Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2953392 A1 2016/01/07

(21) 2 953 392

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) **Date de dépôt PCT/PCT Filing Date:** 2015/06/29
(87) **Date publication PCT/PCT Publication Date:** 2016/01/07
(85) **Entrée phase nationale/National Entry:** 2016/12/21
(86) **N° demande PCT/PCT Application No.:** US 2015/038314
(87) **N° publication PCT/PCT Publication No.:** 2016/003902
(30) **Priorité/Priority:** 2014/06/30 (US62/019,227)

(51) **Cl.Int./Int.Cl.** ***G06Q 50/22*** (2012.01),
G06Q 50/24 (2012.01)

(71) **Demandeur/Applicant:**
BAXTER CORPORATION ENGLEWOOD, US

(72) **Inventeurs/Inventors:**
VALENTINE, MATTHEW A., US;
PADMANI, BHAVESH, US;
BOSSIO, ROBERT, US;
YEVSEYEVA, KRISTINA, US;
MODEKURTI, SRINIVAS, US

(74) **Agent:** SIM & MCBURNEY

(54) **Titre : ECHANGE D'INFORMATIONS MEDICALES GEREES**
(54) **Title: MANAGED MEDICAL INFORMATION EXCHANGE**

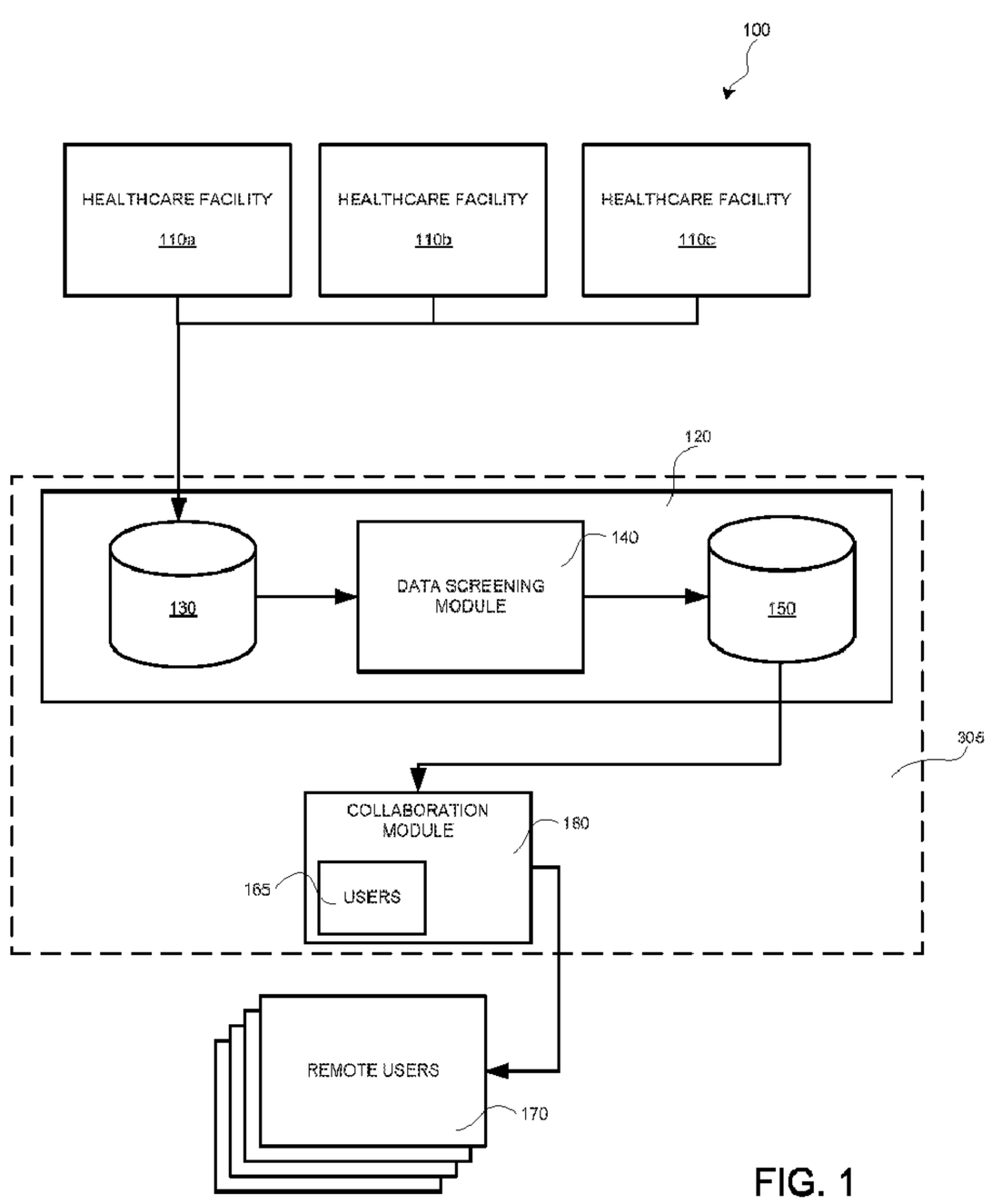


FIG. 1

(57) **Abrégé/Abstract:**
Management of medical information including collection of medical information from a data source, redaction of at least a portion of the medical records, and/or formatting the medical information for access by users. Accordingly, exchange of medical information

(21) **2 953 392**

(13) **A1**

(57) **Abrégé(suite)/Abstract(continued):**
may be facilitated, for example, to facilitate data analytics by internal users and/or one or more external entities. The medical information may have patient identifying information and/or protected health information (PHI) removed therefrom prior to being stored in a shareable data portion for access by users. Further still, the medical information in the shareable data portion may be formatted according to an identity of a user accessing the data, a context in which the data is to be used, and/or a requested format of the data. In turn, the exchange of medical information may facilitate data analytics that may serve a variety of beneficial purposes.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 January 2016 (07.01.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/003902 A1

(51) International Patent Classification:
G06Q 50/22 (2012.01) *G06Q 50/24* (2012.01)

(21) International Application Number:
PCT/US2015/038314

(22) International Filing Date:
29 June 2015 (29.06.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/019,227 30 June 2014 (30.06.2014) US

(71) Applicant: **BAXTER CORPORATION ENGLEWOOD** [US/US]; 9540 S. Maroon CIrcle, Englewood, CO 80112 (US).

(72) Inventors: **VALENTINE, Matthew, A.**; 15 Little Tomoka Way, Ormond Beach, FL 32174 (US). **PADMANI, Bhavesh**; 1877 Creekwater Boulevard, Port Orange, FL 32128 (US). **BOSSIO, Robert**; 102 Renshaw Drive, Palm Coast, FL 32164 (US). **YEVSEYEVA, Kristina**; 1616 Crescent Ridge Road, Daytona Beach, FL 32118 (US). **MODEKURTI, Srinivas**; 1162 Dayton Court, Buffalo Grove, IL 60089 (US).

(74) Agent: **DEPPE, Jon, P.**; Marsh Fishmann & Breyfolge, LLP, 8055 East Tufts Avenue, Suite 450, Denver, CO 80237 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,

[Continued on next page]

(54) Title: MANAGED MEDICAL INFORMATION EXCHANGE

(57) Abstract: Management of medical information including collection of medical information from a data source, redaction of at least a portion of the medical records, and/or formatting the medical information for access by users. Accordingly, exchange of medical information may be facilitated, for example, to facilitate data analytics by internal users and/or one or more external entities. The medical information may have patient identifying information and/or protected health information (PHI) removed therefrom prior to being stored in a shareable data portion for access by users. Further still, the medical information in the shareable data portion may be formatted according to an identity of a user accessing the data, a context in which the data is to be used, and/or a requested format of the data. In turn, the exchange of medical information may facilitate data analytics that may serve a variety of beneficial purposes.

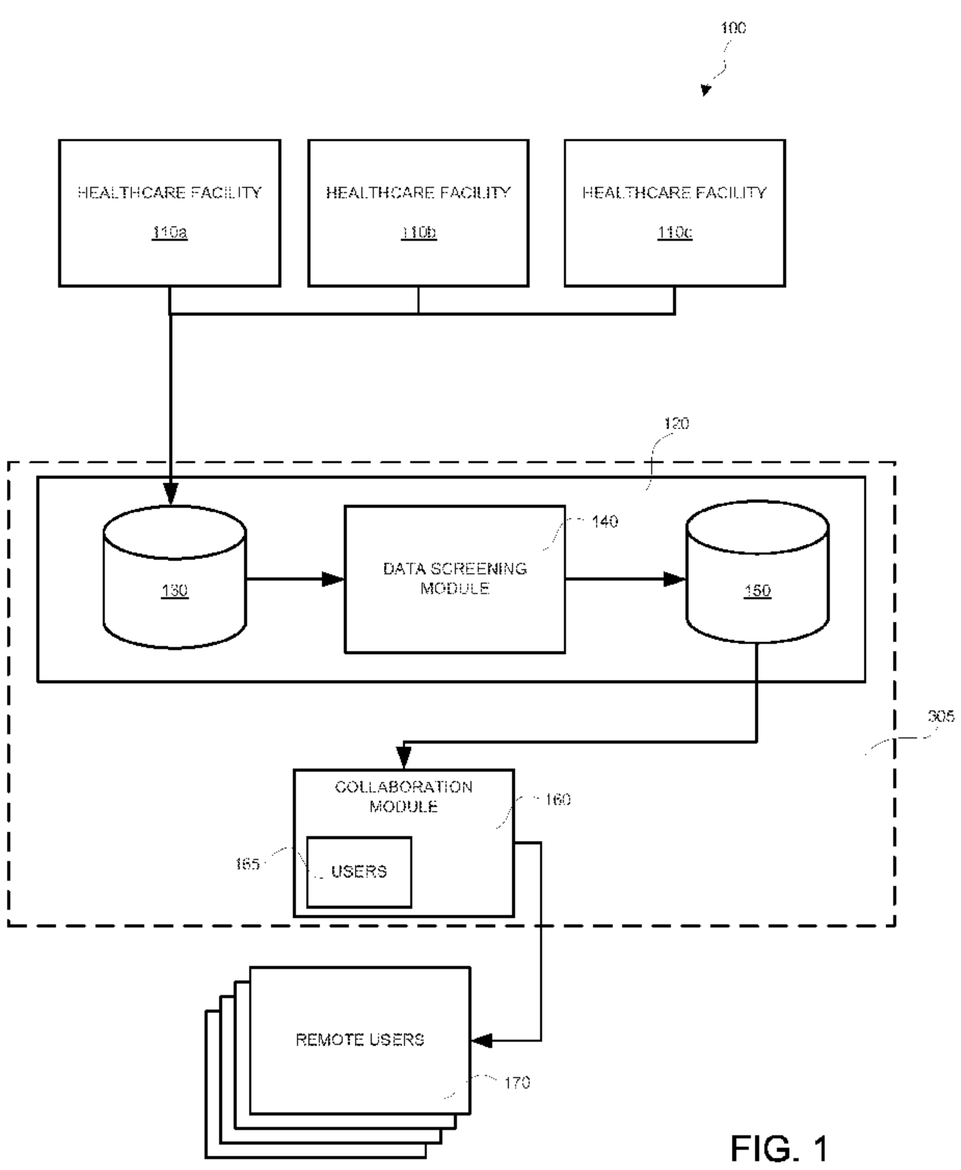


FIG. 1

WO 2016/003902 A1

WO 2016/003902 A1

DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

MANAGED MEDICAL INFORMATION EXCHANGE

CROSS-REFERENCE TO RELATED APPLICATION

This application claims priority from U.S. Provisional Application No.: 62/019,227 filed on June 30, 2014, entitled "MANAGED MEDICAL INFORMATION EXCHANGE," the contents of which are incorporated by reference herein as if set forth in full.

BACKGROUND

Many healthcare facilities utilize pharmacy resources to prepare medication preparations that are to be administered to a patient. Such pharmacy resources may be located locally at the healthcare facility or may be remote from the healthcare facility. In either regard, medication preparations at the pharmacy resource may be prepared in response to receipt of a medication dose order. Such medication dose orders may be, in at least some instances, patient-specific dose orders that are generated by a healthcare professional and correspond to a request for preparation of the medication preparation to be prepared for administration to the patient. In other applications, the dose orders may be stock orders or non-patient-specific.

Many healthcare facilities generate records corresponding to dose orders that are prepared by a pharmacy resource. The records may include information received with the medical dose order and/or information that may be added to the record by the pharmacy resource (e.g., including details about the products and/or preparation used to prepare the dose corresponding to the medical dose order). Such records may be stored and/or used locally at the pharmacy resource for a variety of potential purposes including for example, regulatory compliance, patient safety, inventory management, staffing decisions, or other purposes related to the management of the pharmacy resource and/or medication preparations.

Furthermore, continued developments in communication technology and collaborative tools increasingly make it easier to share and access data in a networked environment (e.g.,

through software services, data sharing platforms, or other network connectivity sometimes collectively referred to as "cloud services"). However, medical information (e.g., including dose order records or the like) may be subjected to access and/or dissemination restrictions. For example, access to such data may be limited to access by appropriate personnel at the healthcare facility or pharmacy resource. For instance, in the United States the Health Insurance Portability and Accountability Act (HIPAA) provides regulatory requirements regarding the handling, dissemination, or other privacy related aspects of medical records that may contain protected health information (PHI). In this regard, the use, dissemination, and/or access to dose order records, and especially patient-specific dose order records that may include PHI may be limited by regulatory compliance and/or other privacy concerns. As such, despite the benefits that may be provided with the ability to collaboratively share data for application of cloud services thereto, limits on the use of data may limit the access to such valuable data.

Furthermore, systems used to maintain and/or generate medical information may be proprietary, such that specific data formats are utilized. Thus data exchange may be limited by data formatting limitations. For instance, data generated or stored in a proprietary format specific to a first entity may not be readable by another entity.

SUMMARY

The present disclosure relates to systems and methods that facilitate collaborative approaches to the management of information, particularly, information related to medication preparation information received in relation to provision of medical care. In this regard, the present disclosure relates to managed exchange of medical information. The exchange of medical information may be improved by use of selective redaction and/or formatting of the medical information. For example, to allow for increased exchange of medical information that may include patient identifying information or protected health information (PHI), certain data of the medical information may be redacted. Furthermore, a cryptographic hash function may be

applied that reliably transforms a portion of information (e.g., information related to patient identifier) into a non-identifying value. In turn, records may still be associated with a given patient while the patient's PHI and/or patient identifying information may be removed.

Furthermore, given the potentially wide array of data analytics that may be applied to medical information exchanged using the description presented herein, the data may be formatted prior to access by users of a data exchange platform to facilitate specific data analytics. This may include a standardized format that is common to all users of the system and/or particularized formats corresponding to particular users, particular uses of the data, and/or particular types of data. In any regard, the use of an exchange platform as described herein may facilitate improved access to data to allow for more expanded, robust, and efficient data analytics in a number of contexts. In particular, inter-party exchange of data may be improved through data formatting rules associated with a collaboration system described herein. As such, data analytics may be expanded as data from a plurality of sources may be utilized and provided in a format. For example, data analytics related to multiple, inter-party data sources may be facilitated by the disclosure presented herein may help improve patient safety (e.g., by identifying potentially harmful trends with a collection of data), provide business intelligence, assist in reducing the cost of healthcare, or other meaningful benefits.

Accordingly, a first aspect includes a system for exchange of information related to patient-specific medication preparations. The system includes a data storage device in operative communication with one or more healthcare facilities to receive, from the one or more healthcare facilities, information regarding patient-specific medication preparations prepared at corresponding respective ones of the one or more healthcare facilities. In embodiments, the medical information may also include non-patient specific data received from one or more additional sources. The data storage device includes a sharable data portion that stores redacted data records having patient identifying (e.g., protected health information (PHI)) removed therefrom. The redacted records correspond to the information regarding medication

preparations that is received from the one or more healthcare facilities. The system also includes a collaboration module that is in operative communication with the data storage device. The collaboration module is operative to access the shareable data portion to extract data from the shareable data portion, transform the extracted data into a data format based at least in part on a predetermined operational need, and load the formatted data into a remotely accessible data storage location that is accessible remotely from the data storage device. In this regard, the predetermined operational need may be based on an identified data analysis to be performed, an identity of a party accessing the data, a requested format by a party accessing the data, or some other particular purpose for the data.

A number of feature refinements and additional features are applicable to the first aspect. These feature refinements and additional features may be used individually or in any combination. As such, each of the following features that will be discussed may be, but are not required to be, used with any other feature or combination of features of the first aspect.

For example, the PHI may include a patient identifier. Furthermore, the system of the first aspect may facilitate removal of patient identifying information, while still allowing an association between data records and a given patient. As such, one or more of the redacted data records stored in the shareable data portion may also comprise a unique identifier that associates one or more portions of the information regarding medication preparations to a given patient without providing identifying characteristics relative to the patient. The unique identifier may include a hash value generated in response to application of a hash function to the patient identifier.

The hash function may be executed by a processor at the data storage device to generate the redacted data records that are stored in the shareable data portion. Alternatively, a hash function may be executed locally at the one or more healthcare facilities to remove patient identifying information prior to providing the data to the data storage device. Accordingly, the system may receive medical information that has been redacted at a data source. As such, the hash function may be executed by a processor at the one or more healthcare facilities to generate

the redacted data records that are received at the central storage server for storage in the sharable data portion. In an embodiment, the hash value may include a deterministic, non-invertable value based on the patient identifier. That is, for each given unique patient identifier used to generate a has value, a corresponding unique hash value is generated. Furthermore, a user may not be able to ascertain the plain text patient identifier using only the hash function.

In an embodiment, the data storage device may also include a backup data portion that comprises complete data records (i.e., that potentially includes PHI) corresponding to at least a portion of the information regarding medication preparations received from the one or more healthcare facilities. The backup data portion and the shareable data portion may be separately accessible on the data storage device. That is, users who access the shareable data portion may not have access to the backup data portion. The collaboration module may provide a plurality of users selective and secure access to the shareable data portion based on a plurality of security layers applied to access the shareable data portion.

In an embodiment, the data format in which the collaboration module provides the redacted data may include a standardized data format accessible by the plurality of users. The data format may include a plurality of distinct data formats. As such, different ones of the plurality of distinct data formats may be accessible by corresponding different respective ones of the plurality of users.

In an embodiment, the data storage device may include a data storage server located remotely from the one or more healthcare facilities. Specifically, the data storage device may comprise a plurality of mirrored data servers distributed at distinct geographic locations. As such, redundancy may be provided such that the likelihood of data loss at both of the distributed data servers is reduced.

In an embodiment, the system of the first aspect may be used in connection with the ordering, preparation, and/or administration of a dose to a patient. As such, the information regarding medication preparations may include dose order records generated in response to

received dose orders for mediation preparations to be administered to a patient.

The system of the first aspect may also include an analytics module in operative communication with the data storage location to retrieve the formatted data. In turn, the analytics module may be operative to perform at least one analysis on the information regarding medication preparations in relation to a specific given patient without the particular identity of the specific given patient. The analysis performed by the data analytics module may at least include analysis with respect to the unique patient identifier. For instance, doses administered to a given patient may be analyzed.

Other analysis may be facilitated or conducted without limitation. Examples of such analysis may include error tracking in relation to one or more given dose order data fields. Accordingly, tracked errors may be examined to determine if a common data parameter exists to facilitate a root cause investigation. For example, high error rates with respect to doses prepared with a given drug or medical product may allow for underlying causes (e.g., a potential confusing label or the like) to be identified with respect to the given drug or medical product.

Further still, data analysis may be facilitated or performed to help parameterize and evaluate a supply chain related to the manufacture, ordering, preparation, distribution, and/or administration of a dose. In this regard, as data related to a given dose, including medical product information used in the preparation of the dose, may be provided to the system, inventory tracking and supply chain evaluation may be conducted at any one or more portions of the supply chain from, for example, a medical product manufacturer to, for example, dose administration. Such analysis may be at least partially based on one or more dose order data fields contained in the medical information received at the system.

In an embodiment, the information regarding medication preparations may be received at the data storage device in accord with a local data policy of each respective one of the one or more healthcare facilities. As such and as stated above, patient identifying information may be removed from the medical information prior to the receipt of the data at the system of the first

aspect. The removal of such patient identifiers may be at least in part based on the local data policy of each respective healthcare facility. The local data policy may be configurable for each respective one of the healthcare-facilities.

A second aspect includes a method for generation of shareable information regarding patient-specific medication preparations. The method includes receiving, from one or more healthcare facilities, information regarding patient-specific medication preparations prepared at corresponding respective ones of the one or more healthcare facilities for administration to a patient. The method further includes storing the information as a shareable data portion stored on a data storage device in the form of redacted data records that correspond to the information regarding patient-specific medication preparations that is received from the one or more healthcare facilities. The redacted records have patient identifying information (e.g., protected healthcare information (PHI)) removed therefrom. The method further includes formatting the redacted data records to a format corresponding with a predetermined operational need and loading the formatted data into a remotely accessible storage location for access by users remote from the storage location.

A number of feature refinements and additional features are applicable to the second aspect. These feature refinements and additional features may be used individually or in any combination. As such, each of the following features that will be discussed may be, but are not required to be, used with any other feature or combination of features of the second aspect. Furthermore, any one or more of the feature refinements and additional features described above in relation to the first aspect may be, but are not required to be, used with the second aspect.

For instance, in an embodiment, the PHI may include at least a patient identifier. The method may further include associating a unique identifier with one or more of the redacted data records that corresponds to a given patient and does not provide identifying capability relative to the patient. As such, the storing may further include applying a hash function to the patient identifier and generating the unique identifier in response to the applying. The unique identifier

may, in turn, comprise a hash value resulting from the applying.

In an embodiment, the method may further include providing a plurality of users selective and secure access to the redacted data records. For instance, to access the redacted data records, a user may be required to undergo a plurality of security layers that may require provision of authentication information.

In an embodiment, the formatting may include formatting the redacted data records to a standardized format accessible by the plurality of users. Additionally or alternatively, the formatting may include formatting the redacted data records to a plurality of distinct data formats. The different ones of the plurality of distinct data formats may be accessible by corresponding different respective ones of the plurality of users.

In an embodiment, the method may further include generating the information regarding medication preparations comprise dose order records in response to received dose orders for mediation preparations to be administered to a patient. The method may also include accessing the data storage location to retrieve the formatted data and analyzing the information regarding medication preparations in relation to a specific given patient without the particular identity of the specific given patient. The method may include performing any one or more of the types of analysis described above in relation to the first aspect.

Additionally, the method may further include that the receiving the information regarding medication preparations is at least partially based on a local data policy of each respective one of the one or more healthcare facilities. As such and as described above, a local data policy may be enforced at the healthcare facility.

While the foregoing has referenced receiving medical information from a healthcare facility, the foregoing system and method aspects may also be utilized to receive medical information from any one or more of a plurality of data sources. Such data sources may include pharmaceutical manufacturers that manufacture drug products or medical products (e.g., that may be used in the preparation of a dose). The data sources may also include hospital information

systems. Hospital information systems may provide data related to inventory tracking of medical products received and/or distributed throughout a facility. The hospital information systems may also provide medical information including medical records or the like. Additional data sources may include, for example, information from medical device operational databases (e.g., including administration devices such as infusion pumps) and/or dispensing cabinets. Furthermore, any one or more of the data sources may, but are not required to, access data for purposes of performing data analytics or the like. Accordingly, data analytics on aggregated data received from a number of sources may be facilitated. In this regard, data originating from a plurality of sources in connection with the manufacture, ordering, preparation, and/or administration of a dose may be aggregated to provide a wider array of analytical options in relation to the data. The improved access to such aggregated, redacted, and formatted data may facilitate improvements in a number of contexts including patient safety, pharmacy efficiency, business development, inventory management, and others.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic view of an embodiment of a system for exchange of information related to medication preparations.

Fig. 2 is a schematic view of an embodiment of a system for exchange of information related to medication preparations.

Fig. 3 is a schematic view of an embodiment of a collaboration platform with collaborative data analytics relative to shared information related to medication preparations.

Fig. 4 is a flow chart depicting an embodiment of a method for exchange of information related to medication preparations.

Fig. 5 is a schematic view of an embodiment of an implementation of a collaboration platform for exchange of medical information in a particular context including dose preparation and administration.

DETAILED DESCRIPTION

The following description is not intended to limit the invention to the forms disclosed herein.

Consequently, variations and modifications commensurate with the following teachings, skill and knowledge of the relevant art, are within the scope of the present invention. The embodiments described herein are further intended to explain modes known of practicing the invention and to enable others skilled in the art to utilize the invention in such, or other embodiments and with various modifications required by the particular applications(s) or use(s) of the present invention.

The present disclosure generally relates to the exchange of medical information, and especially to the management of the exchange of medical information that may include dose order records related to medication preparations prepared for administration to a patient for the purpose of providing data analytics relative to the medical information. The exchange of such medical information may facilitate a data collaboration platform that enables various entities to perform data analytics on the medical information that may originate from a plurality of data sources for a variety of purposed including, for example, to improve patient safety, to track medical trends, to obtain business intelligence, or for other purposes related to the medical information.

Different entities may have the incentive and/or know-how to provide different kinds of analytics. Accordingly, the present disclosure facilitates a collaboration platform that enables widespread sharing of data to a plurality of parties that may each provide data analytics. In turn, providing a data collaboration platform that provides collected and/or aggregated data in an appropriate format to a plurality of potentially unrelated parties may facilitate improved data analytics based on the variety of providers that may access and/or analyze the formatted data that is provided by the platform.

Accordingly, the platform may be facilitated by a collaboration system that includes at least one data storage device comprising a backup data portion and a shareable data portion. The

collaboration system may further include a collaboration module. In this regard, the collaboration system may receive medical information from plurality of data sources. Additionally, the collaboration system may provide access to a plurality of users that access the collaboration system and receive data (e.g., for the purpose of performing data analytics). A party comprising a data source may additionally comprise a party that accesses the collaboration system to access data for the purpose of data analytics. That is, a party (e.g., an individual user, a corporate user, a governmental user, or the like) providing data to the collaboration system may further retrieve data from the collaboration system that includes the data supplied by the party and/or data from other parties that has been aggregated.

A particular concern regarding exchange of medical information includes maintaining the privacy of patients as it relates to the exchange of medical information. For instance, medical information may include patient identifying information (e.g., potentially including protected health information (PHI)). In this regard, dissemination of medical information may subject to restrictions due to regulatory issues (e.g., the Health Insurance Portability and Accountability Act (HIPAA) in the United States may prohibit dissemination of medical information with PHI) or other privacy concerns. Accordingly, the embodiments described herein may be operative to redact medical information to remove patient identifying information (e.g., PHI) from the data.

While removal of PHI or other patient identifying information may be necessary prior to dissemination of medical information for compliance with regulations such as HIPAA or for other privacy factors, it may still be beneficial to associate related medical records to a given patient, even if the identity of a patient is not provided. For instance, if a patient named "Jane Doe" may have a number of medical information records associated with her. The present disclosure facilitates redaction of those medical information records by use of a unique identifier. For instance, Jane Doe's medical records may be associated with "Patient X," where Patient X is non-identifying of Jane Doe. As such, some data analytics may benefit from a non-identifying association between medical records and a given patient (e.g., analytics that relate to trends

relative to given patients or analytics that relate to correlations with specific patients). For purposes of these analytics, simply identifying related medical records for a given patient, even in the absence of identifying information regarding the patient may be beneficial. As such, the embodiments described herein may provide such a unique identifier that may associate medical information for a given patient, but not provide any patient identifying information. For instance, a patient identifier may be used as an input to a one-way cryptographic hash function that generates a hash value that may comprise the unique identifier. In this regard, each unique patient identifier may result in a corresponding unique hash value that does not identify the patient when input to the hash function. As such, the unique identifier (e.g., the hash value) may be used to associate medical information to a given patient without providing patient identification.

As such, a collaboration platform facilitated by the embodiments herein may generate and/or store redacted medical information. A collaboration platform may further provide access to formatted data generated from redacted data records to facilitate data analytics. In turn, the format provided may be a standardized format that is common to all users or may include specialized or particular formats (e.g., proprietary formats) that are based on a user, application, or other criteria. In any regard, the platform described herein including the system and methods described below facilitate improved data sharing to promote application of cloud services and other data analytics to medical information for a variety of purposes.

Fig. 1 depicts an embodiment of a system 100 that facilitates exchange of medical information. In an application, the medical information may include information regarding medication preparations prepared in response to a dose order. For example, a healthcare facility 110 may utilize a local or remote pharmacy resource that is capable of preparing a medication preparation (also referred to herein as a dose) for administration to a patient. In this regard, a plurality of healthcare facilities 110a, 110b, and 110c may be in operative communication with a data storage device 120. While three healthcare facilities 110a-110c are depicted in Fig. 1, fewer

or more healthcare facilities 110 may be in operative communication with the data storage device 120 without limitation.

The healthcare facilities 110a-110c depicted in Fig. 1 may correspond to any appropriate healthcare facility 110 that generates, stores, supplements, or accesses medical information. Accordingly, the healthcare facilities 110 may include but are not limited to hospitals, pharmacies, outpatient care providers, home care providers, or the like. In any regard, the information provided to the data storage device 120 may include any medical information. In an embodiment, the medical information may relate to medication preparations such as doses to be administered to a patient that are prepared in response to a dose order. In a particular embodiment, the medical information may include patient-specific records corresponding to medication preparations (i.e., doses) that the healthcare facility 110 prepared and/or requested to be prepared for administration to a patient. As such, the healthcare facilities 110 may have access to pharmacy resources that may be utilized to prepare medications for administration to a patient. Access to pharmacy resources may include use of a local pharmacy located at the healthcare facility or use of remote pharmacy that provides medical information (e.g., dose order records) and medication preparations to the healthcare facility 110. For example, at least a portion of the healthcare facilities 110 may include hospital facilities that may include local pharmacy resources that generate dose order records in response to receipt of dose orders that correspond to requested medication preparations.

In this regard, the healthcare facility 110 may utilize a pharmacy workflow manager to generate and/or supplement the medical information that is to be provided to the data storage device 120. This pharmacy workflow manager may include any or all details as described in U.S. Application No. 14/022,415, which is incorporated by reference in its entirety. An example of one such pharmacy workflow manager may include the DoseEdge™ pharmacy workflow manager offered by Baxter Healthcare Corporation of Deerfield, IL. In this regard, the healthcare facility 110 may employ a tool that may capture dose order information to generate and/or supplement

dose order records corresponding to a dose to be prepared for administration to the patient. This may include capturing dose order data received from an order entry system and/or supplementing the dose order record with dose order metadata regarding the dose to be prepared and/or the preparation of the dose. As described in greater detail below, the dose order records may comprise medical information that may be provided to the data storage device 120.

In turn, the data storage device 120 may be operative to store the information regarding the medication preparations such as, for example, dose order records received from the healthcare facility 110. In this regard, the healthcare facility 110 may provide a dose order record that corresponds to a dose order received from a healthcare provider. One example may be a dose order record generated in response to a provider generating a dose order that is received at a pharmacy for a medication dose to be administered to a patient. Upon receipt of the dose order, the healthcare facility 110 may generate a dose order record corresponding to the dose order.

The dose order record may contain one or more dose order record data fields. The dose order record data fields may be populated with dose order metadata related to the dose order. The dose order metadata may be obtained from a received dose order (e.g., by way of a dose order entry system or the like) or may be associated with the dose order after receipt of the dose order (e.g., by a pharmacy workflow manager or the like during the management, preparation, and/or distribution of the dose corresponding to the dose order). The dose order record data fields may include one or more fields that provide patient identifying information. For instance, the dose order record data fields may include data related to a patient name, geographic data, pertinent dates (e.g., date of birth, date of admission, date of administration, etc.), telephone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers including license plate numbers, device identifiers and serial numbers, uniform resource locators (URLs), Internet protocol addresses, biometric identifiers (i.e. retinal

scan, fingerprints), identifying images, or any unique identifying number, characteristic or code. The patient identifier may, in this regard, comprise PHI that is associated with a dose order record.

Other potential dose order record data fields may also be provided that relate to the generation, preparation, distribution, and/or administration of the dose. For instance, such dose order record data fields may include, for instance, a scheduled drug administration date/time, an actual drug administration date/time, a scheduled distribution date/time, an actual distribution date/time, an expiration date for the medication preparation, a dilution value, a count of the number of medical products in the dose, a date/time of entry of the dose order, a volume measure of the dose, a date/time of the first dose of a series of doses, an indicator as to whether the dose is a first dose in a series of doses, an indicator of whether the dose comprises hazardous materials, an indicator of whether the dose is a high risk dose, a dose identifier, an indication of whether the dose is a test dose, a label format for a label corresponding to the dose, a nursing unit corresponding to the dose, order instructions, whether the dose order is on hold, a date/time for when the dose order is to be on hold, an overfill amount for the dose, a basal energy expenditure value for a patient, a body surface area value for a patient, a patient height, a patient weight, a duration for how long a dose is pending, a date/time the dose was prepared, whether a label for the dose order has been printed, at what time the dose order label was printed, the name of the printer to which the dose order label was printed, a rate of administration of the dose, an indication of whether the dose was ever rejected by a pharmacist during preparation, a date/time the dose was rejected, the identity of the pharmacist that rejected the dose, an administration route for the dose, a history of scan events for the dose, a date/time of scan events for the dose, a date/time the dose was sorted, an indication of the dose status, an indication of whether the dose was a stock dose, whether the dose was for total parenteral nutrition (TPN), an indication of the type of TPN associated with the dose, a date/time the dose was verified by a pharmacist, an identify of who verified the dose, an indication of who performed a given step related to the dose, dose preparation documentation (e.g., including images of the dose preparation and/or product

preparation for components of the dose order), an error log for the dose or other appropriate information related to the dose. In an embodiment, the dose order record including any one or more of the fields described above may be provided to the data storage device 120.

The data storage device 120 may be located remotely from each healthcare facility 110 with which the data storage device 120 is in communication. In an embodiment, the information received at the data storage device 120 may be a complete data record received from a healthcare facility 110. A complete data record may refer to a data record that contains the same information when received at the data storage device 120 as was contained by the data record at the healthcare facility 110. That is, a complete data record may have no data redacted therefrom. The information received at the data storage device 120 may be dose order records with information related to one or more dose order record fields as described above. Accordingly, the data storage device 120 may thus store a backup copy of the records provided from each respective healthcare facility 110. That is, complete copies of dose order records from the healthcare facility 110 may be provided to and stored on the data storage device 120. Accordingly, the data storage device 120 may include a backup portion 130 that stores the complete data records (e.g., dose order records) received from each respective one of the healthcare facilities 110. As may be appreciated, data provided by the healthcare facilities 110 may be in a proprietary data format that may or may not be readable by third parties without use of corresponding proprietary software executed by the healthcare facility 110.

In an embodiment, the backup data portion 130 may be operative to provide a backup version of data to any one or more of the healthcare facilities 110. For instance, in the event of a data loss at any one or more of the healthcare facilities 110a-110c, the backup data portion 130 may be able to provide a backup copy of a database to the healthcare facility 110 for the purposes of restoring the database. That is, data provided from any respecting one of the healthcare facilities 110 may be provided back to the given healthcare facility 110 as a data backup. As such, provision of the medical information by the healthcare facilities 110 may provide the facilities

110 benefit in the form of a data backup. Thus, medical information that relates to patient health may be efficiently backed up at the backup data portion 130 and available for restoration at the healthcare facility 110 in the event of a data loss at the facility 110.

The data storage device 120 may also include a shareable data portion 150. The shareable data portion 150 may store data records that have at least a portion of the medical information redacted therefrom. For example, in an embodiment, records in the shareable data portion 150 may have personal health information (PHI) removed therefrom. In this regard, a data screening module 140 may be provided. The data screening module 140 may access the complete data records stored in the backup data portion 130. The data screening module 140 may remove one or more portions of data (e.g., PHI or other patient identifying information) from the records. In turn, the redacted data records may be stored in the shareable data portion 150.

As such, the backup data portion 130 and the shareable data portion 150 may be separated such that access to each respective data portion may be controlled. While the data portions may reside on the same device (e.g., a common drive, server, or the like), the data portions may be segregated such that access on one portion may not allow for access to the other. In an embodiment, the data portions may be stored on different corresponding devices.

It may be advantageous to provide associations between the data records correspond to a given patient even if the given patient is not identified (i.e., even if the records are redacted). Thus, the system 100 may be operative to associate redacted records and a patient to determine what medication preparations were associated with a given patient without providing information that identifies the actual patient. As the identity of the patient may comprise PHI, the identity of the patient may be redacted from the record while still providing an associative relationship between all records for a given patient. That is, the data screening module 140 may generate a unique identifier that corresponds to a given patient but is not capable of identifying the patient. As such, all data records associated with that patient may be assigned the unique identifier

corresponding to the patient. All data records for the given patient may therefore be identified while the identity of the patient themselves may not be provided.

One example of a unique identifier may comprise a hash value generated by application of a cryptographic hash function to one or more portions of the complete data record prior to storing the redacted record in the shareable portion 150. In turn, the redacted data records may be stored with a generated hash value, which may comprise a unique identifier. In an embodiment, the complete dose record may include one or more patient identifier. For instance, the dose records may include field containing the patient name and/or other identifying information related to the patient such as, for example, a facility identifier for the patient, a date of birth, a social security number, or other patient identifying information as described above. Accordingly, the patient identifier may include PHI. In turn, any one or more of the patient identifiers of the complete dose record may comprise an input to the hash function. The resulting hash value output may provide the unique identifier that may be stored in corresponding relation to the redacted data records stored in the shareable data portion 150.

The data screening module 140 may apply a hash function to one or more patient identifier fields of the complete dose order records. For instance, one or more cryptographic hash functions may be applied such as, for example, SHA-1, SHA-2, SHA-3, MD5, RIPEMD-128/256, RIPEMD-320, RTR0, or other appropriate hash functions now existing or later developed. Preferably, the applied hash function is deterministic. That is, for each given unique input a corresponding unique output is provided by the function without data collisions. Furthermore, the hash function is preferably non-invertable. For example, when provided with a hash value resulting from the hash function, the input that resulted in the hash value should not be ascertainable. Thus, the hash function preferably provides a one-way conversion of the patient identifier to a non-identifying unique value that is unique for each given one of a plurality of patients. In turn, the unique value for a given patient may be the same each time the hash function is applied. Thus, two or more different dose order records associated with a given patient may both receive the same unique

identifier upon application of the hash function to the records. As such, a review of the resulting redacted dose order records containing the unique identifier in place of a patient identifier may allow for dose order records corresponding to a given patient may be identified based on a common unique value (e.g., a hash value). The hash value may also be further encoded, e.g. using Base64 encoding on the resulting hash value.

The system 100 may also include a collaboration module 160. The collaboration module 160 may access the shareable data portion 150 containing the redacted data records. In turn, the collaboration module 160 may retrieve the redacted data records for transformation into a format that may be useable by one or more remote users 170 and/or local users 165 of the system 100. The format into which the collaboration module 160 transforms the redacted data may be at least partially based on a predetermined operational need of the local user 165 or remote user 170 that requests the data from the collaboration module 160.

The collaboration module 160 may facilitate selective, secure access to local users 165 and/or remote users 170 who wish to access the formatted data extracted by the collaboration module 160 from the shareable data portion 150. In this regard, a plurality of access layers may be provided that must be satisfied by users prior to accessing the formatted data from the shareable data portion 150. For instance, the remote user 170 may be required to access a first layer such as a virtualized private network (VPN) or the like. Accessing the VPN may require a remote user 170 to provide appropriate credentials (e.g., a valid user name and password combination, a cryptographic key, a one-time password, a biometric value, etc.). A local user 165 may be required to be utilizing an access terminal on a common network with the collaboration module 160 (e.g., a local area network or the like). A user may then access the collaboration module 160 with further credentials (e.g., a valid user name and password, a cryptographic key, a one-time password, a biometric value, etc.). Once the user has joined the VPN or accessed the collaboration module 160 on a common network and provided the necessary credentials to access the collaboration module 160, the user may have access to the formatted data at the

collaboration module 160 based on the redacted data records in the shareable data portion 150. As such, a plurality of access layers may be provided to reduce unauthorized access to the shareable data portion 150.

The collaboration module 160 may access the redacted data records in the shareable data portion 150 and extract the data therefrom. In turn, the collaboration module 160 may transform the data into a given format that is loaded (e.g., to a storage device at the collaboration module 160 and/or in the shareable data portion 150) for access by users 165/170. The format of the data may comprise a standardized format. The standardized format may in turn be accessible by all those who access the collaboration module 160. The standardized format may include an extensible markup language (XML) format. The standardized format may additionally or alternatively be provided as a delineated text file, a pivot table, or any other standardized format or data view. In this regard, data that may be provided in a proprietary format (e.g., as described above) may in turn be formatted such that the data may be accessed and/or viewed by other parties/users that are incapable of viewing the data in the proprietary format provided. As such, the data may be more widely disseminated to provide further data analytics relative thereto.

In an embodiment, the collaboration module 160 may format the redacted data from the shareable data portion 150 into a format at least in part based on the user who is to access the data, an application in which the data is to be used, a requested format of the user, and/or other appropriate criteria. For instance, different remote users 170 may have access to the collaboration module. As described above, access to the collaboration module 160 by a remote user 170 may include one or more layers of access protocols that require authentication including, for example, providing a user name and password. In this regard, access to the collaboration module 160 may at least in part identify the remote user 170 accessing the collaboration module 160. In this regard, the format of the data to which a remote user 170 has access may at least depend on the identity of the user 170. For instance, a first remote user 170 may be associated with a first party and receive the formatted data in a first format associated with the first party

(e.g., a proprietary data format corresponding to the first party). A second remote user may be associated with a second party and receive the formatted data in a second format associated with the second party (e.g. a proprietary format associated with the second party). The first and second formats may be different and may be unique to the particular user accessing the collaboration module 160. As will be described in greater detail below, different remote users 170 of the formatted data provided by the collaboration module 160 may have different operational needs as it relates to the data stored in the shareable data portion 150. As such, the format of the data presented to a user 165/170 may be based on an anticipated use of the data and/or a requested format by the user 165/170.

As may be appreciated in Fig. 1, the data storage module 120 and collaboration module 160 may collectively comprise a collaboration system 305. In this regard, the healthcare facilities 110a-110c may comprise data sources that provide data to the collaboration system 305. In turn, users 170 and/or 165 may access the data provided by the data sources 110a-110c by utilizing the collaboration system 305. In this regard, the embodiment depicted in Fig. 1 provides one exemplary embodiment of a collaboration system 305, however as will be appreciated in further reference to Fig. 2 below, other embodiments of collaboration systems 305 are contemplated.

Furthermore, the various components depicted in Fig. 1 may be in operative communication over one or more networks. That is, the various modules and devices depicted may each be in operative, networked communication. The network communications may utilize a wide area network such as the Internet or the like. Additionally or alternatively, the communications may be by way of one or more local area networks, intranets, private networks, or the like. Furthermore, the modules and devices may comprise integrated systems or may be provided discretely. For instance, in an embodiment, the data storage device 120 may include discrete hardware for each of the backup data portion 130 and the shareable data portion 150. For instance, each respective data portion may be provided on separate hardware such as separate hard drives, separate servers, or the like. Alternatively the portions may comprise

segregated data spaces on a common device such as a common hard drive, a common server, or the like. In this same regard, the data screening module 140 and/or collaboration module 160 may each be stand alone modules executing on discrete hardware devices or either module may be executed on a common hardware device that may or may not also contain the backup data portion 130 and/or the shareable data portion 150.

Fig. 2 depicts another embodiment of a system 200 for exchange of information. The variations and details described above in relation to Fig. 1 may be applicable to the system 200 of Fig. 2 unless specified otherwise. The system 200 generally includes healthcare facilities 210a and 210b that are in operative communication with a primary data storage device 222. The primary storage device 222 may be in operative communication with a secondary or backup data storage device 224. In turn, a datamart module 260 may be in operative communication with the backup data storage device 224. Remote users 270 may access the datamart module 260. In turn, medical information received from the healthcare facilities 210a and 210b may be selectively provided to the remote users 270 for advantageous data analytics relative thereto.

As shown in Fig. 2, each healthcare facility 210 may include a backup services module 212. The backup services module 212 may be in operative communication with one or more local database of the healthcare facility. For instance, the backup service module 212 at the healthcare facility 210a may be in operative communication with local databases 214 and 216. In this regard, local databases 214 and 216 may store information at the healthcare facility 210a. Backup service 212 at healthcare facility 210b may be in operative communication with a local database 218 at healthcare facility 210b. In an embodiment and as described above, the information may include dose order records corresponding to dose orders for medication preparations to be administered to a patient.

In any regard, the backup service module 212 may access a local database at the healthcare provider 210 and provide information to the primary data storage device 222. The backup service module 212 may periodically poll the one or more databases with which it is in

operative communication and provide any new or modified records to the primary data storage device 222. Alternatively, the backup service module 212 may continuously monitor one or more database and provide records to the primary data storage 232 in a real time or near real time basis.

The backup service module 212 may also apply a local backup policy established by each respective healthcare facility 210. For instance, a healthcare facility 210 may wish not to provide information containing certain data fields (e.g., those fields corresponding to patient identifiers and/or PHI) to the primary data storage device 232. In this case, the backup service 212 may facilitate redaction of one or more portions of the data from the data prior to providing the data to the primary data storage device 232. In an embodiment, the backup service module 212 may be operative to generate a unique identifier corresponding with a given patient as was discussed above in connection with the data screening module 140. That is, the backup service module 212 may locally generate a unique value that uniquely associates a given patient with one or more data records, yet is non-identifying of the patient. As such, the backup service 212 may be operative to apply a hash function to the data records to redact a patient identifier from the records. In turn, the information provided from the backup service 212 to the primary data storage device 222 may include a unique identifier in lieu of patient identifying information.

The primary data storage device 222 may include a backup data portion 232 at the primary data storage device 222. The primary data storage device 222 may also be in operative communication with a backup data storage device 224. The backup data storage device 224 may include a backup data portion 234. The backup data portion 232 of the primary data storage device 222 may be replicated and stored in the backup data portion 234 of the backup data storage device 224. The primary data storage device 222 and the backup data storage device 224 may be distributed at distinct geographic locations. For example, the primary data storage device 222 may be located at a first geographic location on the east coast of the United States and the backup data portion 224 may be located at a second geographic location on the west

coast of the United States. Periodically, the primary data storage device 222 may communicate data from the backup data portion 232 to the backup data portion 234 of the backup data storage device 224. As such, a backup of the backup data portion 234 may be stored at each location. Accordingly, the use of geographically distributed storage device locations may reduce the potential for data loss at both facilities simultaneously. Thus, in addition to the primary data storage device 222 facilitating data backup services for the healthcare facilities 210, a further backup potential is created by use of the backup data storage device 224. As such, in the event of a data loss at a healthcare facility 210 and/or the primary data storage device 222, the backup data storage device 224 may provide backup copies of data to the facility 210 and/or primary data storage device 222 to facilitate data recovery.

The backup data storage device 224 may include a data screening module 240. Although, the data screening module 240 could be located at the primary data storage device 224 in addition to or as an alternative to the backup data storage device 224 without limitation. In either regard, the operation of the data screening module 240 would be the same. As described in relation to Fig. 1, the data screening module 240 may generate a unique identifier associated with a patient identifier for the purpose of redacting a portion of the data records (e.g. including patient identifiers and/or PHI) to be stored in a shareable data portion 250 at the backup data storage device 224. In the embodiment depicted in Fig. 2, data records may be provided in a redacted form from the backup service module 212 at the healthcare facility. In this regard, the data screening module 240 may further redact the data records or pass the previously redacted records on to the shareable data portion 250. In any regard, the information stored in the shareable data portion 250 may be redacted (e.g., the data may have patient identifiers and/or PHI removed therefrom).

The shareable data portion 250 may be in operative communication with a collaboration module 262. The collaboration module 262 may be provided in a datamart module 260. The datamart module may allow for the collaboration module 262 to extract, transform (e.g., format), and load formatted data into a datamart storage device 264 for access by remote users 270.

Again, the formatted data may be provided in a standardized form or may be provided in particular given forms accessible by the remote users 270 as discussed above.

In this regard, Fig. 2 depicts another embodiment of a collaboration system 305 the comprises the primary data storage device 222, the backup data storage device 224 and the data more module 260. In this regard, collaboration system 305 may include geographically remote backup data storage devices for the purpose of providing additional data redundancy. In this regard, the healthcare facilities 210a and 210b may comprise data sources that provide medical information to the collaboration system 305. In turn, the collaboration system 305 may provide access to the redacted and formatted medical information to remote users 270.

Fig. 3 depicts a schematic view of an embodiment of a collaboration platform 300 that may be used to provide medical information from one or more data sources to users for the purpose of facilitating data analytics on the medical information. The collaboration platform 300 may include a collaboration system 305. The collaboration system 305 may comprise a system such as collaboration system 305 described above in relation to system 100 shown in Fig. 1 or collaboration system 305 shown in Fig. 2. In any regard, the collaboration system 305 may receive information from a healthcare facility 310. In turn, the information may be provided in a shareable data portion of the collaboration system 305 for access by users such that the information received from the healthcare facilities 310 is transformed prior to access by one or more third parties. For instance, the transformation may include redacting patient identifiers and/or PHI from the data and/or transforming the data into a format useful to users of the system 305.

However, the collaboration system 305 may also be in operative communication with one or more other sources of data in addition or as an alternative to the healthcare facilities 310. For instance, the collaboration system 300 may be in operative communication with a medical device operational database (e.g., a dose administration device database or other appropriate source of medical device information), a hospital information system 314, external pharmacy resources 316,

and/or any other appropriate source of medical information. In the event the medical information received from the data source (e.g., the healthcare facility 310, the medical device operational database, the hospital information system 314, the external pharmacy resources 316 and/or any other appropriate source of medical information) contains information to be redacted (e.g., patient identifiers and/or PHI), the collaboration system 305 may be operative to redact the medication information and, for instance, generate a unique identifier that is related to, but does not identify a patient as described above.

The collaboration system 305 may provide access to formatted data generated from one or more data sources. The data provided by the collaboration system 305 may include redacted data records with patient identifiers and/or PHI removed therefrom regardless of the source of the data. The data provided by the collaboration system 305 may also be formatted as described above in relation to the embodiments of collaboration modules discussed above. The collaboration system 305 may thus format data from a plurality of sources that may originate in different formats. As such, the collaboration system 305 may be operative to combine and/or aggregate data from the different sources for presentation to users in a standard or particular format.

The collaboration system 305 may, thus, aggregate and format a large amount of medical data from a plurality of sources. In turn, users may access the aggregated and formatted data of the collaboration system 305. Such users may be local users 320 that locally access the collaboration system 305 (e.g., are users on a common network with the collaboration system 305 such as users of a local area network, intranet, or the like). Thus, internal analytics within a given organization may be facilitated. Furthermore, external users 330 may access the collaboration system 305 (e.g., users that access the system 305 by way of a wide area network or the like). In turn, internal analytic users 320 and/or external service providers 330 may have access to the collaboration system 305. The format available to and/or accessible by different users may depend upon the user's identity, whether the user is an internal or external user, and/or

a given purpose for which the user is accessing the data.

The modules described herein may comprise software, hardware, or a combination of both. For instance, the modules of the system may include specifically configured hardware such as application specific integrated circuits (ASICs), programmable field gate arrays, or other appropriate processors. In an embodiment, the modules may include a microprocessor in operative communication with a memory. The memory may comprise a non-transitory computer readable medium that may include machine-readable instructions. As such, the processor may access the memory and be specifically configured by the machine-readable instructions stored therein to execute any of the functionality described herein. Additionally, the modules described above may be executed using a common processor in operative communication with a memory that provides the functionality of a plurality of modules. In this regard, the modules may be executed using a single common processor or different modules may be executed using different processors.

Turning to Fig. 4, an embodiment of a method 400 for exchange of medical information by way of a collaboration platform is depicted in the form of flow chart. The method may include collecting 402 information from one or more data sources. As described above, the data sources from which medical information is collected may include healthcare facilities, medical device operational databases, hospital information systems, external pharmacy resources, or any other appropriate sources of medical information. In turn, the method 400 may include storing 404 medical information in a backup data portion. As described above, the shareable data portion may comprise a portion of a data storage device.

In an embodiment, the method 400 may include creating 406 backup data records. The back of data records may comprise a copy of complete records stored in the backup data portion. The backup data records may be stored in a remote geographic location separate from the backup data portion stored in step 404. In turn, the backup data records may be used to restore lost or corrupted data at a healthcare facility and/or other data source.

The method 400 may also include accessing 408 the complete medical information (e.g., the complete data records). As described above, it may be beneficial to redact a portion of the complete data records to, for example, remove patient identifying information therefrom. In this regard, the method 400 may include redacting 410 one or more portions of information from the medical records accessed at step 408. As described above, the redacting 410 may include applying a hash function to generate hash value based at least in part on a portion of the data records including, for example, a patient identifier and/or PHI. The method 400, in turn, includes storing 412 the redacted medical information in a shareable data portion. The shareable data portion may be separate from the backup data portion such that selective access to either portion may be separately facilitated.

In an embodiment, the method 400 includes extracting 414 the redacted records from the shareable data portion. The method 400 may further include formatting 416 redact data records into a data format that may be useful to a user accessing the redacted records (e.g., for purposes of data analytics). In this regard, the format may be standardized format presented all users of the system or may be particularly directed to a particular user and/or data analytic context for which the data is to be used. The method 400 may further include loading 418 the formatted redacted records (e.g., by a collaboration module or the like) to facilitate access to the formatted redacted records. In turn, the method 400 may include permitting 420 selective, secure access to the formatted redacted data records by users of the platform. As described above, the users may each have access to a standardized format or may be presented with a specific format of data based on the identity user, and indicated application for which the data is to be used, or a requested format type by the user.

In turn, the medical information collected 402 from the various sources of medical information may be transformed and made available to users to perform, for example, data analytics on the medical information. Accordingly, the method 400 may include performing 422 data analytics with respect to the formatted redacted records there selectively accessed 420.

Examples data analytics may include, for example, monitoring trends with respect to ordered doses for the purpose of improving patient safety relative to the ordered doses and/or improving business opportunities by gaining actionable business intelligence data relative to the activities corresponding to the medical information gained from the one or more sources. Other data analytics may be contemplated such as those described in greater detail below. In this regard, the data analytics may be provided in the form of the plurality of services by users may access and/or perform data analytics on the redacted, formatted medical information in a cloud architecture (e.g., using networked resources) to facilitate improved efficiency, speed, and/or utilization of resources relative thereto.

Fig. 5 depicts an embodiment of a platform 500 utilizes a collaboration system 305 aggregate data in turn provide redacted formatted data to one or more users who in turn access the data. As such, the collaboration system 305 may comprise a collaboration system according to the embodiment of a collaboration system 305 depicted in Fig. 1 and/or embodiment of a collaboration system 305 depicted in Fig. 2. Furthermore, any other appropriate combination of modules, components, or other devices comprising a collaboration system 305 and provided that facilitates redaction and formatting of medical information provided from one or more sources. In this regard, collaboration system 305 may include additional or fewer modules than those described with respect to the specific embodiments described in Figs. 1 and 2. As such, the embodiments depicted in Fig. 1 and Fig. 2 are exemplary, but not limiting.

In Fig. 5, the collaboration system 305 is discussed in relation to the context of preparation of a dose for a patient. In this regard, the solid arrow lines in Fig. 5 may represent flow of physical goods between the various entities described. The dash-dot lines in Fig. 5 represent flow data between the various entities in the collaboration system 305. Accordingly, the platform 500 shown in Fig. 5 represents one particular application of a collaboration system 305 is a relates to the flow of materials in connection with preparation and administration of the dose to the patient and healthcare facility.

The platform 500 may include a pharmaceutical manufacturer 510. The pharmaceutical manufacturer 510 may manufacture a medical product of a dose such as a drug compound and/or other intermediaries including diluents or the like. Accordingly, the pharmaceutical manufacturer 510 may provide the manufactured medical product to a hospital that employs a hospital information system 512. Specifically, an inventory management system at a healthcare facility may be executed by the hospital information system 512 may allow for receipt and tracking of goods from the pharmaceutical manufacturer 510.

The pharmaceutical manufacturer 510 may also provide data to the collaboration system 305. In this regard, the pharmaceutical manufacturer 510 may comprise a data source that provides medical information collaboration system 305. Examples of pertinent data that the pharmaceutical manufacturer 510 may provided the collaboration system 305 may include for example, medical product identifiers, lot numbers, expiration dates, inventory management numbers, product concentrations, product sizes, or other information related to medical products manufactured by the pharmaceutical manufacturer 510.

The inventory management component of the hospital information system 512 may, after receipt of medical products from the pharmaceutical manufacturer 510, monitor the medical products including, for example at time in which a medical product is requested at a pharmacy and/or track information associated with medical products including, for example lot numbers, expiration dates, product identifiers, or the like. As such, a pharmacy workflow manager 514 may be provided in the pharmacy of a healthcare facility. The pharmacy workflow manager 514 may receive products from the inventory management system of the hospital information system 512. For instance, the pharmacy workflow manager 514 may request medical products for use in preparation of doses from the inventory management system 512. As such, inventory management system 512 may facilitate provision of medical products to the pharmacy for tracking by the pharmacy workflow manager 514.

The inventory management portion of the hospital information system 512 may also

provide data to the collaboration system 305. Exemplary data may include, for example, average inventory levels, current inventory levels, inventory supply parameters including average durations a medical product is maintained in stock prior utilization, and/or data concerning the movement of medical products within a hospital including, for example, provision of drug products to the pharmacy workflow manager 514 for use in preparation of a dose.

The pharmacy workflow manager 514 may facilitate preparation of doses for administration to patients. As described above, the preparation of doses may be in response to received dose orders from healthcare providers or the like. As such, the pharmacy workflow manager 514 may receive dose order information as described above. Furthermore, the pharmacy workflow manager 514 may supplement such data with information related to the preparation of the dose. For example, images may be captured related to the medical product(s) utilized to prepare the dose. Furthermore, data may be gathered from medical products and used to populate specific dose order records corresponding to a dose order. The dose order may or may not be patient specific. In this regard, the dose order record may include information regarding a lot number or an expiration date of a medical product used to prepare the dose. Additionally, the pharmacy workflow manager 514 may supplement data such as the identity of the pharmacy technician who prepared the dose, the pharmacist who approved the dose, as well as parameters related thereto such as the time/date when such events occurred. Furthermore, the pharmacy workflow manager 514 may present to a pharmacy technician a protocol for use in preparation of the dose. The specific protocol utilized may also be associated with the dose order record.

The pharmacy workflow manager 514 may also provide data to the collaboration system 305. In this regard, the one or more portions of the data described above that is the generated and/or received by the pharmacy workflow manager 514 may be provided. In this regard, the pharmacy workflow manager 514 may provide information related to the preparation of a dose and/or related to the medical product(s) used to prepare the dose. Furthermore, the data provided

by the pharmacy workflow manager 514 to the collaboration system 305 may include information related to the time/date at which certain events relative to the dose order occur. The pharmacy workflow manager 514 may also detect errors that occur during the preparation of the dose order. For example, a pharmacy technician may scan an incorrect medical product to be used in connection with the dose to be prepared. While the pharmacy workflow manager 514 may alert the pharmacy technician of the error such that it may rectified, the pharmacy workflow manager 514 may further record the performance of the error in connection with the dose order with which it occurred.

The pharmacy workflow manager 514, upon dispensation of a dose from the pharmacy, may provide the dose to a dose dispensing cabinet 516. The dose dispensing cabinet 516 may be accessible by patients, healthcare facility personnel, or others to retrieve a dose once prepared. This regard, the dose dispensing cabinet 516 may track and/or collect certain information related to the dose. Examples of such data may include the time a dose is placed or retrieved in the dispensing cabinet 516 prior to retrieval, the identity of a person stocking and/or retrieving a dose from the dose dispensing cabinet 516, number of available doses in the dispensing cabinet 516, the number of free storage areas in the dose dispensing cabinet 516, or other relevant data. The dose dispensing 516 may also track errors related to the retrieval of dose orders from the dose dispensing 516. For example, unauthorized attempts to access storage location may be recorded. Furthermore, erroneous attempts to access storage location or attempt to access the incorrect story location may also be tracked. As such, any or all the data collected or available to the dose dispensing cabinet 516 may also be provided to the collaboration system 305.

Once the dose is retrieved from the dose dispensing cabinet 516, the dose may be administered to a patient using an administration device 518. That is, healthcare facility personnel such as a nurse or the like may retrieve a dose from the dose dispensing cabinet 516. The dose may in turn be connected to an administration device 518. The administration device 518 may,

for example, be an infusion pump utilized to deliver the dose to a patient. In this regard, the administration device 518 may record information regarding the dose administered such as, the patient to which the doses administered, or other relevant information such as the time of administration, parameters regarding the administration (e.g., administration rate, administration duration, etc.), or other information collected regarding the administration of the dose. The administration device 518 may further provide any such information it has access to or generates to the collaboration system 305.

Once doses are delivered to a patient, a patient record portion of a hospital information system 520 may be updated to record the administration of the dose to the patient. For example, parameters such as the hospital personnel responsible for the administration of the dose, the time/date of the dose, or other relevant medical record information including health care provider notes or the like be recorded in the patient records of the hospital information system 520. Furthermore, this information may also be provided to the collaboration system 305. The administration device 518 may further track errors. For example, the administration device 518 may include checks to ensure proper programming of the administration device 518. In the event that an improper programming is made, the error may be recorded by administration device 518.

Accordingly, the collaboration system 305 may collect information from the various stages related to the manufacture, preparation, and/or administration of the dose to the patient. As described above, the collaboration system 305 may aggregate, redact, and format such data. In turn, the collaboration module of the collaboration system 305 may allow access to the aggregated, redacted, and formatted data for purposes of data analytics. As briefly stated above, it may be valuable for the sources of data (e.g. any one or more of the entities described in Fig. 5) to not only provide data to collaboration system 305, but also retrieve data from the collaboration system 305 for a number of different reasons. As may be appreciated in Fig. 5, the entities shown may not only provided to collaboration system 305 may also each comprise users that in turn have access to the collaboration system 305 to access the aggregated, redacted, and

formatted data. In this regard, by virtue the collaboration system 305 providing redaction and formatting, any one or more of the entities shown in Fig. 5 may have access to a shareable data portion of the collaboration system 305 to gain access to data for use in data analytics.

This may open the available data to each one of the specific entities beyond that for which they are solely responsible. That is, the pharmaceutical manufacturer 510 may access the collaboration system 305 to obtain data related to the hospital information system 512 and/or 520, a pharmacy workflow manager 514, a dose dispensing cabinet 516, or an administration device 518. Absent the collaboration system 305, the collection in or use of such data may be arduous at each individual one of the entity shown in Fig. 5 may be required to solicit information directly from other entities and be subjected to concern such as data privacy and security. However, the collaboration system 305 may provide a central aggregation, redaction, and formatting of a pool of shared data that in turn provides efficient access to data for purposes the data analytics beyond that available for each individual entities on portion of the data supplied to collaboration system 305.

Some relevant examples of data analytics that made performed utilizing the platform 500 shown in Fig. 5 may include analysis that provides for improved patient safety, medical results, inventory management, business insight, security, or other useful outcomes related to the data analysis. For example and as described above, errors may be tracked at one or more the pharmacy workflow manager 514, dose dispensing cabinet 516, or administration device 518. In an effort to improve patient safety, a pharmaceutical manufacturer 510 may review data provided by the collaboration system 305. As the data aggregated by the collaboration system 305 may provide insights to the occurrence of errors with respect to a number of parameters including a particular medical product utilized to prepare the dose, the pharmaceutical manufacturer 510 may determine if error rates at any one or more of the pharmacy workflow manager 514, dose dispensing 516, or administration device 518 are more prevalent with a particular medical product. Identification of such trends may in turn allow the pharmaceutical manufacturer 510 to determine

a root cause of a source of the error and remedy the root cause. For example, in the pharmacy workflow manager 514, confusing labeling of packaging may result in an increased error rate with respect to a particular medical product. In turn, the pharmaceutical manufacturer 510 may identify the increased error rate with respect to the medical product and in turn launch a root cause analysis. In turn, a source of the error in the form of the confusing labeling may allow the pharmaceutical manufacturer 510 to improve the labeling and reduce the errors associated with the medical product.

Similarly, one or more of the entities in Fig. 5 may be interested in analytics with respect to inventory for purposes of improving supply-chain characteristics at any one or more portions of the supply chain between the pharmaceutical manufacturer and the administration of the dose to the patient. For example, the data provided by the collaboration system 305 allow for analytics with respect to turnaround times, throughput of doses, cycle times, or the like. Furthermore, information provided the various sources of data may allow for analysis with respect to the best source doses. For example, a pharmacy workflow manager 514 may determine, based on data analyzed from the collaboration system 305, whether it is more efficient to produce a dose within the pharmacy or, for example, buy premade doses from an outside vendor. Furthermore, an entity responsible for a dose dispensing cabinet 516 may utilize data retrieved the collaboration system 305 determine whether diversion a product from the dose dispensing cabinet is occurring.

In this regard, number of valuable parameters contained within the data provided by the collaboration system 305 may be leveraged to provide useful insights during data analytics. Specifically, given the foregoing discussion regarding the de-identifying of medical information while preserving the ability to associate various portions of the medical information with a given patient, patient specific analysis may be undertaken. This may be useful for providing insight regarding administration of doses to particular patient. For example, the delay between dose order entry and dose administration may be examined with respect particular patients. In turn, correlations with respect to types of medication, administration routes of medication, the nursing

unit associated with the doses, or even facilities in general, can be made. That is, metrics with regard to these various parameters may be examined in connection with delays between dose order and administration to provide increases in efficiency for the process of preparing and administering the doses to a patient. Such may be particularly valuable in urgent or "STAT" doses with the understanding that the time sensitivities associated with such doses may be critical to patient outcomes in certain instances such as an emergency context.

While the invention has been illustrated and described in detail in the drawings and foregoing description, such illustration and description is to be considered as exemplary and not restrictive in character. For example, certain embodiments described hereinabove may be combinable with other described embodiments and/or arranged in other ways (e.g., process elements may be performed in other sequences). Accordingly, it should be understood that only the preferred embodiment and variants thereof have been shown and described and that all changes and modifications that come within the spirit of the invention are desired to be protected.

What is claimed is:

1. A system for exchange of information related to patient-specific medication preparations, the system comprising:

a data storage device in operative communication with one or more healthcare facilities to receive, from the one or more healthcare facilities, information regarding patient-specific medication preparations prepared at corresponding respective ones of the one or more healthcare facilities, wherein the data storage device comprises a sharable data portion that stores redacted data records having patient identifying information removed therefrom and that corresponds to the information regarding medication preparations that is received from the one or more healthcare facilities; and

a collaboration module that is in operative communication with the data storage device, wherein the collaboration module is operative to access the shareable data portion to extract data from the shareable data portion, transform the extracted data into a data format based at least in part on a predetermined operational need, and load the formatted data into a remotely accessible data storage location that is accessible remotely from the data storage device.

2. The system of claim 1, wherein the patient identifying information comprises protected health information (PHI) that at least comprises a patient identifier.

3. The system of claim 2, wherein one or more of the redacted data records stored in the shareable data portion comprise a unique identifier that associates one or more portions of the information regarding medication preparations to a given patient without providing identifying characteristics relative to the patient.

4. The system of claim 3, wherein the unique identifier comprises a hash value generated in response to application of a hash function to the patient identifier.

5. The system of claim 4, wherein the hash function is executed by a processor at the data storage device to generate the redacted data records that are stored in the shareable data portion.

6. The system of claim 4, wherein the hash function is executed by a processor at the one or more healthcare facilities to generate the redacted data records that are received at the data storage device for storage in the sharable data portion.

7. The system of claim 4, wherein the hash value comprises a deterministic, non-invertable value based on the patient identifier.

8. The system of claim 1, wherein the data storage device further comprises:

a backup data portion that comprises complete data records including the patient identifying information corresponding to at least a portion of the information regarding medication preparations received from the one or more healthcare facilities.

9. The system of claim 7, wherein the backup data portion and the shareable data portion are separately accessible on the data storage device.

10. The system of claim 1, wherein the collaboration module provides a plurality of users selective and secure access to the shareable data portion based on a plurality of security layers applied to access the shareable data portion.

11. The system of claim 10, wherein the data format comprises a standardized data format accessible by the plurality of users.

12. The system of claim 10, wherein the data format comprises a plurality of distinct data formats, wherein different ones of the plurality of distinct data formats are accessible by corresponding different respective ones of the plurality of users.

13. The system of claim 1, wherein the data storage device comprises a data storage server located remotely from the one or more healthcare facilities.

14. The system of claim 13, wherein the data storage devices comprise a plurality of mirrored data servers distributed at distinct geographic locations.

15. The system of claim 1, wherein the information regarding medication preparations comprise dose order records generated in response to received dose orders for mediation preparations to be administered to a patient.

16. The system of claim 1, further comprising:

an analytics module in operative communication with the data storage location to retrieve the formatted data;

wherein the analytics module is operative to perform at least one analysis on the information regarding medication preparations in relation to a specific given patient without the particular identity of the specific given patient.

17. The system of claim 16, wherein the at least one analysis comprises at least one of error analysis, inventory management, or supply chain management.

18. The system of claim 1, wherein the information regarding medication preparations are received at the data storage device in accord with a local data policy of each respective one of

the one or more healthcare facilities.

19. A method for generation of shareable information regarding patient-specific medication preparations, the method comprising:

receiving, from one or more healthcare facilities, information regarding patient-specific medication preparations prepared at corresponding respective ones of the one or more healthcare facilities for administration to a patient;

storing the information as a shareable data portion stored on a data storage device in the form of redacted data records that correspond to the information regarding patient-specific medication preparations that is received from the one or more healthcare facilities, wherein the redacted records have patient identifying information removed therefrom;

formatting the redacted data records to a format corresponding with a predetermined operational need; and

loading the formatted data into a remotely accessible storage location for access by users remote from the storage location.

20. The method of claim 19, wherein the patient identifying information comprises protected health information (PHI) that comprises at least a patient identifier.

21. The method of claim 20, further comprising:

associating a unique identifier with one or more of the redacted data records that corresponds to a given patient and does not provide identifying capability relative to the patient.

22. The method of claim 21, wherein the storing further comprises:

applying a hash function to the patient identifier; and

generating the unique identifier in response to the applying, wherein the unique identifier

comprises a hash value resulting from the applying.

23. The method of claim 19, further comprising:

providing a plurality of users selective and secure access to the redacted data records.

24. The method of claim 19, wherein the formatting comprises formatting the redacted data records to a standardized format accessible by the plurality of users.

25. The method of claim 19, wherein the formatting comprises formatting the redacted data records to a plurality of distinct data formats, wherein different ones of the plurality of distinct data formats are accessible by corresponding different respective ones of the plurality of users.

26. The method of claim 19, further comprising:

generating the information regarding medication preparations comprise dose order records in response to received dose orders for mediation preparations to be administered to a patient.

27. The method of claim 19, further comprising:

accessing the data storage location to retrieve the formatted data;

analyzing the information regarding medication preparations in relation to a specific given patient without the particular identity of the specific given patient.

28. The method of claim 27, wherein the analyzing comprises at least one of error analysis, inventory management, or supply chain management.

29. The method of claim 19, wherein the receiving the information regarding medication

preparations is at least partially based on a local data policy of each respective one of the one or more healthcare facilities.

5

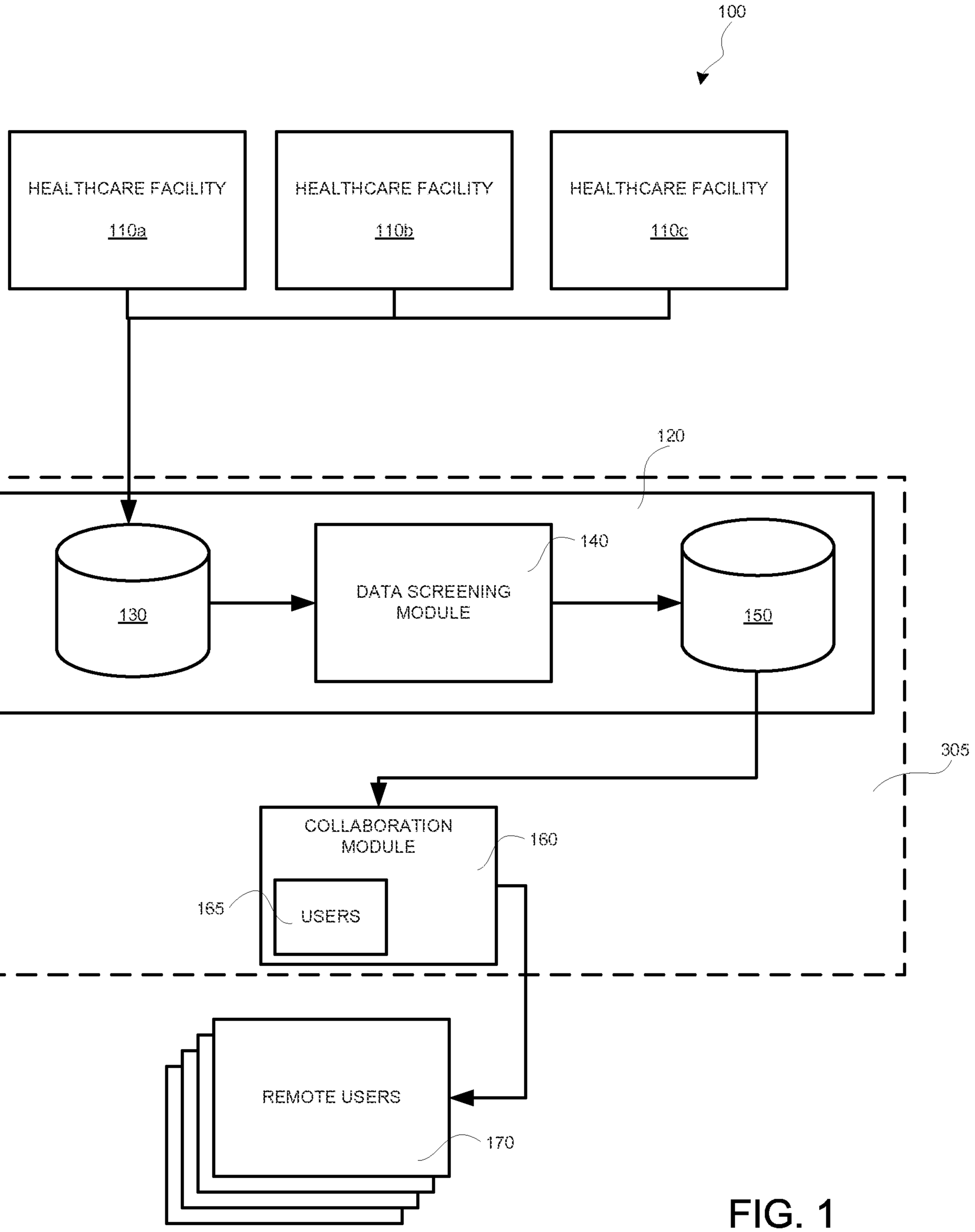

100
HEALTHCARE FACILITY
110a
HEALTHCARE FACILITY
110b
HEALTHCARE FACILITY
110c
120
130
140
DATA SCREENING MODULE
150
305
COLLABORATION MODULE
160
165
USERS
REMOTE USERS
170

FIG. 1

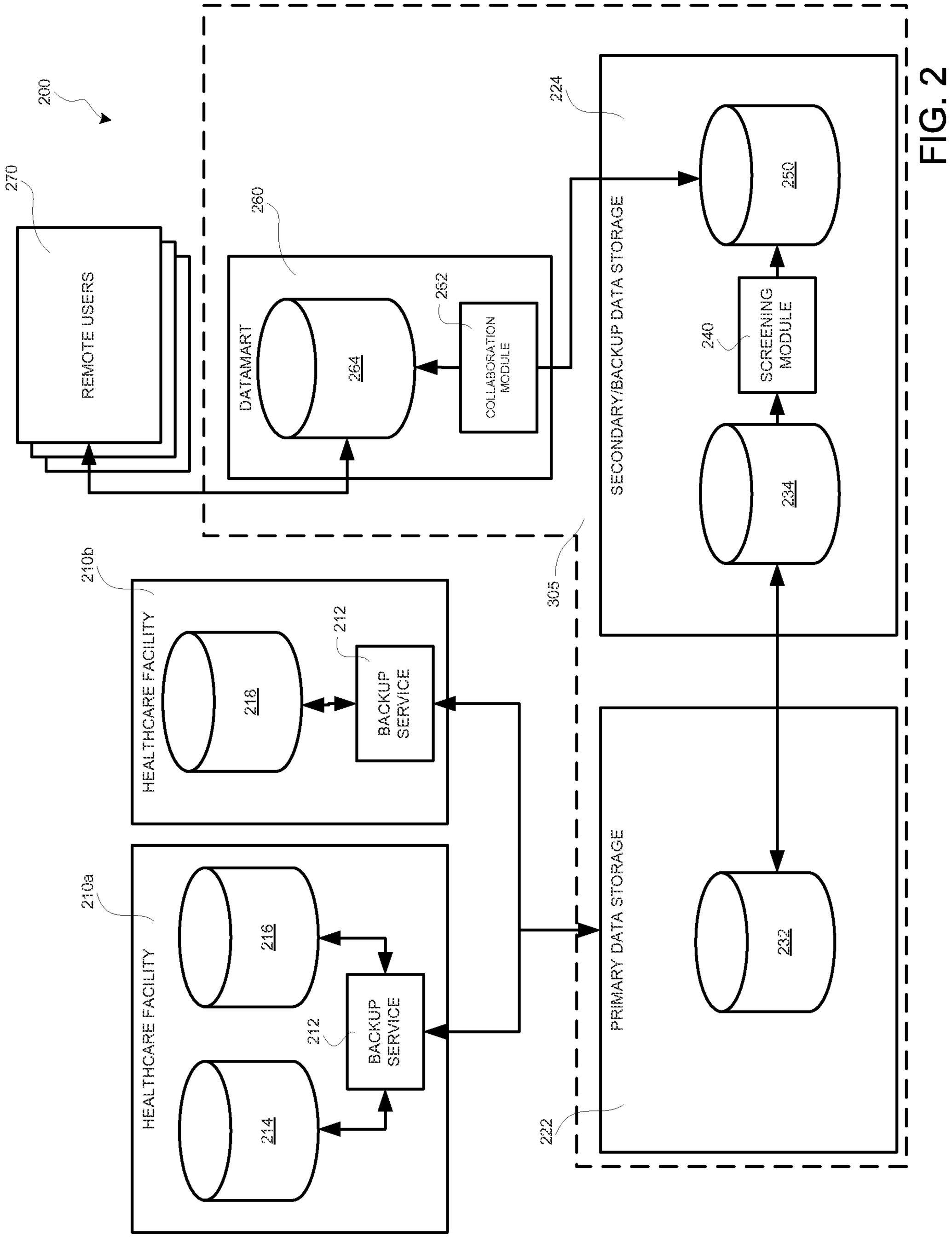

200
270
REMOTE USERS
260
DATAMART
264
262
COLLABORATION MODULE
224
SECONDARY/BACKUP DATA STORAGE
250
240
SCREENING MODULE
234
305
210b
HEALTHCARE FACILITY
218
212
BACKUP SERVICE
210a
HEALTHCARE FACILITY
216
212
BACKUP SERVICE
214
PRIMARY DATA STORAGE
232
222

FIG. 2

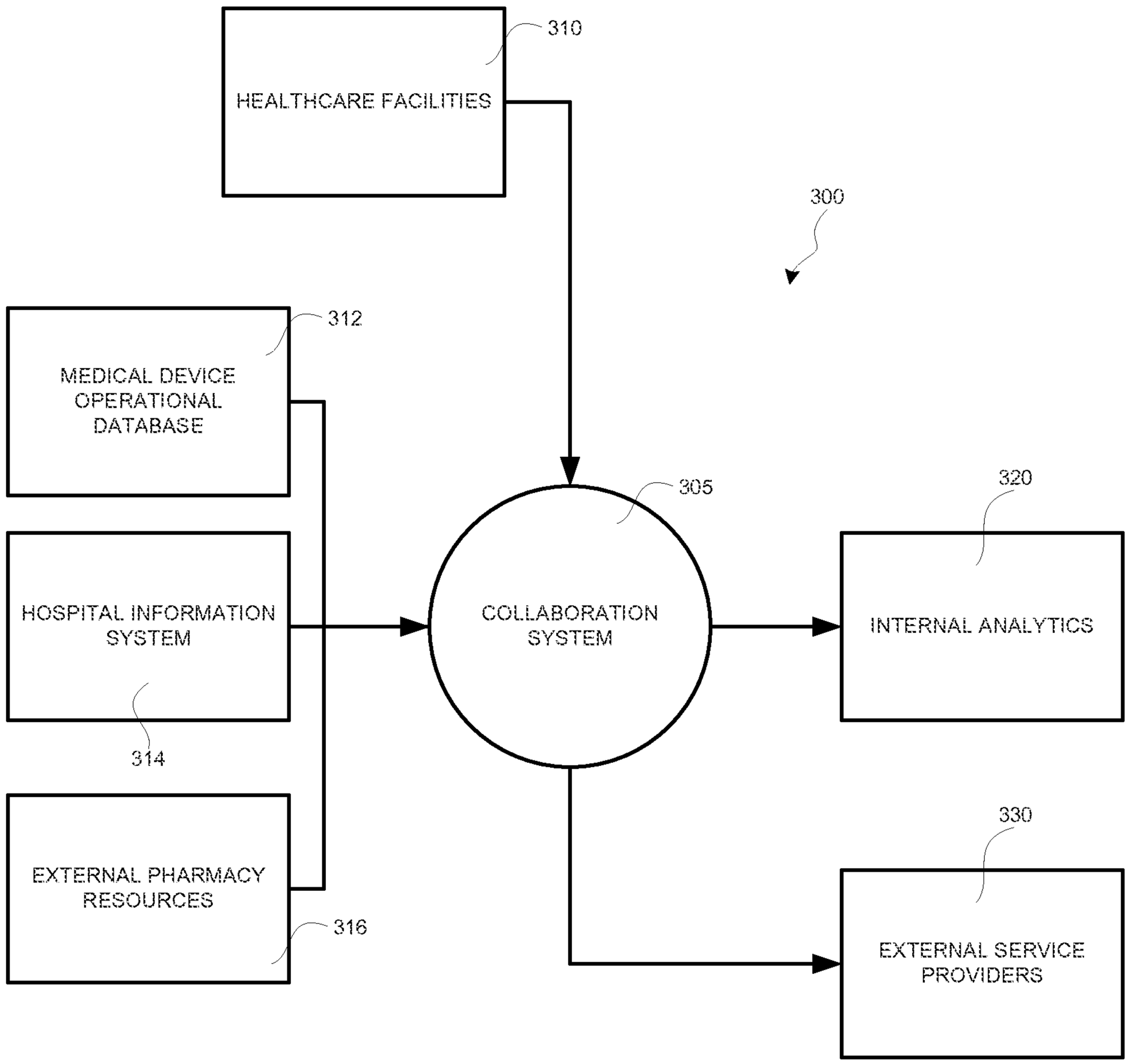

HEALTHCARE FACILITIES
310
300
MEDICAL DEVICE OPERATIONAL DATABASE
312
HOSPITAL INFORMATION SYSTEM
314
EXTERNAL PHARMACY RESOURCES
316
305
COLLABORATION SYSTEM
320
INTERNAL ANALYTICS
330
EXTERNAL SERVICE PROVIDERS

FIG. 3

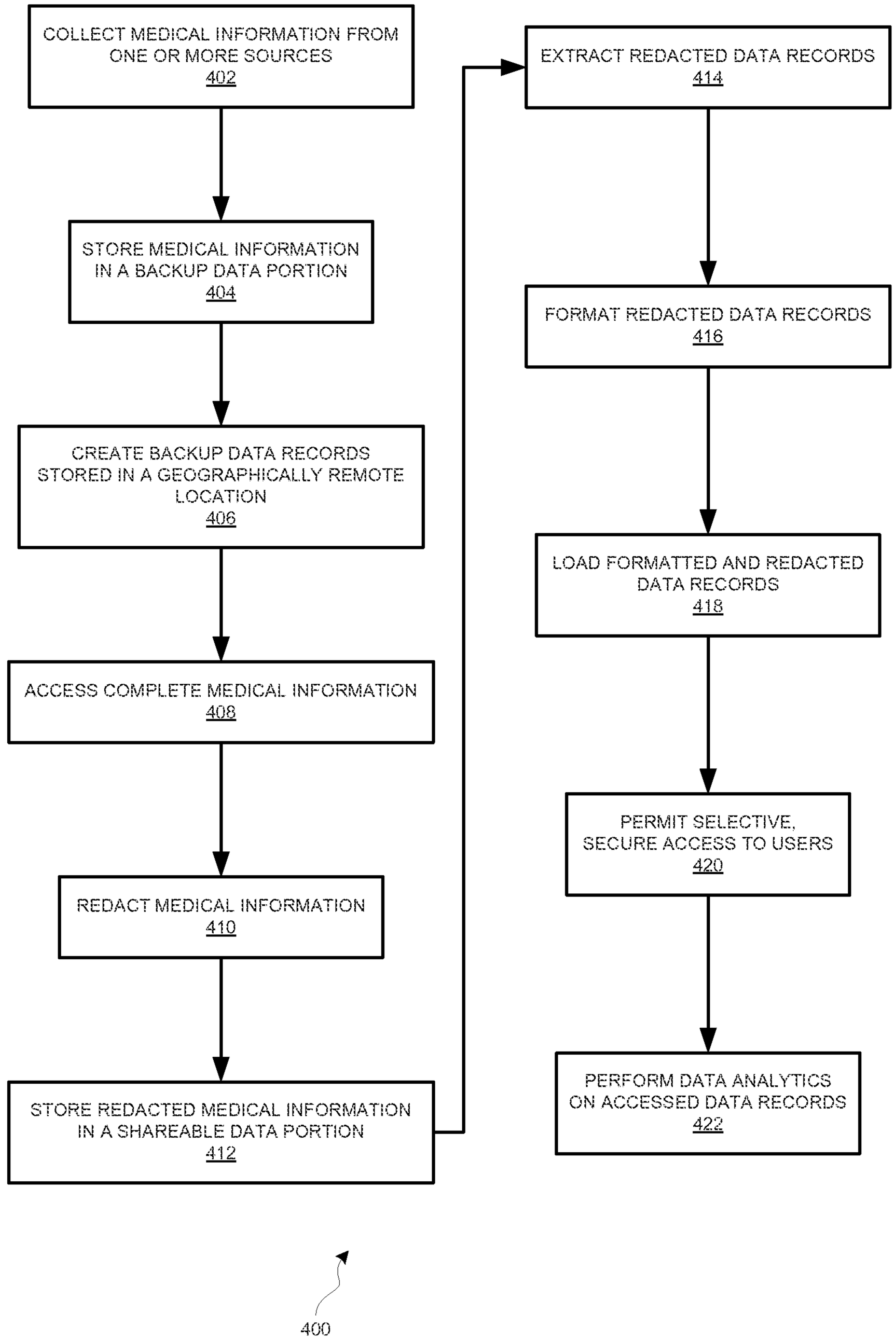

COLLECT MEDICAL INFORMATION FROM ONE OR MORE SOURCES
402
STORE MEDICAL INFORMATION IN A BACKUP DATA PORTION
404
CREATE BACKUP DATA RECORDS STORED IN A GEOGRAPHICALLY REMOTE LOCATION
406
ACCESS COMPLETE MEDICAL INFORMATION
408
REDACT MEDICAL INFORMATION
410
STORE REDACTED MEDICAL INFORMATION IN A SHAREABLE DATA PORTION
412
EXTRACT REDACTED DATA RECORDS
414
FORMAT REDACTED DATA RECORDS
416
LOAD FORMATTED AND REDACTED DATA RECORDS
418
PERMIT SELECTIVE, SECURE ACCESS TO USERS
420
PERFORM DATA ANALYTICS ON ACCESSED DATA RECORDS
422
400

FIG. 4

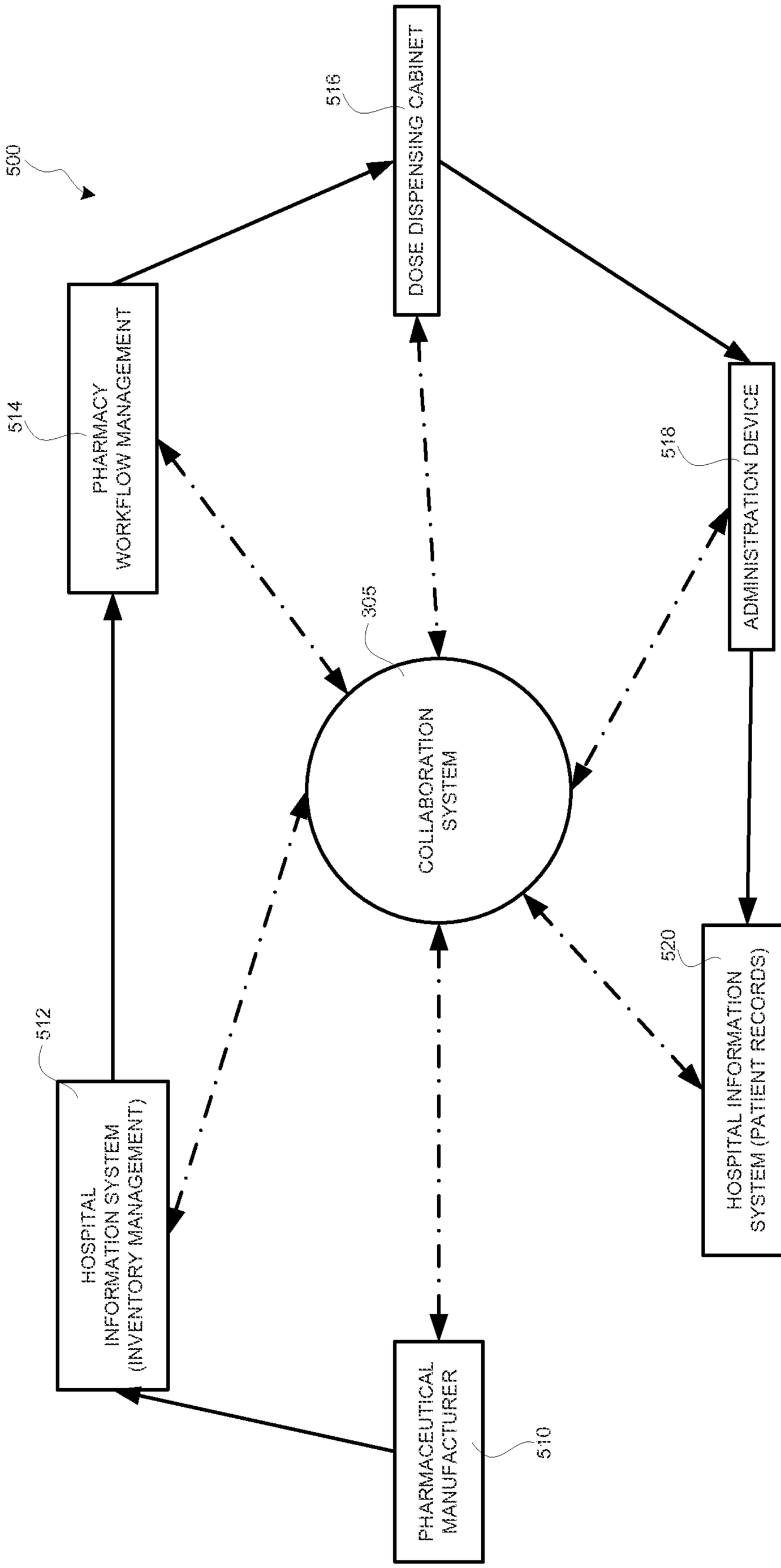

500
514
PHARMACY WORKFLOW MANAGEMENT
516
DOSE DISPENSING CABINET
518
ADMINISTRATION DEVICE
305
COLLABORATION SYSTEM
512
HOSPITAL INFORMATION SYSTEM (INVENTORY MANAGEMENT)
520
HOSPITAL INFORMATION SYSTEM (PATIENT RECORDS)
510
PHARMACEUTICAL MANUFACTURER

FIG. 5

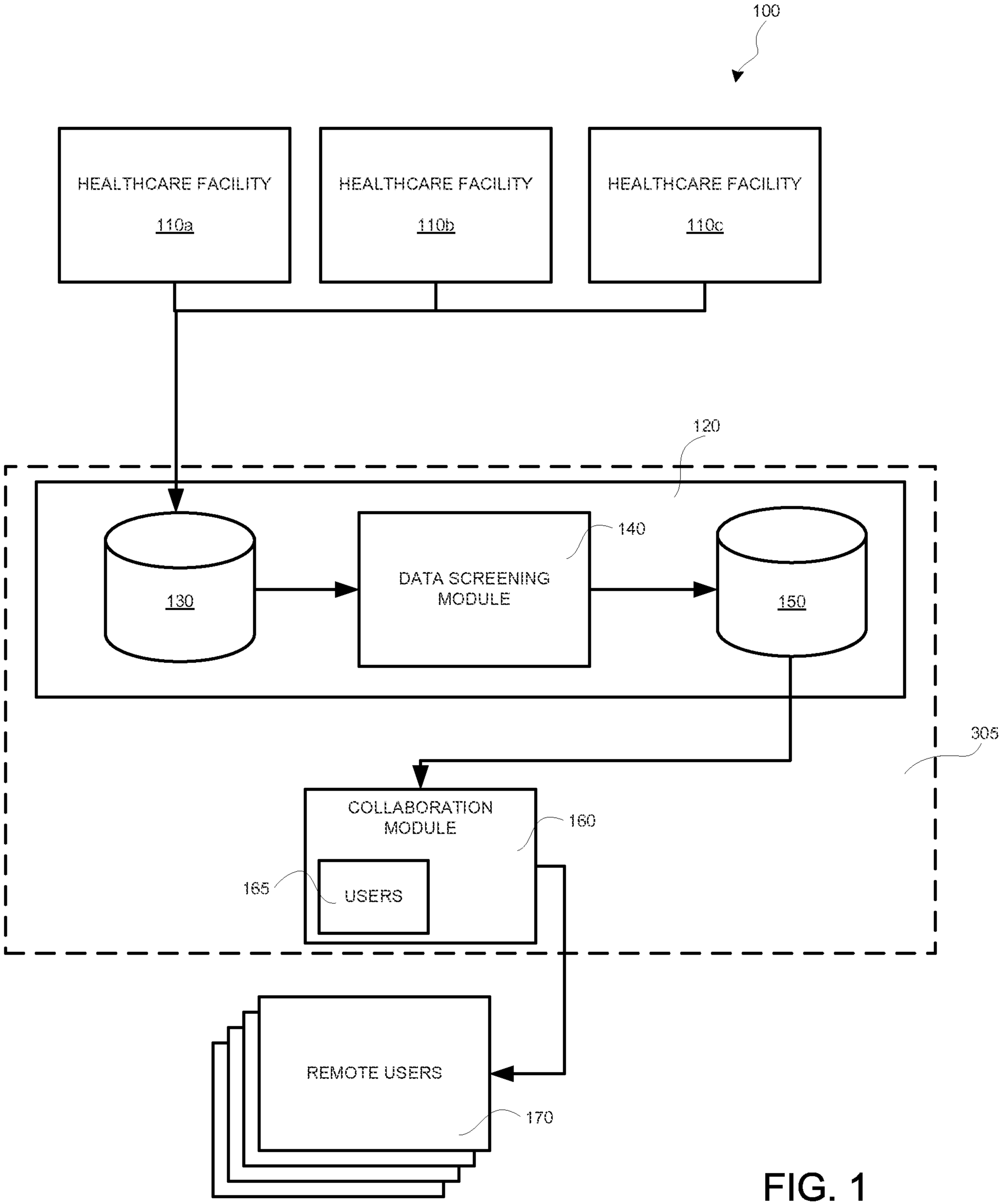

100
HEALTHCARE FACILITY
110a
HEALTHCARE FACILITY
110b
HEALTHCARE FACILITY
110c
120
130
DATA SCREENING MODULE
140
150
305
COLLABORATION MODULE
160
165
USERS
REMOTE USERS
170

FIG. 1