Claims

1. An automated data processing method for secure, private, and trusted monitoring, management, and communication of medical information corresponding to a patient, the method comprising:

providing a data communication network;

providing a set of provider-side data processing resources corresponding to a medical care provider associated with the patient, the set of provider-side data processing resources coupled to the data communication network, the set of provider-side data processing resources comprising a provider-side computing system;

providing a set of patient-side data processing resources, the set of patient-side data processing resources coupled to the data communication network, the set of patient-side data processing resources comprising:

a patient identification / biometrics module configured for generating patient identification / biometrics data corresponding to the patient in response to patient input;

a biomarker monitoring device associated with the patient, the biomarker monitoring device configured to monitor a set of patient biomarkers and store corresponding patient biomarker data in a biomarker data store; and

a Personal Identity and Information Manager (PIIM) corresponding to the patient, the PIIM comprising data processing resources configured for establishing direct trust relationships between the PIIM and each of the patient, the biomarker monitoring device, and the care provider;

establishing a first direct trust relationship between the PIIM and the patient by way of: communication between the PIIM and the patient identification / biometrics module following patient input directed to the patient identification / biometrics module, performing patient validation operations, and establishment of a currently active patient identity;

establishing a second direct trust relationship between the PIIM and the biomarker data monitoring device by way of communication between the PIIM and the biomarker data monitoring device under the currently active patient identity, and validation of the biomarker data monitoring device; and

establishing a third direct trust relationship between the PIIM and the care provider by way of communication between the care provider computing system and the PIIM, PIIM validation of the care provider, and provision of a biomarker data decryption key corresponding to the currently active patient identity and the biomarker monitoring device to the care provider computing system or a set of network-based data processing resources couplable or coupled to the set of provider-side computing resources by way of the data communication network, wherein the biomarker data decryption key enables decryption of encrypted biomarker data corresponding to the currently active patient identity and the biomarker monitoring device.

2. The method of claim 1, wherein establishing the first direct trust relationship comprises:

generating patient identification data by way of the patient identification / biometrics module in response to patient interaction therewith;

provision of the patient identification data to the PIIM;

PIIM performance of the patient validation operations using the patient identification data, during which the PIIM attempts to validate the patient identification data;

PIIM generation and storage of a new unique patient identity corresponding to the patient in response to unsuccessful validation of the patient identification data; and

PIIM retrieval of a previously generated and stored unique patient identity as the currently active patient identity in response to successful validation of the patient identification data.

3. The method of claim 2, wherein establishing the second direct trust relationship comprises:

establishing communication between the PIIM and the biomarker monitoring device under the currently active patient identity;

PIIM performance of biomarker monitoring device validation operations in which the PIIM attempts to validate a hardware identity and/or a software identity of the biomarker monitoring device; and

following successful PIIM validation of the hardware identity and/or the software identify of the biomarker monitoring device:

PIIM generation and storage, or PIIM retrieval, of a unique code corresponding to the biomarker monitoring device; and

PIIM generation of an ephemeral biomarker data encryption key by which patient biomarker data can be encrypted during a biomarker monitoring session corresponding to the currently active patient identity.

4. The method of claim 3, wherein as part of the biomarker monitoring device validation operations, the PIIM attempts to validate secure boot protocol data generated by the biomarker monitoring device.

5. The method of claim 3, wherein establishing the third direct trust relationship comprises:

PIIM generation of a biomarker data decryption code corresponding to the active patient identity and the biomarker monitoring device;

PIIM association of the biomarker data decryption code with a unique one-time use code;

communication of the unique one-time use code to the set of provider-side data processing resources;

attempted validation of the one-time use code by way of communication between the set of provider-side data processing resources and the PIIM; and

in response to successful validation of the one-time use code, generating the biomarker data decryption key corresponding to the currently active patient identity and the biomarker monitoring device.

6. The method of claim 5, wherein the set of patient-side data processing resources further comprises a patient computing device corresponding to the patient, and wherein communication of the one-time code to the set of provider-side data processing resources comprises:

communicating the one-time use code from the PIIM to the patient computing device; and

subsequently communicating the one-time use code from the patient computing device to the set of provider-side data processing resources.

7. The method of claim 6, wherein the one-time use code is encoded in a matrix barcode or a Quick Response (QR) code.

8. The method of claim 5, wherein attempted validation of the one-time use code comprises:

communication of an assertion signed by the care provider's digital signature to the PIIM; and

PIIM determination of whether the assertion was digitally signed by a trusted authority or an approved delegate of the trusted authority.

9. The method of claim 1, wherein the PIIM comprises one of: (a) integrated circuitry provided as part of the biomarker monitoring device; (b) integrated circuitry carried by a smart card or a patient identification card belonging to the patient; (c) integrated circuitry associated with a customized Subscriber Identity Module (SIM) card, wherein customized SIM card is carried by a smartphone corresponding to the patient and which forms a portion of the patient-side data processing resources; and (d) a set of program instructions stored in a memory of and executable by a processing unit of a patient computing device corresponding to the patient and which forms a portion of the patient-side data processing resources.

10. The method of claim 1, wherein the provider computing system is configured for executing a patient management application by which a current prescription comprising a current prescription protocol corresponding to the patient is definable by the care provider, wherein the current prescription protocol specifies a biomarker that the patient is to monitor by way of the biomarker monitoring device and a corresponding biomarker monitoring schedule, wherein the set of patient-side data processing resources further comprises a patient computing device executing an automated prescription management agent, and wherein the method further comprises:

communicating the current prescription protocol to the PIIM; and

at least one of automatically:

presenting instructions, coaching, guidance, reminders, or recommendations relating to the current prescription protocol to the patient;

performing biomarker data analysis upon biomarker data generated by the biomarker monitoring device in relation to the current prescription protocol;

performing prescription compliance analysis indicating patient compliance with the current prescription protocol;

adaptively providing the patient with feedback based on patient input, the biomarker data analysis, and/or the prescription compliance analysis; and

adaptively adjusting the current prescription protocol based on patient input, the biomarker data analysis, and/or the prescription compliance analysis

by way of execution of the prescription management agent.

11. The method of claim 10, further comprising communicating the prescription management agent from the set of provider-side data processing resources to the patient computing device by way of the data communication network.

12. The method of claim 11, wherein the prescription management agent comprises a state machine executable by a processing unit of the patient computing device.

13. The method of claim 12, wherein the PIIM comprises a prescription checkbot, and wherein the method further comprises prescription checkbot analysis of prescription management agent state transitions corresponding to execution of the current prescription protocol, and prescription checkbot determination of whether aspects of the current prescription protocol fall outside of or too closely approach recognized or established guidelines or contraindications for patient safety.

14. The method of claim 13, wherein the method further comprises prescription checkbot limiting, restricting, or preventing (a) the presentation of particular instructions, recommendations, or information to the patient, and/or (b) the prescription management agent's adaptive adjustment of particular prescription protocol parameters based on the prescription checkbot's analysis of one or more current prescription protocol state transitions correspondingto execution of the current prescription protocol.

15. The method of claim 10, wherein the patient computing device comprises a smartphone having a memory in which the prescription management agent resides, and a processing unit configured for executing the prescription management agent.

16. The method of claim 1, further comprising:

acquiring patient biomarker data by way of the biomarker monitoring device;

encrypting, storing, and processing the patient biomarker data;

selectively communicating at random times each of dummy data and actual patient data comprising at least one of patient biomarker data, summary data corresponding to patient biomarker data, and an emergency alert to a destination external to the set of patient-side dataprocessing resources and which comprises one of the set of provider-side data processing resources and a set of network based data processing resources couplable or coupled to theset of provider-side data processing resources, wherein the communication of the dummydata to the external destination occurs at least 50% more frequently than the communication of actual patient data to the external destination.

17. The method of claim 16, further comprising avoiding communication of actual patient data corresponding to normal, non-emergency medical situations to the external destination.

18. The method of claim 1 or claim 9, wherein the PIIM comprises a trusted computing base.