PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: Christopher S. Dodson
Nexsen Pruet PLLC
227 West Trade Street
Suite 1550
Charlotte, NC 28202
United States of America

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	19 AUG 2020

Applicant's or agent's file reference	FOR FURTHER ACTION
054232-00031	See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US20/23818	20 March 2020 (20.03.2020)	22 March 2019 (22.03.2019)

International Patent Classification (IPC) or both national classification and IPC
IPC - H04L 29/06, 29/04; G06F 21/62; G16H 50/70 (2020.01)
CPC - H04L 63/0457, 63/0421, 63/166; G06F 21/62; G16H 50/70

Applicant
Nephron Pharmaceuticals Corporation

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☒ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	14 May 2020 (14.05.2020)	Shane Thomas PCT Help Desk Telephone No. 571-272-4300

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US20/23818

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(b)).

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US20/23818

Box No. IV Lack of unity of invention

1. ☒ In response to the invitation (Form PCT/ISA/206) to pay additional fees the applicant has, within the applicable time limit:

   ☐ paid additional fees.

   ☐ paid additional fees under protest and, where applicable, the protest fee.

   ☐ paid additional fees under protest but the applicable protest fee was not paid.

   ☒ not paid additional fees.

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is

   ☐ complied with.

   ☒ not complied with for the following reasons:

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-27 are directed towards a method authenticating a network packet by recovering a dual payload using a member of a list of public keys.
Group II: Claims 28-51 are directed towards a system for remote management of patient compliance pushing packets to network coordinates.

The inventions listed as Groups I-II do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical features of Group I include at least a method for processing data from mobile medical devices, comprising: receiving a network packet, the network packet comprising a first digital signature; authenticating the network packet by recovering the dual payload from at least the first digital signature using a member of a list of public keys assigned to authorized data sources; using the member of the list of public keys to identify a patient; inserting the anonymous data into a record for the patient in a privacy-compliant database; and
pushing the anonymous data to a distributed ledger without any patient identification information, which are not present in Group II.

The special technical features of Group II include at least a system for remote management of patient compliance, comprising: a processor; a non-transitory computer readable memory in communication with the processor; a data source in communication with the processor; a reference to predetermined network coordinates stored in the memory; use instructions for treating a medical condition stored in the memory, and program code stored in the memory, the program code executable by the processor to perform data communication operations, the data communication operations comprising: processing signals from the data source to obtain device data; inserting dual payloads and device signatures applied to the dual payloads into network packets; device signatures applied to the hashes; and pushing the network packets to the predetermined network coordinates in response to internally-generated prompts, which are not present in Group I.

The common technical features shared by Groups I-II are a mobile medical device; a first payload of the dual payload; a second payload of the dual payload comprising a digital signature and a hash.

However, these common features are previously disclosed by US 2019/0036688 A1 to THIRDWAYV, INC. (hereinafter "THIRDWAYV"). THIRDWAYV discloses a mobile medical device (mobile device communicating with a glucose monitor; para [0023]); a first payload of the dual payload (communicating one or more payloads (first of the dual payload); para [0102]); a second payload of the dual payload comprising a digital signature and a hash (communicating one or more payloads (second of the dual payload) comprising a digital signature computing using a secure hash output value; para [0102]).

Since the common technical features are previously disclosed by THIRDWAYV, these common features are not special and so Groups I-II lack unity.

4. Consequently, this opinion has been established in respect of the following parts of the international application:

   ☐ all parts.

   ☒ the parts relating to claims Nos. Group I: Claims 1-27

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US20/23818

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-27	YES
	Claims	none	NO
Inventive step (IS)	Claims	none	YES
	Claims	1-27	NO
Industrial applicability (IA)	Claims	1-27	YES
	Claims	none	NO

2. Citations and explanations:

Claims 1-2, 3/1,3/2, 4/1,4/2, 5/1,5/2, 6/1,6/2, 7/6/1,7/6/2, 8/7/6/1,8/7/6/2, 9/1,9/2, 10/1,10/2, 11/1, 11/2, 13/1, 13/2, 14, 15, 17/1, 17/2, 19/1, 19/2, 20/1, 20/2, 27/1, 27/2 lack an inventive step under PCT Article 33(3) as being obvious over US 2017/0272410 A1 to MPH TECHNOLOGIES OY (hereinafter "MPH") in view of WO 2018/201009 A1 to ANONOS INC (hereinafter "ANONOS").

As per claim 1, MPH discloses a method for processing data from mobile devices (secure forwarding of messages (processing data) between computers that use mobility signaling (mobile devices); para [0053]), comprising: receiving a network packet (an encapsulated message (network packet) is sent to an intermediate computer; para [0040]), the network packet comprising a first digital signature and a dual payload (the message sent (network packet) contains a unique identity including an SPI value (first digital signature) and an Encapsulating Security Payload/ESP+Authentication Header/AH bundle (dual payload); para [0042]), a first payload of the dual payload comprising anonymous data (the Encapsulating Security Payload/ESP (first payload) encapsulates the packet securely (anonymous data); para [0080]), a second payload of the dual payload comprising a second digital signature and a hash (the Authentication Header/AH (second payload) includes a Security Parameters Index/SPI (hash) and IPsec sequence number of the unique identity (second digital signature); para [0042]); authenticating the network packet by recovering the dual payload from at least the first digital signature (the bit string, or SPI (first digital signature), is used in SPI translation ensuring the gateway accepts the packet (recovering the dual payload), where the security gateway checks the authenticity of the packet before decryption; para [0084], [0086], [0131]) using a member of a list of public keys assigned to authorized data sources (decryption is done using Internet Key Exchange/IKE keys (a member of a list of public keys) as part of the IKE protocol between the first computer and intermediate computer (authorized data sources); para [0131]). MPH does not disclose wherein the mobile devices are mobile medical devices; using the member of the list of public keys to identify a patient; inserting the anonymous data into a record for the patient in a privacy-compliant database; and pushing the anonymous data to a distributed ledger without any patient identification information. ANONOS discloses wherein the mobile devices are mobile medical devices (data subjects utilize mobile smart devices in the medical services context; para [097], [0221]); using the member of the list of public keys to identify a patient (authentication of a privacy client residing on a Data Subject device (identify a patient) using Association Keys with public key encryption technology (member of the list of public keys); para [035], [0223], [0375]); inserting the anonymous data into a record for the patient in a privacy-compliant database (converting data into Non-Attributing Data Element Values/NADEVs obscured using dynamically changing de-identifiers/DDIDs (inserting the anonymous data into a record) enabling the Data Subject (patient) to operate in a dynamically anonymous manner interacting with data attribute-to-Data Subject association information stored in a database associated with the privacy server (privacy-compliant database); para [014], [035], [053], [0369]); and pushing the anonymous data to a distributed ledger without any patient identification information (storing (pushing) the DDID configured to replace the data obtained from the first data subject (anonymous data) in a first element of a distributed ledger where the data has been de-identified (without any patient identification information); para [0108]; claim 1 of ANONOS). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the mobile devices are mobile medical devices; using the member of the list of public keys to identify a patient; inserting the anonymous data into a record for the patient in a privacy-compliant database; and pushing the anonymous data to a distributed ledger without any patient identification information as disclosed by ANONOS, to gain the advantage of reconciling the tensions between auditable and immutable information stores enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

-***-Continued Within the Next Supplemental Box-***-

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US20/23818

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Claims 19/1, 19/2 are objected to under PCT Rule 66.2(a)(iii) as containing the following defects in the form or contents thereof: Claims 19/1, 19/2 recite "wherein the second payloads are anonymous". As best understood, these are considered typographical errors and will be interpreted as "wherein the second payload is anonymous".

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US20/23818

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Claims 9, 10 are objected to under PCT Rule 66.2(a)(v) as lacking clarity under PCT Article 6 because claims are indefinite for the following reason: Claims 9, 10 refer to "the instructions". There is lack of antecedent basis for these limitations in the claims. As best understood, for the purpose of this written opinion, this is interpreted as "instructions" to restore clarity, continuity and proper antecedent basis to the claims.

Claim 24 is objected to under PCT Rule 66.2(a)(v) as lacking clarity under PCT Article 6 because the claim is indefinite for the following reason: Claim 24 refers to "the ciphertext". There is lack of antecedent basis for this limitation in the claim. As best understood, for the purpose of this written opinion, this is interpreted as "a ciphertext" to restore clarity, continuity and proper antecedent basis to the claim.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US20/23818

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

-***-Continued from Box V: Citations and Explanations-***-

As per claim 2, MPH discloses a method for processing data from mobile devices (secure forwarding of messages (processing data) between computers that use mobility signaling (mobile devices); para [0053]), comprising: receiving a network packet from a mobile device (an encapsulated message (network packet) is sent to an intermediate computer from the first computer (mobile device); para [0040]), the network packet comprising a dual payload (the message sent (network packet) contains a unique identity including an SPI value and an Encapsulating Security Payload/ESP+Authentication Header/AH bundle (dual payload); para [0042]), a first payload of the dual payload comprising anonymous data (the Encapsulating Security Payload/ESP (first payload) encapsulates the packet securely (anonymous data); para [0080]), a second payload of the dual payload comprising a digital signature and a hash (the Authentication Header/AH (second payload) includes a Security Parameters Index/SPI (hash) and IPsec sequence number of the unique identity (digital signature); para [0042]); authenticating the network packet by verifying the digital signature (the unique identity (digital signature) is used in SPI translation ensuring the gateway accepts the packet (verifying), where the security gateway checks the authenticity of the packet before decryption; para [0084], [0086], [0131]) using a member of a list of public keys assigned to authorized data sources (decryption is done using Internet Key Exchange/IKE keys (a member of a list of public keys) as part of the IKE protocol between the first computer and intermediate computer (authorized data sources); para [0131]). MPH does not disclose wherein the mobile devices are mobile medical devices; using the member of the list of public keys to identify a patient; inserting the anonymous data into a record for the patient in a privacy-compliant database; and pushing the anonymous data to a distributed ledger without any patient identification information. ANONOS discloses wherein the mobile devices are mobile medical devices (data subjects utilize mobile smart devices in the medical services context; para [097], [0221]); using the member of the list of public keys to identify a patient (authentication of a privacy client residing on a Data Subject device (identify a patient) using Association Keys with public key encryption technology (member of the list of public keys); para [035], [0223], [0375]); inserting the anonymous data into a record for the patient in a privacy-compliant database (converting data into Non-Attributing Data Element Values/NADEVs obscured using dynamically changing de-identifiers/DDIDs (inserting the anonymous data into a record) enabling the Data Subject (patient) to operate in a dynamically anonymous manner interacting with data attribute-to-Data Subject association information stored in a database associated with the privacy server (privacy-compliant database); para [014], [035], [053], [0369]); and pushing the anonymous data to a distributed ledger without any patient identification information (storing (pushing) the DDID configured to replace the data obtained from the first data subject (anonymous data) in a first element of a distributed ledger where the data has been de-identified (without any patient identification information); para [0108]; claim 1 of ANONOS). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the mobile devices are mobile medical devices; using the member of the list of public keys to identify a patient; inserting the anonymous data into a record for the patient in a privacy-compliant database; and pushing the anonymous data to a distributed ledger without any patient identification information as disclosed by ANONOS, to gain the advantage of reconciling the tensions between auditable and immutable information stores enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

As per claims 3/1 and 3/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. Modified MPH additionally discloses comprising: authenticating the hash by the verifying the second digital signature applied to the hash using the member of the list of public keys (verifying (authenticating) the unique identity comprising the SPI value (hash) and IPsec sequence number (second digital signature applied to the hash) based upon the key exchange protocol (using the member of the list of public keys); para [0042], [0047], [0054]).

As per claims 4/1 and 4/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. MPH does not disclose wherein the member of the list of public keys is assigned to a mobile medical device. ANONOS discloses wherein the member of the list of public keys is assigned to a mobile medical device (authentication of a privacy client residing on a Data Subject device (mobile medical device) using Association Keys with public key encryption technology (member of the list of public keys is assigned); para [035], [0223], [0375]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the member of the list of public keys is assigned to a mobile medical device as disclosed by ANONOS, to gain the advantage enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

As per claims 5/1 and 5/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. MPH does not disclose wherein the anonymous data is pushed to the distributed ledger from a wallet or from a peer in a distributed ledger network. ANONOS discloses wherein the anonymous data is pushed to the distributed ledger (as previously disclosed by ANONOS) from a wallet or from a peer in a distributed ledger network (on a peer-to-peer basis in the distributed ledger network; para [0430]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the anonymous data is pushed to the distributed ledger from a wallet or from a peer in a distributed ledger network as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

-***-Continued Within the Next Supplemental Box-***-

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US20/23818

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

-***-Continued from Previous Supplemental Box-***-

As per claims 6/1 and 6/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. MPH does not disclose wherein the pushing comprises passing instructions and the second digital signature to a peer in a distributed ledger network, the instructions executable by the peer to add the hash to the distributed ledger. ANONOS discloses wherein the pushing comprises passing instructions and the second digital signature to a peer in a distributed ledger network (storing (pushing) the DDID configured to replace the data obtained from the first data subject (passing instructions) in a first element of a distributed ledger where the data has been de-identified using a DDID (second digital signature) linking the transactions on a peer-to-peer basis in the distributed ledger network; para [0108], [0432], [0432]; claim 1 of ANONOS), the instructions executable by the peer to add the hash to the distributed ledger (the algorithmic/programming method (instructions executable) for the peer-to-peer network of computers to chain the blocks (add the hash) in the distributed ledger; para [0430], [0432]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the pushing comprises passing instructions and the second digital signature to a peer in a distributed ledger network, the instructions executable by the peer to add the hash to the distributed ledger as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

As per claims 7/6/1 and 7/6/2, MPH in combination with ANONOS discloses the method of claims 6/1 and 6/2, respectively. MPH does not disclose wherein the pushing further comprises passing a digital signature for the privacy-compliant database applied at least to the instructions and the hash to the peer. ANONOS discloses wherein the pushing further comprises passing a digital signature for the privacy-compliant database (converting data (the pushing) into Non-Attributing Data Element Values/NADEVs obscured using dynamically changing de-identifiers/DDIDs (passing a digital signature) enabling the Data Subject interacting with data attribute-to-Data Subject association information stored in a database associated with the privacy server (privacy-compliant database); para [014], [035], [053], [0369]) applied at least to the instructions and the hash to the peer (the algorithmic/programming method (applied to the instructions) for the peer-to-peer network of computers to chain the blocks (the hash) in the distributed ledger; para [0430], [0432]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the pushing further comprises passing a digital signature for the privacy-compliant database applied at least to the instructions and the hash to the peer as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

As per claims 8/7/6/1 and 8/7/6/2, MPH in combination with ANONOS discloses the method of claims 7/6/1 and 7/6/2, respectively. MPH does not disclose wherein the digital signature for the privacy-compliant database is applied to at least the instructions, the hash, and the second digital signature. ANONOS discloses wherein the digital signature for the privacy-compliant database is applied to at least the instructions, the hash, and the second digital signature (converting data into Non-Attributing Data Element Values/NADEVs obscured using dynamically changing de-identifiers/DDIDs (digital signature for the privacy-compliant database) enabling the Data Subject to operate in a dynamically anonymous manner (applied to the instructions) interacting with data attribute-to-Data Subject association information (the hash) stored in a database associated with the privacy server using the IPsec sequence number (second digital signature); para [014], [035], [053], [0369]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the digital signature for the privacy-compliant database is applied to at least the instructions, the hash, and the second digital signature as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

As per claims 9/1 and 9/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. Modified MPH additionally discloses wherein instructions are obtained from the second payload (the Authentication Header/AH (the second payload) includes a Security Parameters Index/SPI and IPsec sequence number of the unique identity (instructions obtained); para [0042]).

As per claims 10/1 and 10/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. Modified MPH additionally discloses wherein instructions are obtained from the second digital signature (the protocol (instructions obtained) is based on the IPsec sequence number field (second digital signature); para [0051]).

As per claims 11/1 and 11/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. MPH does not disclose authorizing access to at least one of the privacy-compliant database record, a block in a blockchain referencing the hash in the distributed ledger, and the hash in the distributed ledger. ANONOS discloses authorizing access to at least one of the privacy-compliant database record, a block in a blockchain referencing the hash in the distributed ledger, and the hash in the distributed ledger (send the first value related to the first data subject to the first requesting party over the network (authorizing access) in response to the first request when the first requesting party is authorized to receive the first value corresponding to the data attribute-to-Data Subject association information stored in a database (the privacy-compliant database record); para [035]; claim 1 of ANONOS). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include authorizing access to at least one of the privacy-compliant database record, a block in a blockchain referencing the hash in the distributed ledger, and the hash in the distributed ledger as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

-***-Continued Within the Next Supplemental Box-***-

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US20/23818

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

-***-Continued from Previous Supplemental Box-***-

As per claims 13/1 and 13/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. MPH does not disclose wherein the authorized data source comprises a sensor or a dispenser. ANONOS discloses wherein the authorized data source comprises a sensor or a dispenser (enforcing de-identification and/or re-identification policies at the point of data ingress (authorized data source) in communication with sensors; para [0409]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the authorized data source comprises a sensor or a dispenser as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

As per claim 14, MPH in combination with ANONOS discloses the method of claim 2. MPH does not disclose wherein the mobile medical device further comprises a mechanical actuator, wherein the authorized data source is activated into a data collection mode by the mechanical actuator. ANONOS discloses wherein the mobile medical device further comprises a mechanical actuator, wherein the authorized data source is activated into a data collection mode by the mechanical actuator (the programmable device (mobile medical device) may allow a controlling entity to interact through the controlling entity interface 2750 (activated into a data collection mode) using a button (mechanical actuator); para [0584]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the mobile medical device further comprises a mechanical actuator, wherein the authorized data source is activated into a data collection mode by the mechanical actuator as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

As per claim 15, MPH in combination with ANONOS discloses the method of claim 14. MPH does not disclose wherein the mechanical actuator is configured for operation by the patient.
ANONOS discloses wherein the mechanical actuator is configured for operation by the patient (the button (mechanical actuator) to receive input from the user interface (operation) by the Data Subject (patient); para [0576], [0584]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the mechanical actuator is configured for operation by the patient as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

As per claims 17/1 and 17/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. MPH does not disclose wherein electronic health records databases are separate from the privacy-compliant database and the distributed ledger.
ANONOS discloses
wherein electronic health records databases are separate from the privacy-compliant database and the distributed ledger (an original cleartext representation of a source data tables (electronic health records databases) before converting the data into Non-Attributing Data Element Values/NADEVs obscured using dynamically changing de-identifiers/DDIDs stored in the distributed ledger (separate from) and enabling the Data Subject to interact with data attribute-to-Data Subject association information stored in a database associated with the privacy server (separate from the privacy-compliant database); para [014], [035], [053], [0369], [0379]; claim 1 of ANONOS). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein electronic health records databases are separate from the privacy-compliant database and the distributed ledger as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

As per claims 19/1 and 19/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. Modified MPH additionally discloses wherein the second payload is anonymous, with no patient identification information (the Authentication Header/AH (second payload) includes a Security Parameters Index/SPI (anonymous) and an IPsec sequence number (no patient identification information); para [0042]).

As per claims 20/1 and 20/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. MPH does not disclose wherein the second payload comprises a smart contract or reference to a smart contract. ANONOS discloses wherein the second payload comprises a smart contract or reference to a smart contract (the data obtained (second payload) is protected using elements of a smart contract; para [0444]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the second payload comprises a smart contract or reference to a smart contract as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

As per claims 27/1 and 27/2, MPH in combination with ANONOS discloses the method of claim 1 or 2, respectively. Modified MPH additionally discloses wherein the anonymous data comprises at least one duration-of-use for the mobile device (the resulting packet (anonymous data) includes a Time-To-Live field (duration-of-use); para [0099]). MPH does not disclose wherein the mobile device is a mobile medical device; and at least one timestamp. ANONOS discloses wherein the mobile device is a mobile medical device (data subjects utilize mobile smart devices in the medical services context; para [097], [0221]); and at least one timestamp (storing information pertaining to time stamps; para [0253]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the mobile device is a mobile medical device; and at least one timestamp as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]).

-***-Continued Within the Next Supplemental Box-***-

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US20/23818

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

-***-Continued from Previous Supplemental Box-***-

Claim 12 lacks an inventive step under PCT Article 33(3) as being obvious over MPH in view of ANONOS, and further in view of US 2017/0259050 A1 POP TEST LLC (hereinafter "POP").

As per claim 12, MPH in combination with ANONOS discloses the method of claim 2. MPH does not disclose wherein the mobile medical device gathers and transmit data and the further mobile medical devices are drug delivery devices. ANONOS discloses wherein the mobile medical device gathers and transmit data (data subjects utilize mobile smart devices (to gather and transmit data) in the medical services context; para [097], [0221]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the mobile medical device gathers and transmit data as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]). POP discloses the further mobile medical devices are drug delivery devices (drug delivery device configured for wireless communication with other ingestible drug delivery devices (further mobile medical devices); abstract). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include the further mobile medical devices are drug delivery devices as disclosed by POP, to gain the advantage of enabling storage of provenance data of the drug delivery device therein.

Claim 16 lacks an inventive step under PCT Article 33(3) as being obvious over MPH in view of ANONOS, and further in view of US 7634995 B2 to GRYCHOWSKI, J et al. (hereinafter "GRYCHOWSKI").

As per claim 16, MPH in combination with ANONOS discloses the method of claim 2. MPH does not disclose wherein the mobile medical device is a nebulizer. GRYCHOWSKI discloses wherein the mobile medical device is a nebulizer (a nebulizer includes a sensor estimating how much medication is delivered; column 7, line 15-31). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the mobile medical device is a nebulizer as disclosed by GRYCHOWSKI, to gain the advantage of providing support with other types of medical devices with programming to limit the amount of drugs that can be administered.

Claim 18 lacks an inventive step under PCT Article 33(3) as being obvious over MPH in view of ANONOS, and further in view of US 2018/0094953 A1 to COLSON, S et al. (hereinafter "COLSON").

As per claim 18, MPH in combination with ANONOS discloses the method of claim 2. MPH does not disclose wherein the public key is created by a manufacturer of the mobile medical device.
COLSON discloses wherein the public key is created by a manufacturer of the mobile medical device (customers can then use the manufacturer's public key to verify the authenticity packaged medical device; para [0127], [0180]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the public key is created by a manufacturer of the mobile medical device as disclosed by COLSON, to gain the advantage of verifying authenticity of medical devices.

Claims 21-26 lack an inventive step under PCT Article 33(3) as being obvious over MPH in view of ANONOS, and further in view of US 2011/0173452 A1 to NAN, X et al. (hereinafter "NAN").

As per claim 21, MPH in combination with ANONOS discloses the method of claim 2. MPH does not disclose wherein the digital signature is generated by a key signing chip onboard the mobile medical device. NAN discloses wherein the digital signature is generated by a key signing chip onboard the mobile medical device (the user inputs data to be signed (the digital signature is generated) by the CPK Built-in chip (key signing chip onboard the mobile medical device); para [0241]-[0243]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the digital signature is generated by a key signing chip onboard the mobile medical device as disclosed by NAN, to gain the advantage of using a built-in key signing chip for local key authentication.

As per claim 22, MPH in combination with ANONOS and NAN discloses the method of claim 21. MPH does not disclose wherein the key signing chip comprises a private key, the private key used to generate the digital signature. NAN discloses wherein the key signing chip comprises a private key, the private key used to generate the digital signature (the CPK system (key signing chip) uses a private key to generate the digital signature; para [0110], [0244], [0245]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the key signing chip comprises a private key, the private key used to generate the digital signature as disclosed by NAN, to gain the advantage of using a built-in key signing chip for local key authentication.

-***-Continued Within the Next Supplemental Box-***-

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US20/23818

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

-***-Continued from Previous Supplemental Box-***-

As per claim 23, MPH in combination with ANONOS discloses the method of claim 2. Modified MPH additionally discloses wherein the mobile device comprises a device identification code, the device identification code being a member of the list of public keys (the computer (mobile device) provides decryption initiated using an IKE cookie (device identification code) to establish Internet Key Exchange/IKE keys (a member of a list of public keys) as part of the IKE protocol between the first computer and intermediate computer; para [0130], [0131]). MPH does not disclose wherein the mobile device is a mobile medical device; the public keys paired to a private key used to generate the digital signature. ANONOS discloses wherein the mobile device is a mobile medical device (data subjects utilize mobile smart devices in the medical services context; para [097], [0221]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include wherein the mobile device is a mobile medical device as disclosed by ANONOS, to gain the advantage of enabling an authorized user to unlock the "true" meaning of such information, given a particular time and context (ANONOS; para [012]). NAN discloses the public keys paired to a private key used to generate the digital signature (the CPK system uses a private key among any number of public key/private key pairs to generate the digital signature; para [0054], [0110], [0244], [0245]). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to modify the teaching of MPH to include the public keys paired to a private key used to generate the digital signature as disclosed by NAN, to gain the advantage of using a built-in key signing chip for local key authentication.

As per claim 24, MPH in combination with ANONOS and NAN discloses the method of claim 23. Modified MPH additionally discloses verifying the digital signature (an authenticator using the signature payload (verifying); para [0200]-[0203]), comprising: passing a series of parameters through one or more predetermined digital signature verification functions (RSA-based authentication (predetermined digital signature verification function) uses a pre-shared key and hash (series of parameters); para [0200]-[0203]), the series of parameters comprising: a ciphertext and a parameter derived from the device identification code (the hash payload (a ciphertext) and pre-shared key (parameter derived) where the internet key exchange/IKE protocol uses the identification from a lookup table (device identification code); para [0200]-[0203], [0250]-[0259]).

As per claim 25, MPH in combination with ANONOS and NAN discloses the method of claim 24. Modified MPH additionally discloses wherein the parameter derived from the device identification code (as previously disclosed by MPH) is at least a portion of the device identification code (the pre-shared key (parameter derived) by the internet key exchange/IKE protocol uses the identification from a lookup table (portion of the device identification code); para [0200]-[0203], [0250]-[0259]).

As per claim 26, MPH in combination with ANONOS and NAN discloses the method of claim 24. Modified MPH additionally discloses wherein the device identification code corresponds to, comprises, or is used to derive a public key, the public key corresponding to a private key used to form the digital signature (the pre-shared key (to derive a public key) is derived using the internet key exchange/IKE protocol which uses the identification from a lookup table (the device identification code corresponds to); para [0200]-[0203], [0250]-[0259]).

Claims 1-27 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.