Electronic Acknowledgement Receipt

EFS ID:	32329689
Application Number:	62656993
International Application Number:	
Confirmation Number:	7966
Title of Invention:	QuantH V1.0 Secure Healthcare Blockchain Data Storage Platform

UNITED STATES PROVISIONAL PATENT APPLICATION

Assignee: Quantum Medical Transport, Inc. a Delaware Public Company.

Description

FIELD OF THE INVENTION

- [0002]

The present invention known as **QuantH V1.0** generally relates to an interoperable secure healthcare data exchange via blockchain data storage platform in a fully HIPPA compliant manner. More specifically, embodiments of the present invention provide a distributed ledger system and related method for seamlessly linking a plurality of disparate, remote health records sources to enable the real-time collection, processing and centralized storage of health records, along with enabling controlled access to the decentralized storage. The system envisions integration with cloud based blockchain distributed ledger data storage via distributed nodes.

BACKGROUND OF THE INVENTION

- [0003]

In April 2004, in Executive Order 13335, President George W. Bush revealed his vision for the future of health care in the United States. The President's plan involves a health care system that puts the needs of the patient first, is more efficient, and is cost effective. This plan is based on the following tenets:

- Medical information follows consumers (patients) so that they are at the center of their own care
- Consumers (patients) choose physicians and hospitals based on clinical performance results made available to them
- Clinicians have consumers' (patients') complete medical history, computerized ordering systems, and electronic reminders
- Quality initiatives measure performance and support quality-based competition in the industry
- Public health and bioterrorism surveillance is seamlessly integrated into care
- Clinical research is accelerated and post-marketing surveillance will be expanded.

- [0010]

  In order to achieve these and other desired benefits, the President has charged the Secretary of the Department of Health and Human Services (DHHS) with executing this vision and established the Office of the National Coordinator for Health Information Technology (ONCHIT) to develop and maintain a strategic plan to guide the nationwide implementation of interoperable Electronic Health Records (EHRs) in both the public and private health care sectors to facilitate health information exchange. A fully functional platform for secure health information exchange deployed on a regional or national basis could provide the framework for authorized, secure, timely, and accurate exchanges of health information among patients, clinicians and other providers and authorized entities.

- [0011]

  A fully functional platform for secure health information exchange via blockchain distributed ledger deployed on a regional or national basis could provide the framework for authorized, secure, timely, and accurate exchanges of health information among patients, clinicians and other providers and authorized entities. The solution proposed in the present invention, as described below, will allow the widespread exchange of health care information by maximizing interoperability among health care software applications, particularly EMR/EHRs. This approach could be used in support of a National Health Information Network (NHIN) or support Regional Health Information Organizations (RHIOs) and Regional Health Communities (RHCs).

- [0012]

  At the same time, the global market for Health IT is large and expected to grow rapidly. Of that, likely half will be spent on EMR/EHR capabilities. Healthcare organizations are facing increasing sophisticated cybersecurity attacks, which is pushing entities to remain vigilant in keeping protected health information (PHI) secure. The HIPPA Security Rule is a national standard that can help organizations maintain current and comprehensive healthcare data security. The HIPPA Security Rule was designed “to protect the privacy of individuals’ health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care according to HHS. The Security Rule was also created to be flexible for healthcare organizations, allowing entities to implement procedures, policies, and technologies appropriate for the entity, its size, entity structure and risks to patients e-PHI. Healthcare Ransomware attacks Contribute to 2017 Top Data Breaches. The Security Rule requires convered entities to maintain reasonable and appropriate administrative safeguards, technical safeguards, and physical safeguards.

- [0013]

There are many different suppliers to the healthcare market, and these include offerings from mainstream vendors, and also specialized, boutique providers to the health industry. Most current products are specific to a care domain, or provide an extremely “thin” layer of functionality across a care setting. Other products are specific to the underlying architecture and provide, typically, standards based interface to a vendor's business logic and architecture. There is a need for a truly flexible “middleware” architecture that is agnostic to underlying architectures, whilst being able to interface to both existing systems and newly developed technologies in a secure, robust manner protecting both the privacy of patients, and the integrity of the care process.

- [0014]

Healthcare technologies have expanded over the last 25 years typically in an organic manner. This has meant that technologies have developed at the same pace as healthcare, with associated advances in specific areas. To date, technology vendors have addressed their forays into healthcare through the interfacing with existing platforms, or the development of functionality that simply replicates that which is currently offered by competitive vendors. Innovation, such as it is, is led by clinical need rather than technological capability, and, treatment of the healthcare enterprise as a single domain has not occurred.

- [0015]

The healthcare market is a global one, whereas healthcare provision is by necessity regional, and there are few truly country (or nation) wide providers of healthcare. However, political motivations, based upon an understanding of technological potency, are driving the need for an enterprise approach to healthcare that pushes the boundaries of existing technologies. Indeed, the drive for a truly national healthcare record is one that will require extensive innovation and evolution of current technologies with novel approaches being required to seemingly intractable problems.

- [0016]

While other countries, including the United Kingdom and Australia, have attempted to create a national, centralized medical record repository, these efforts have met mixed results. Furthermore, the methods employed in other countries partially rely on state control of health facilities, thereby allowing systemic harmonization of health records which is not possible in the United States where the privately created health records may have varying formats and contents. Moreover these previous solutions could not be scaled to operate with the significantly larger number of medical records in the United States, the world's largest health care market.

- [0017]

QuantH V1.0 leading the path toward secure blockchain-based medical records storage and sharing implementation of a patient controlled, blockchain-based system. To understand how blockchain technology can improve the security and efficiency of electronic health data storage and sharing, it is first necessary to provide an overview of blockchain technology and its benefits.

Blockchain technology rests on three foundational principles. First, data is stored in a public, indestructible transaction ledger that anyone can read. Because the transactions can never be deleted or changed, there is always a complete and irrefutable record of all transactions. Second, blockchains are implemented in a decentralized network of computing nodes, which makes them robust against failures and attacks. Decentralization also means that no entity owns or controls the blockchain. Third, the metadata describing each transaction is available to everyone on the system, but that does not mean the data stored within the blockchain is readable. Blockchain relies on pseudoanonymity (replacing names with identifiers) and public key infrastructure (PKI), which allows the blockchain's contents to be encrypted in a way that is prohibitively expensive to crack. When applying blockchain technology to health data, each of these foundational principles apply.

Distributed Healthcare Transaction Ledger

Healthcare providers, payers and patients would contribute encrypted data, which would reference a patient ID, to a public blockchain. This could include clinical data that is stored in EHR systems today; claims history and gaps in care from payers; and family history and device readings from patients. This information would be encrypted and stored in the blockchain and could only be decrypted by parties that have the patient's private key.

Because the ledger is indestructible, no one can erase or alter the record. Updates include metadata records of the date, time, location and entity making the update. In this way, a blockchain-based medical record will be self-auditing.

Public Key Cryptography is an encryption system that uses pairs of keys: a "public key" available to everyone and a "private key" that is known only to its holder. Either key may be used to encrypt a message, but the other key must decrypt the message. Practically speaking, there are two use cases involving public and private keys. First, a sender can encode a message with a public key and be sure that only the holder of the private key can decrypt it. Second, a message or document can be encrypted with a private key. If the message makes sense when it is decrypted using the corresponding public key, it's guaranteed that the holder of the private key is the party that encrypted the message. This is sometimes called "signing" a message because it is analogous to someone putting his unique signature on a document.

Blockchain also supports a concept called M-of-N signatures or “multisig,” meaning that there are a total of N cryptographic keys, and at least M of them have to be present in order to decrypt the data. In this way, the patient can provide keys to authorized caregivers, doctors and others to grant access without the patient’s specific key. This is useful when the patient is incapacitated and cannot provide consent to access the data.

Public Key Cryptography is an important concept for blockchain. All transactions are signed with private keys as a way of establishing the participants’ identities. In the context of storing healthcare data in a blockchain, cryptography would have the additional role of encrypting the contents of the message, so that only intended users can read its contents.

Currently in the ecosystem of health records, each hospital or health system serves as its own central authority to provide record keeping and transmission services.

The traditional, centralized transaction infrastructure is a natural solution to the problem. While it has many advantages, there are also drawbacks. A centralized infrastructure is vulnerable to hackers using ransom ware, failure, corruption and attack. This architecture causes the information silos that are prevalent in healthcare today to be significantly vulnerable.

Blockchain replaces the centralized infrastructure with a distributed one. The blockchain software is running on thousands of nodes distributed across an entire network globally. To process a transaction, it is distributed to all the network nodes, and the transaction is cleared when the nodes have reached a consensus to accept the new transaction into the common ledger.

The process is technologically sophisticated, but it replaces entire record keeping and transaction processing institutions. This lowers transaction overhead in terms of price and execution time. It also means there is no single point of failure, providing a more robust, safer infrastructure.

Implementation of the QuantH Blockchain Solution

To implement a blockchain-based healthcare record system, EHRs and other record keeping systems would encrypt and send a transaction containing patient care documents – encounter notes, prescriptions, family histories, etc. – into the public healthcare blockchain. The transaction would include a digital signature from the contributor to trace provenance and the patient’s blockchain ID as the recipient of the transaction.

After the documents are stored in the blockchain, patients would use a web-based or mobile application to view their blockchain contents and to grant or revoke access to specific parties via their private key.

The distributed blockchain system has a number of advantages over current methods of record keeping:

1. Patients become the platform, owning and controlling access to their healthcare data. This removes all obstacles to patients acquiring copies of their healthcare records or transferring them to another healthcare provider.

2. Because data is stored on a decentralized network, there is no single institution that can be robbed or hacked to obtain a large number of patient records.

3. Data is encrypted in the blockchain and can only be decrypted with the patient's private key. Even if the network is infiltrated by a malicious party, there is no practical way to read patient data.

4. The infrastructure itself provides auditing and non-repudiation capabilities. The methods used to add the data to the blockchain also include tamperproof timestamps, account IDs, and methods of determining if the contents have been altered.

A blockchain-based method of storing healthcare data includes all the expected criteria of a medical record keeping system, and it goes beyond what a traditional, centralized system can do because it improves patients' access to their records and strengthens security against data breaches.

The proposed solution begins with today's health IT systems, primarily EHRs, but also potentially includes laboratory information systems, radiology systems, payer databases, medical devices and consumer devices. These systems will continue to operate as they do today, storing data in their proprietary databases. In addition to storing its own copy of the data, each system will also transmit a copy to the blockchain-based PHR.

All EHR systems that are Meaningful Use compliant must provide the ability for patients to view, download and transmit their health information in human readable as well as machine readable format15. The document format is C-CDA, a machine-readable XML format. By applying a style sheet to the C-CDA document, it becomes an HTML file that can be read by a human using a web browser.

Many health systems satisfy the view/download/transmit criterion by making C-CDA documents available to the patient on a patient portal. From there, the patient can download or forward the document to the destination of their choice. Some EHR systems also offer other methods of transmission that do not require a patient portal.

There are two primary options for connecting an EHR's view/download/transmit function to a blockchain-based PHR:

Option 1: EHR vendors implement a blockchain client within their EHR software that communicates health information directly and automatically to the blockchain-based PHR. This would be the preferred option, but it requires effort and cooperation on the part of EHR vendors.

Option 2: EHR vendors use existing protocols, such as REST, SOAP or Direct Messaging to send health information to a blockchain-based PHR, which is equipped to receive data according to these standards. This would mean that the blockchain-based PHR would need to be able to handle these communication protocols and configured to receive documents from various sources.

Patient Granting Access

- Patient A grants access to EHR to Practitioner A
- Practitioner A's ID is added to Patient A's authorized asset on the ledger
- Patient A's ID is added to Practitioner A's authorized asset on the ledger
- The Symmetric key for the EHR is decrypted with Patient A's private key
- Symmetric key is then encrypted with Practitioner A's public key

Patient Revoking Access

- Patient A revokes access from Practitioner A
- Practitioner A's ID is removed from Patient A's authorized asset
- Patient A's ID is removed from Practitioner A's authorized asset
- Patient A's private key is used to decrypt Symmetric key for EHR which is used to decrypt the EHR
- The EHR is encrypted with a new Symmetric key
- The new Symmetric key is encrypted with Patient A's public key and the public keys of all the remaining ID's that have permission.

Practitioner Referring Patient

- Practitioner A updates the permissions to allow Practitioner B to access the Patient's EHR.
- Chaincode will check that the Practitioner A has permission on the EHR.
- Practitioner A uses its private key to decrypt the EHR's symmetric key
- Practitioner B's public key is used to encrypt the Symmetric key
- Practitioner B's ID is added to Patient A's authorized asset
- Patient A's ID is added to Practitioner B's authorized asset

In essence, the blockchain is a shared database. Unlike a traditional database, however, there is no central ownership. Instead, data is managed through the consensus of participants in a network, who work together (with the help of cryptography) to decide what gets added, while each participant maintains an identical, full copy of all transactions. The network can be public (like bitcoin, open to anyone) or private (restricted to certain members). When new information needs to be added, every computer on the network is notified and updates its copy accordingly. The result is an expansive and distributed source of truth — built not from trust, but through cryptographically enforced consensus. Yet blockchain's most important attribute is its immutability: once something has been added, it is permanent — stored across thousands of computers, cryptographically locked in history.

The technical details of how this is done are somewhat complex, but involve public/private key encryption (for anonymity), proof-of-work (for agreement on what gets added to the ledger), longest-chain rule (for resolving conflict), and peer-to-peer networks (for communication).

SUMMARY OF THE INVENTION

- [0025]

The solution described herein documents a novel approach to building and deploying a HIPPA Compliant Secure Medical Blockchain technology platform that enables the exchange of semantically normalized data between different health care institutions. Embodiments of the present invention provide a system and related method for seamlessly linking a plurality of disparate, remote health records sources to enable the real-time collection, processing and de-centralized storage of health records, along with enabling controlled access to the de-centralized storage. This platform can be used to support clinical care at the regional or national level, public health surveillance, clinical trials, drug monitoring, care management initiatives, ePrescriptions, and other health care processes.

- [0026]

Here are some of the other ways that QuantH V1.0 Medical blockchain platform may benefit health care:

- *Clinical data sharing*. Advance directives, genetic studies, allergies, problem lists, imaging studies, and pathology reports are just some of the data elements that could be distributed. Alternately, instead of storing actual patient data, blockchain could be used to store access controls — like who a patient has authorized to see their health data — even if the clinical data itself is stored by the EHR.
- *Public health*. A shared, immutable stream of de-identified patient information could more readily identify pandemics, independent of governmental bodies currently aggregating this data — for example, an influenza reporting system.
- *Research and clinical trials*. Distributing patient consent or trial results could foster data sharing, audit trials, and clinical safety analyses.
- *Administrative and financial information*. Insurance eligibility and claims processing workflows could benefit from blockchain and have decreased transactional costs.
- *Patient and provider identity*. National (or international) patient or provider identities could be secured in the blockchain, providing the basis for health data portability and security.
- *Patient-generated data*. Personal health devices, “wearables,” “Internet of Things” (IOT) devices, and patient-reported outcomes are just some examples of patient-generated data that could leverage the blockchain for security and sharing.

The greatest potential of QuantH blockchain technology is the empowering of patients to own and gather their own data. Our health information technology framework — directly disrupts the siloed, centralized data stores that dominate health care data today.

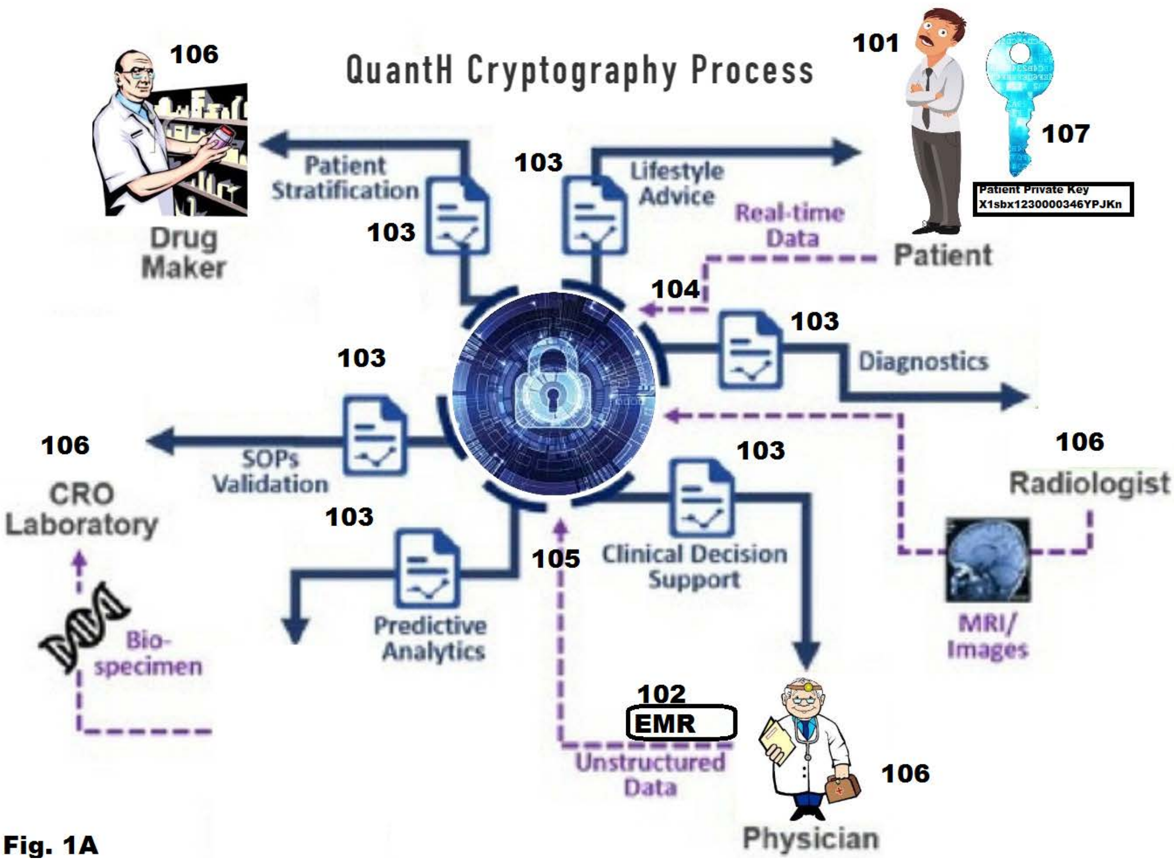

Fig. 1A

BRIEF DESCRIPTION OF THE DRAWINGS

- [0027]

  A more complete understanding of the present invention and advantages thereof may be acquired by referring to the following description taken in conjunction with the accompanying drawings in which like reference numbers indicate like features, and wherein:

- [0028]

  FIGS. **1**A is a high-level schematic diagram of an interoperable healthcare data exchange platform accordance with embodiments of the present invention;

- [0029]

  FIG. 1A depicts high-level schematic diagram of QuantH V1.0 a secure blockchain data output system for the an interoperable healthcare data exchange platform in accordance with embodiments of the present invention;

- [0030]

FIGS. 1A -101 depicts Patient also known as user agrees to share health data. A Heath wallet creates pseudonymous address known as public key and stores as smart contract on the blockchain. User gives permission for certain release of medical records under specific conditions via private key. Once permission is granted only permissioned personnel can access.

- [0031]

FIG. 1A-102 is a schematic diagram of EHR health data collection network that transmits patient permissioned medical records to blockchain nodes or blockchain cloud through encryption in accordance with embodiments of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

- [0032]

FIG. 1A-103 depicts an interoperable healthcare blockchain distributed ledger of medical records data exchange network. Specifically, the network **103** which includes fully permissioned medical facility, practitioner, researcher, pharmacy, imaging or insurance company. As described in greater detail below, the network **103** appends updated or adds new records or collects health care data from multiple disparate electronic health records (EHR) systems **102** at various locations. The EHRs, for example, may be associated with doctors, hospitals, other treatment centers, insurance companies, etc. Consequently, the various EHR systems **102** store the EHR in different formats and protocols. In response, in the network **102**, each of the EHR systems **102** has an associated interface adapter **102** for preparing and standardizing the EHR for transmission to a messaging handling node that verifies, authenticates and appends to the blockchain corresponding to the pseudonymous patient record in the distributed ledger. For example, interface adapter **102** known as the EHRs appends, a standardized XML schema for the transmission and processing of health records. The a messaging handling node **105** receives the standardized EHRs and forwards the standardized EHRs to the decentralized blockchain to store and organize the standardized EHRs to allow the stored, standardized EHRs to be accessed and processed as needed by the authenticated and fully permissioned medical facility, practitioner, researcher, pharmacy, imaging or insurance company.

- [0033]

FIGS. **1**A-104 comprises a general overview of the interoperable healthcare blockchain data exchange platform **105** of the present invention. The interoperable healthcare data exchange platform **104** records the transaction and creates an audit trail in the distributed ledger which cannot be altered, via remote General Practice (GP) applications **102** generally representing provider systems containing electronic health records (EHRs) **102** to enable the real-time collection, processing and de-centralized storage of health records in the blockchain **105**, along with enabling controlled access to the centralized storage.

- [0034]

FIGS. **1**A-105 As described is the pseudonymous health data blockchain maintained on a distributed ledger of nodes, which are independent servers that are part of the worldwide blockchain. No single node contains a complete patient set of records, thus creating a high level multi-sig secure data storage protocol that is only accessible via patient private key leaving the patient in control of their medical records.

- [0035]

FIGS. **1**A-106 Patient authorized fully permissioned medical facility, practitioner, researcher, pharmacy, imaging or insurance company append, update and share health records data in real time, messages containing electronic medical data **102** input from multiple of general purpose (GP) applications **106** representing various, disparate providers and sources of health records **102**.

- [0036]

FIGS. 1A-107 Describes Public Key Cryptography is an encryption system that uses pairs of keys: a “public key” available to everyone and a “private key” that is known only to its holder. Either key may be used to encrypt a message, but the other key must decrypt the message. Practically speaking, there are two use cases involving public and private keys. First, a sender can encode a message with a public key and be sure that only the holder of the private key can decrypt it. Second, a message or document can be encrypted with a private key. If the message makes sense when it is decrypted using the corresponding public key, it’s guaranteed that the holder of the private key is the party that encrypted the message. This is sometimes called “signing” a message because it is analogous to someone putting his unique signature on a document.

Blockchain also supports a concept called M-of-N signatures or “multisig,” meaning that there are a total of N cryptographic keys, and at least M of them have to be present in order to decrypt the data. In this way, the patient can provide keys to authorized caregivers, doctors and others to grant access without the patient’s specific key. This is useful when the patient is incapacitated and cannot provide consent to access the data.

Public Key Cryptography is an important concept for blockchain. All transactions are signed with private keys as a way of establishing the participants’ identities. In the context of storing healthcare data in a blockchain, cryptography would have the additional role of encrypting the contents of the message, so that only intended users can read its contents.

Currently in the ecosystem of health records, each hospital or health system serves as its own central authority to provide record keeping and transmission services.

The traditional, centralized transaction infrastructure is a natural solution to the problem. While it has many advantages, there are also drawbacks. A centralized infrastructure is vulnerable to hackers using ransom ware, failure, corruption and attack. This architecture causes the information silos that are prevalent in healthcare today to be significantly vulnerable.

Blockchain replaces the centralized infrastructure with a distributed one. The blockchain software is running on thousands of nodes distributed across an entire network globally. To process a transaction, it is distributed to all the network nodes, and the transaction is cleared when the nodes have reached a consensus to accept the new transaction into the common ledger.

The process is technologically sophisticated, but it replaces entire record keeping and transaction processing institutions. This lowers transaction overhead in terms of price and execution time. It also means there is no single point of failure, providing a more robust, safer infrastructure.

- [0116]

Embodiments of the present invention enable the operating and maintaining of a RHIO. The ability to normalize data and interface with a wide variety of systems results in an architecture that can scale and promote the sharing of health care data across a wide variety of provider organizations and systems. For example, the data blockchain **105** may be operated by a service provider such as a Regional Health Information Organization (RHIO) which would initially be comprised of affiliated hospitals, staff, laboratories, physicians, care givers, intermediate and long term care providers and pharmacies. Each would have access to the RHIO operated central server and each would have an encryption code for its list of patients. That code would enable unidirectional input on a unique patient by patient basis to the central server, subject only to input programming criteria to insure clean data and limited bidirectional communication to confirm data receipt and to control the standardization of data, i.e., insure it is clean data. The encryption code would be secured through the patient hardware key plus the user name and password of the provider. This combination of code input would insure communication uniquely solely with the patient's record for input purposes only since the provider would not have the patient name and password. Rather, the combination of key code with provider name and password would limit the provider (via the server program software) to data input only in one preferred embodiment.

- [0117]

The RHIO would preferably create a backup record of all input data on a real time basis. That backup data record would replicate the RHIO data in case of system failure and would immediately be on line upon detection of a system failure. Such redundancy is a preferred feature of the system and would provide a source of information that could be separately used for research.

- [0118]

  That is, certain fields of information could be rendered inaccessible for research purposes, such as name, address, social security number, etc. However, other fields of information could be made available for statistical research. Such research access could be subject to pre-access approval by the RHIO or other server operator and could also comprise an income source for the RHIO, e.g., payment for access to the medical information regarding the history of certain drug use. Again, the access to information would require patient permission that would be solicited and obtained upon assignment of and providing the patient with a key device, password, etc. All at the same time the patient would also likely provide various medical instructions such as a living will, organ donation information, emergency instructions, etc.

- [0119]

  Emergency access by certain providers could be insured by a combination of the authorized providers key code and the patient name and/or password, and/or encryption key. For example, an emergency medical service (EMS) may have an encryption key device that, in combination with the device or password and/or name of an accident victim, provides access to that victim/patient's medical record. Thus, the patient/victim may have an RFID device, a USB device, or even a “smart card” which in combination with the EMS encryption key will permit access to the unique medical record of the patient/victim. The available information will typically, in such circumstances, comprise an emergency subset of patient information per a program that limits the information to the “need to know in emergency situation.”

- [0120]

  As can be seen, the system eliminates duplication of records, standardizes record keeping, permits access as needed, provides for contribution of information by multiple sources and most importantly is dependent upon patient participation.

- [0121]

  The platform **105** of the present invention integrates both existing software assets and new technologies along with operating and execution processes to develop a technology platform, repeatable operational and development architecture and processes that support the ability to manage dynamic data from multiple types of stakeholders—patients, providers, etc. as well as aggregating data from multiple, different clinical systems and EHRs within and across health provider organizations, laboratories, health insurance organizations and/or governmental agencies, by using common acquisition, interoperability, transformation and transaction and medical terminology normalization processes.

- [0122]

  In this way, the platform **105** effectively merges patient records from multiple sources and avoids duplicate records that result in increased errors and decrease information availability. The platform further enables authorized, secure, timely, and accurate exchanges of semantically normalized health information among patients, clinicians, other providers and authorized entities. The platform further provides a scalable security and access architecture to facilitate trust, auditing and cross-domain data access management that facilitates interoperability and/or federation. Overall the platform provides a robust data model and de-identification/re-identification capabilities, supporting the secondary use of patient information (e.g. epidemiology studies, biosurveillance activities, screening, quality assurance, cost containment, clinical research and disease management) Secondary Uses means those uses that are not the provision of direct healthcare to a patient or group of patients. The Platform may further optionally provide for the provision of analytical facilities to support secondary uses, as well as supporting a National Health Information Network (NHIN), Regional Health Information Organizations (RHIOs) and Regional Health Communities (RHCs) in exchanging information and be flexible for the growth and scalability of these initiatives.

- [0123]

  Embodiments of the present invention provide readily available packaged solutions for most the architecture's technical components. Given the diverse and rapidly expanding landscape of possible technology solutions for the architecture, selecting the most appropriate solution for the architecture will require discussions and evaluation of the existing environment. Therefore, in this response potential vendors are mentioned but this is purely for indicative purpose and not a formal selection.

- [0124]

  Moreover, the present invention provides innovative emerging solutions to provide high value for the architecture. For example, a networking solution, such as Oracle Cloud Blockchain may play a vital role in the proposed solution. The networking solution may be leveraged to develop a standard architecture layer for member institutions. The (OCBD) can be rapidly deployed and will provide the advanced security and manageability required in the architecture's distributed architecture. QuantH V1.0 has agreed to enter Beta testing with Oracle.

Patent Citations (6)

Publication number Priority date Publication date Assignee Title

US20010034615A1 *2000-03-152001-10-25 Gregg WilkinsonApparatus for and method of assessing, monitoring, and reporting on behavioral health disorders
US20040083217A1 *2002-10-252004-04-29 Cameron Brackett Method, system, and computer product for collecting and distributing clinical data for data mining
US20060100738A1 *2002-12-192006-05-11 Koninklijke Philips Electronics N.V. Method and apparatus for selecting the operating parameters for a medical imaging system
US20060129435A1 *2004-12-152006-06-15 Critical Connection Inc. System and method for providing community health data services
US7685262B2 *2003-01-242010-03-23 General Electric Company Method and system for transfer of imaging protocols and procedures
Family To Family Citations
WO2005088506A1 *2004-02-272005-09-22 Guidant Corporation Systems and methods for accessing and distributing medical information
* Cited by inventor

Cited By (115)

Publication number Priority date Publication date Assignee Title
US20040172558A1 *2002-11-182004-09-02 Terrance Callahan Method and system for access control
US20060222003A1 *2005-03-292006-10-05 Oracle International Corporation HTB gateway for healthcare transaction base
US20070265879A1 *2006-03-312007-11-15 Cerner Innovation, Inc. Method for automated configuration, implementation and/or maintenance of a healthcare information system
US20070276869A1 *2006-03-312007-11-29 Cerner Innovation, Inc. Method for selectively associating content items with pre-configured alternatives based upon directed user input
US20070294111A1 *2006-06-142007-12-20 General Electric Company Systems and methods for identification of clinical study candidates
US20080015895A1 *2006-03-312008-01-17 Cerner Innovation, Inc. Automated configuration, implementation and/or maintenance of a healthcare information system
US20080021572A1 *2006-04-212008-01-24Tadayuki Yamaguchi Quality control system and quality control information delivery device
US20080263187A1 *2007-04-232008-10-234 Dk Technologies, Inc. Interoperability of Network Applications in a Communications Environment
US20080270185A1 *2007-04-302008-10-30 Thomas Gossler Method and device for providing a medical report
US20080294463A1 *2007-01-262008-11-27 Cerner Innovation, Inc. System-determined indication for facilitating the conversion of medication claims to active medications
US20090150451A1 *2007-12-072009-06-11 Roche Diagnostics Operations, Inc. Method and system for selective merging of patient data
US20090327297A1 *2008-06-272009-12-31 Microsoft Corporation Establishing patient consent on behalf of a third party
US20090326982A1 *2008-06-272009-12-31 Microsoft Corporation Establishing a patient - provider consent relationship for data sharing
US20090326983A1 *2006-05-242009-12-31 Kunz Linda H Data collection and data management system and method for use in health delivery settings
US20090326981A1 *2008-06-272009-12-31 Microsoft Corporation Universal health data collector and advisor for people
US20100030580A1 *2005-06-072010-02-04 Angadbir Singh Salwan Physician to patient network system fo real-time electronic communication & transfer of patient health information
US20100088117A1 *2008-10-022010-04-08 Siemens Medical Solutions Usa, Inc. Multi-Mode Medical Data Reporting System
US20100145727A1 *2008-12-082010-06-10 Microsoft Corporation Interaction between healthcare software products
US20100161354A1 *2008-12-222010-06-24 Joon Ho Lim System and method of providing health care using universal health platform

US20100169121A1 *2008-12-312010-07-01 Cerner Innovation, Inc. Patient to device association based on suggested devices
US20100169120A1 *2008-12-312010-07-01 Cerner Innovation, Inc. Patient to device association
US20100257190A1 *2009-04-012010-10-07 Ariel Farkash Method and System for Querying a Health Level 7 (HL7) Data Repository
WO2010124137A1 *2009-04-222010-10-28 Millennium Pharmacy Systems, Inc. Pharmacy management and administration with bedside real-time medical event data collection
US20100287006A1 *2009-05-072010-11-11 Cerner Innovation, Inc. Clinician to device association
US20110077910A1 *2009-09-292011-03-31 Electronics And Telecommunications Research Institute Universal adapter for personal health device standardization of non-standardized healthcare device and operating method thereof
US20110077965A1 *2009-09-252011-03-31 Cerner Innovation, Inc. Processing event information of various sources
US20110093519A1 *2009-10-192011-04-21 Ios Health Systems, Inc. System and method of employing a client side device to access local and remote data during communication distruptions
US20110106564A1 *2009-10-302011-05-05 Don Hachmeister Electronic medical records interoperability
US20110145014A1 *2009-12-152011-06-16 Suzette Jacqueline Avneri International life-saving rapid retrieving tool
US20110173168A1 *2010-01-122011-07-14 Microsoft Corporation Data versioning through data transformations
WO2011089568A1 *2010-01-212011-07-28 Indegene Life systems Pvt. Ltd. Method for organizing clinical trial data
US20110202556A1 *2010-02-122011-08-18 Unival, Inc. Dynamic data management system and method for collecting data from disperse sources in real-time
US20110246224A1 *2009-02-252011-10-06 Greenway Medical Technologies, Inc. System and method for analyzing, collecting, and tracking quality data across a vast healthcare provider network
US8050938B12002-04-192011-11-01 Greenway Medical Technologies, Inc. Integrated medical software system with enhanced portability
US20120041783A1 *2010-08-132012-02-16 Mckee John Henry Integrated Electronic Patient Health Care and Billing Coordination System
US20120046969A1 *2010-08-182012-02-23 Roy Schoenberg Converting Medical Data to a Data Format for Exportation from a Brokerage System
US20120072235A1 *2010-09-162012-03-22S RM Institute of Science and Technology System and Method for Personal Healthcare Analysis and Distributable Archive
US20120117158A1 *2010-11-052012-05-10 Mark Cummings Collaborative computing and electronic records
US20120124080A1 *2010-11-162012-05-17 Mckesson Financial Holdings Limited Method, apparatus and computer program product for utilizing dynamically defined java implementations for creation of an efficient typed storage
US20120136676A1 *2007-10-312012-05-31 AT&T Intellectual Property I, L.P. Method and apparatus for multi-domain anomaly pattern definition and detection
US20120173475A1 *2010-12-302012-07-05Cerner Innovation, Inc. Health Information Transformation System
US20120173585A1 *2010-12-302012-07-05Yue Pan Obtaining hierarchical information of planar data
US20120215560A1 *2010-07-212012-08-23dbMotion Ltd. System and methods for facilitating computerized interactions with emrs
US20120215860A1 *2011-02-212012-08-23 General Electric Company Methods and systems for receiving, mapping and structuring data from disparate systems in a healthcare environment
CN102651051A *2011-02-282012-08-29 国际商业机器公司 System and method for identifying clinical pathway implementation deviation
US20120239824A1 *2011-03-172012-09-20 Carefusion 303, Inc. Scalable communication system
US20130006665A1 *2010-12-292013-01-03 Unival, Inc. Remote data management system with business intelligence in real-time
WO2013016324A2 *2011-07-252013-01-31 Atlas Database Software Corp. System and method for sharing electronic information

WO2013097905A1 *2011-12-292013-07-04 Fundacio Privada Barcelona Digital Centre Tecnologic System and method for extracting and monitoring multidimensional attributes regarding personal health status and evolution
US20130197939A1 *2012-01-262013-08-01 Netspective Communications Llc Social health care record system and method
US20130231957A1 *2012-02-202013-09-05 Medicomp Systems, Inc. Intelligent filtering of health-related information
US8538860B12011-09-162013-09-17 Accushares Holdings LLC System and method for the creation and rebalancing of beneficial interests in index tracking and other investment vehicles over multiple market periods using fixed or regularly resetting prices to calibrate outstanding interest counts with liquidation entitlements
CN103340608A *2013-07-042013-10-09 安徽易科技术有限公司 Method for processing data formats of home-based care health files in differentiated mode
US20130304512A1 *2008-08-052013-11-14 Net.Orange, Inc. System and method for sharing data in a clinical network environment
US20130332873A1 *2012-06-122013-12- 12 Qvera, Llc Health Information Mapping System With Graphical Editor
US20130339053A1 *2012-04-112013-12-19 Children's National Medical Center Regional analysis of electronic health record data using geographic information systems and statistical data mining
US8621489B2 *2009-12-162013-12-31 Koninklijke Philips N.V. Universal medical device driver adapter
US8630935B1 *2011-06-262014-01-14 Jack Fonss System and method for the creation and rebalancing of beneficial interests in tracking investment vehicles over multiple market
US8650045B22010-09-022014-02-11 Medical Management International, Inc. Electronic health record sharing using hybrid architecture
US20140046681A1 *2012-08-132014-02-13 ZirMed, Inc. Response Message Normalization System
US20140047129A1 *2012-08-092014-02-13 Mckesson Financial Holdings Method, apparatus, and computer program product for interfacing with an unidentified health information technology system
US20140129258A1 *2012-11-052014-05-08 Intelligent Medical Objects, Inc. System and Method for Generating and Implementing a Stateless Patient History Module
US8732070B22012-03-152014-05-20 Accushares Holdings LLC System and process for creating, monitoring, and transforming multiple interests of one or more issuer entities at system determined intervals based on a variable or index
US8738396B22002-04-192014-05-27 Greenway Medical Technologies, Inc. Integrated medical software system with embedded transcription functionality
US20140164018A1 *2012-12-122014-06-12 Debra Thesman Methods for administering preventative healthcare to a patient population
US8781853B22002-04-192014-07-15 Greenway Medical Technologies, Inc. Integrated medical software system with location-driven bill coding
US8788679B22008-12-222014-07-22 Koninklijke Philips N.V. Method for exchanging data
US20140207476A1 *2011-06-272014-07-24 Fisher & Paykel Healthcare Limited Data capture and routing system and method
US20140207686A1 *2013-01-212014-07-24Humetrix.Com, Inc. Secure real-time health record exchange
JP2014137698A *2013-01-162014-07-28Hitachi Systems Ltd Medical information analysis system
US20140316810A1 *2013-03-302014-10-23Advantage Health Solutions, Inc. Integrated health management system
US20150006201A1 *2013-06-282015-01-01 Carefusion 303, Inc. System for providing aggregated patient data
US20150019259A1 *2013-06-242015-01-15 Acupera, Inc. Systems and Methods for Establishing and Updating Clinical Care Pathways
US20150095068A1 *2013-10-012015-04-02 Cerner Innovation, Inc. Population health management systems and methods for clinical and operational programs
US20150100347A1 *2013-10-042015-04-09 Shivprasad Nikam Universal online healthcare marketplace
US20150127384A1 *2008-08-052015-05-07 Net.Orange, Inc. Operating system
US20150149362A1 *2015-02-042015-05-28 vitaTrackr, Inc. Encryption and Distribution of Health-related Data

WO2015077898A1 *2013-11-292015-06-04 Plexina Inc. System for converting native patient data from disparate systems into unified semantic patient record repository supporting clinical analytics
US20150161413A1 *2015-02-162015-06-11 vitaTrackr, Inc. Encryption and distribution of health-related data
US20150178454A1 *2007-01-252015-06-25 Alegeus Technologies, Llc Centralized eob archiving and access
US20150187038A1 *2013-12-272015-07-02 General Electric Company System for integrated protocol and decision support
US9075869B1 *2012-08-312015-07-07 Trizetto Corporation System and method for facilitating the collection, analysis, use and management of clinical analytics results to improve healthcare
US20150205846A1 *2014-01-212015-07-23 PokitDok, Inc. System and method for dynamic document matching and merging
US9111018B22010-12-302015-08-18 Cerner Innovation, Inc Patient care cards
US9129046B22013-02-252015-09-084 Medica, Inc. Systems and methods for managing a master patient index including duplicate record detection
WO2015148614A1 *2014-03-282015-10-01 Hc1.Com, Inc. System and method for multi-tenant healthcare relationship management
US9183064B22011-12-302015-11-10 General Electric Company Intelligent mediation of messages in a healthcare product integration platform
WO2016003902A1 *2014-06-302016-01-07 Baxter Corporation Englewood Managed medical information exchange
US20160042124A1 *2014-08-082016-02-11 Practice Fusion, Inc. Electronic health records data management systems and methods
WO2016019465A1 *2014-08-052016-02-11 Complete Concussion Management Inc. System and method for providing access to electronic medical records
US20160117293A1 *2014-10-232016-04-28 International Business Machines Corporation Natural language processing-assisted extract, transform, and load techniques
WO2016071660A1 *2014-11-062016-05-12 Ieso Digital Health Limited Computer-based system for providing psychological therapy
US20160180040A1 *2014-12-232016-06-23 Cerner Innovation, Inc. Predicting glucose trends for population management
US9390153B1 *2012-02-212016-07-12 Dmitriy Tochilnik User-configurable radiological data transformation routing and archiving engine
US20170061081A1 *2011-02-182017-03-02 Mmodal Ip Llc Computer-Assisted Abstraction for Reporting of Quality Measures
WO2017116452A1 *2015-12-312017-07-06 Sole Guerra Alberto System for acquisition, processing and visualization of clinical data of patients
US9734146B12011-10-072017-08-15 Cerner Innovation, Inc. Ontology mapper
US9741001B22000-05-182017-08-22 Carefusion 303, Inc. Predictive medication safety
US9774702B22009-10-192017-09-26 Tritan Software Corporation System and method of employing a client side device to access local and remote data during communication disruptions
US20170287093A1 *2012-02-212017-10-05 Dicom Systems, Inc. User-configurable radiological data transformation, integration, routing and archiving engine
WO2017184176A1 *2016-04-222017-10-26 Merge Healthcare Incorporated Systems and methods for providing aggregated customizable clinical decision support information
US9818164B22009-09-252017-11-14 Cerner Innovation, Inc. Facilitating and tracking clinician-assignment status
US9876852B22015-07-232018-01-23 Microsoft Technology Licensing, Llc Coordinating actions across platforms
US9931252B22011-12-212018-04-03 Sca Hygiene Products Ab Method and computer program for monitoring use of an absorbent product
Family To Family Citations
US8065166B22007-10-302011-11-22 Onemednet Corporation Methods, systems, and devices for managing medical images and records
US9171344B22007-10-302015-10-27 Onemednet Corporation Methods, systems, and devices for managing medical images and records

US8566818B22007-12-072013-10-22 Roche Diagnostics Operations, Inc. Method and system for configuring a consolidated software application
US8365065B22007-12-072013-01-29 Roche Diagnostics Operations, Inc. Method and system for creating user-defined outputs
US8112390B22007-12-072012-02-07 Roche Diagnostics Operations, Inc. Method and system for merging extensible data into a database using globally unique identifiers
US8819040B22007-12-072014-08-26 Roche Diagnostics Operations, Inc. Method and system for querying a database
US7996245B22007-12-072011-08-09 Roche Diagnostics Operations, Inc. Patient-centric healthcare information maintenance
US9003538B22007-12-072015-04-07 Roche Diagnostics Operations, Inc. Method and system for associating database content for security enhancement
US9760677B22009-04-292017-09-12 Onemednet Corporation Methods, systems, and devices for managing medical images and records
CN103364191B *2013-07-012016-01-20 中国航空工业集团公司沈阳发动机设计研究所 A large, test and control remote data exchange method
CN103390062A *2013-07-312013-11-13 常州北大众志网络计算机有限公司 Data conversion and change method of medical detection equipment
* Cited by inventor