, testing/radiology centers, and First Responders. Furthermore, Government Health Information Exchanges may transparently oversee regulatory compliance.

Underpinned by proven encryption algorithms, Authentication specifications, Public Key Cryptography, and Blockchain Technology, the solution establishes a distributed, secure, and scalable Information layer for Electronic Health Record Implementations.

While the availability and security of Patient data is often perceived as a compromise; the proposed solution promises to address the lack of availability, regulatory transparency, and security inherent in present Health Data Information Systems.

The MeshEHR API interfaces with the backend data-base, a Blockchain. End users interface with the API through an Intuitive Graphical user interface. The proposed API may be manipulated from on-premise installations, mobile devices, or Web applications, so long as the device has an active internet connection.

The immediate prerequisite to access data, or authoritatively attribute it, is the demonstration of ownership of a private key to a customer profile. This profile is essentially a unique directory for information on the blockchain. Profiles can receive data (Patient receiving diagnoses) or send it (Authorized Practitioner posting test results to Patient profile). These Profiles represent destinations for transactions on the MeshEHR network. Profile Ids are alphanumeric, and average 32-33 characters. (1EHRMeshHtKNngkdXEeobR76b53LETtpyT). This Identifier is a Base58 encoded hash of the Customer Key Pair.

Key ownership is demonstrated via signatures derived from a private key. Signatures are provably associated with the customer profile, but insufficient to reproduce the signature (steal the profile). Due to the native architecture of blockchain technology, customer profiles mandate a signature to broadcast transactions, like a diagnoses, or sharing that diagnoses with another party.

The implementation of HEART WG specifications within the MeshEHR API solution is highly effective for securing tokenized, user managed access to Customer Profiles. Utilizing OAUTH 2.0 and OpenID Connect, users can implement 2-Factor Authentication (2-FA), Password Protection, mnemonics, and Smart Cards for identity verification. These specifications empower people to leverage secure offline key-pairs anywhere through accredited UMA

Bitr, Inc
Christian Mate Jr.
chrischain98@gmail.com

specifications.

Cost Structure for the MeshEHR API is proposed as a per/API-call subscription service.

Authoritative Network participants such as Doctors Offices, Hospitals, Healthcare Systems, Existing EHR Providers, and Specialists pay a set Subscription fee for annual issuance of MeshEHR API credentials. These Participants are broken down into Tiers based upon monthly transaction volume. API use is monitored via the volume of transactions conducted under a set of API credentials.

Tier 2 Subscription Fee	# API Calls	Rate
$12,500.00	140000	$0.80

In the following forecast, The MeshEHR API is projected to process over 250,000 API calls by Q217.

Revenue and Expense Breakdown	***Year 1***
Revenue	$230,000.00
Cost of Sales	$130,000.00
Gross Margin %	43.00%
SG&A	$30,000.00
R&D	$40,000.00
Investment Funds Received	$750,000.00
Cash at Beginning of Year	$15,000.00
Cash at End of Year	$865,000.00

Potential Partners that have expressed interest in Bitr, Inc and the Mesh API include The Harvard Angel Alumni, Draper Associates, Day One Investments, and TEDCO. Currently there are no Institutional funding agreements executed with Bitr, Inc.

Bitr, Inc is a Delaware C-Corporation that has developed and researched Blockchain Applications since 2015. Bitr, Inc possesses intellectual property pertaining to the data architecture employed by the proposed product, MeshEHR API. This Patent (USPTO 62291213) pertains to identity authentication, management, and secure attribution/access of information. This identity management architecture is FIPS 201 compliant and also meets LoA 4 Benchmarks.

Bitr, Inc
Christian Mate Jr.
chrischain98@gmail.com

Development Plan and Timeline

Key Activities and Milestones to be undertaken during Phase 2 of the Move Health Data Forward Challenge include: Development of Node.js API Syntax, Refinement of Technical Documentation, Development of Node.js API, deploy Server stack instance with integrated OAUTH, UMA, and OpenID Connect. After the Prototype is functional, deployed and implemented with HEART specifications, we will then test, benchmark, and demonstrate the API through a Consumer-Facing Interface. This demonstration will feature multiple processes mapped to EHR constructs.

By recording the use of the API, data liquidity, patient participation, and health information flow, we are able to define metrics that are indicative of both the success of the MeshEHR API, and the impact of secure, available health information within the Healthcare Community. Putting present EHR implementation metrics side-by-side, we are able to cite the cost-saving advantages of MeshEHR compared traditional systems. Beyond metrics comparisons, the implications of the MeshEHR API are likely not enumerable in currency. By increasing availability of health information, and securing an interoperable platform for it to reside, people can be treated faster, more efficiently, and in more places. There are several inferable instances wherein inaccessible patient data carries significant negative consequences. We will be closely monitoring the impact and metrics of MeshEHR during the transition into implementation phase.

To implement MeshEHR, there is a process of registration for network participants. For newly registered Patients, this can be as simple as setting up mobile banking. Practitioners, offices, Healthcare Systems, and other authoritative entities, however, must provide additional specialized information. When partnering with a Healthcare Provider, specialized processes including unique Service level agreements are required.

As with any EHR implementation, it is imperative that regulatory compliance, data protection laws, and logical/physical access control are satisfied. The Data Architecture employed by MeshEHR does not put network participants, including doctors, health systems, and patients, responsible for protected health information. Through HEART WG specifications, secure authentication tokens are produced as a prerequisite to the generation of a cryptographic signature at the time of the interaction with the MeshEHR API. This signature is generated on an offsite Hardware Security Module (HSM). HSMs are a type of crypto-processor that secure private keys and generate signatures without exposing them. In this instance, the private key is to that of a Customer Profile. HIPAA Compliance within the MeshEHR API is effectively by design; the availability of patient information, ownership, and security of that information is ensured by transparent smart-contracts enforced by the MeshEHR Network. However, Network Participants are still required to comply with HIPAA Regulations pertaining to physical security and logistics.

Authoritative Participants such as doctors and Healthcare Systems inherently possess certain

Bitr, Inc
Christian Mate Jr.
chrischain98@gmail.com

responsibilities when it comes to Healthcare Information. These responsibilities are largely unchanged from traditional record storage methods. Authoritative Participants are entrusted to attribute accurate information to Patient Health Records. They are responsible for their passphrase, and the security of any external authentication credentials such as Smart Cards. Authoritative participants are capable of attributing information to other profiles, validating claims made by other patients, and requesting information or tests from the patient. If authentication credentials are compromised, the entity is responsible to report it. In this event, MeshEHR Security Staff will immediately disable access to the key-pair and migrate information to a new, un-compromised key-pair. Following the securitization of the event, harm analysis and reduction are undertaken by Administrative Staff and additionally reported to the applicable public entities.

Similar to the responsibility of a PIN number, Patients are responsible for MeshEHR login credentials. Multi-Faceted security including 2-FA (Two Factor Authentication), and PIN may be implemented with HEART WG OAUTH 2/ OpenID Connect Token issuance. Through the Consumer-Facing Interface, Patients may view their records, share them with verified doctors, link their insurance and view their healthcare network. With MeshEHR, Patient records are the Patient's.