



- (51) International Patent Classification:
G06Q 40/00 (2012.01)
- (21) International Application Number:
PCT/US2017/026851
- (22) International Filing Date:
10 April 2017 (10.04.2017)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
62/320,363 8 April 2016 (08.04.2016) US
- (71) Applicants: **EMOCHA MOBILE HEALTH INC.** [US/US]; 1812 Ashland Avenue, Suite 100, Baltimore, MD 21205 (US). **JOHNS HOPKINS UNIVERSITY** [US/US]; 3400 N. Charles Street, Baltimore, MD 21218 (US).
- (72) Inventors; and
- (71) Applicants : **SHAH, Maunank** [US/US]; c/o Johns Hopkins University, 3400 N. Charles Street, Baltimore, MD

21218 (US). **BOLLINGER, Bob** [US/US]; c/o Johns Hopkins University, 3400 N. Charles Street, Baltimore, MD 21218 (US). **CHANG, Larry** [US/US]; c/o Johns Hopkins University, 3400 N. Charles Street, Baltimore, MD 21218 (US). **MCKENZIE-WHITE, Jane** [US/US]; c/o Johns Hopkins University, 3400 N. Charles Street, Baltimore, MD 21218 (US).

(72) Inventor: **SEIGUER, Sebastian**; c/o Emocha Mobile Health Inc., 1812 Ashland Avenue, Suite 100, Baltimore, MD 21205 (US).

(74) Agents: **HAUGHEY, Paul C.** et al.; Kilpatrick Townsend & Stockton LLP, Mailstop: IP Docketing - 22, 1100 Peachtree Street, Suite 2800, Atlanta, GA 30309 (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, DJ, 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, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA,

[Continued on next page]

(54) Title: VIDEO-BASED ASYNCHRONOUS APPOINTMENTS FOR SECURING MEDICATION ADHERENCE

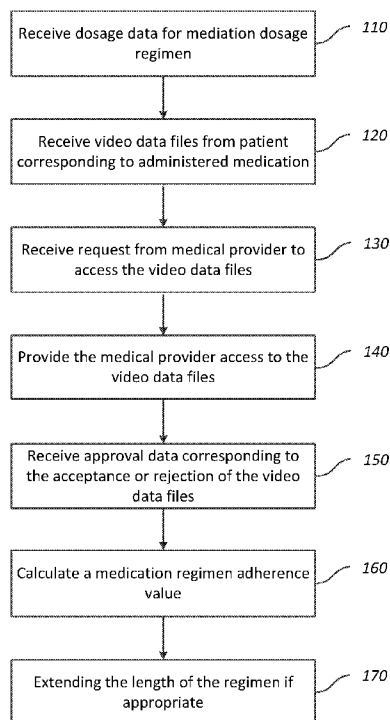


FIG. 1

(57) Abstract: Certain embodiments include a computer-implemented method comprising receiving dosage data corresponding to a medication dosage regimen for a medication prescribed to a patient and receiving, from a remote mobile device, video data files including video of the patient administering the medication at intervals defined by the medication dosage regimen. A request by a medical provider to access the one or more video data files is received and access is provided based on a set of credentials. Approval data is received from the provider to indicate whether the video data files show proof of the patient taking a correct dosage of the medication as defined in the medication dosage regimen. A medication regimen adherence value is then calculated based on the medication dosage regimen and the approval data medication.



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.

TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, 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).

(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,

Published:

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

VIDEO-BASED ASYNCHRONOUS APPOINTMENTS FOR SECURING MEDICATION ADHERENCE

5

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a PCT application and claims the benefit and priority of U.S. Provisional Application No. 62/320,363, filed April 8, 2016 and titled "VIDEO-BASED
10 ASYNCHRONOUS APPOINTMENTS FOR SECURING MEDICATION ADHERENCE," which is hereby incorporated herein by reference in its entirety for all purposes.

BACKGROUND OF THE INVENTION

15 [0002] The present disclosure relates in general to health care, and in particular to systems and methods for video Directly Observed Therapy (DOT).

[0003] Medication adherence is a significant problem in the United States, with adherence levels for self-administered medication at about 60%. Tuberculosis (TB) is contagious and has a high mortality rate, which is why the long-held standard of care is Directly Observed
20 Therapy, or DOT. In DOT, the clinician is required to watch the patient take their medication in person. With DOT, adherence levels of over 90% can be achieved, but requires daily, in-person treatment, which can be far too costly for the system and burdensome for the patient. Other medications may be administered using DOT, such as Hepatitis C Virus (HCV) medications, HIV medications, opioid addiction therapy medications, etc.

25 [0004] In the United States, health departments spend millions of dollars driving to patients' homes every day to conduct DOT on TB patients. While there are only approximately 10,000 new cases of TB per year, the high mortality rate makes DOT critical. As such, health departments use their limited resources in such a manner because poor adherence to TB treatments can lead to more dangerous drug resistant forms of TB, spread of
30 the disease, and deterioration of the patient's health. More than 11 million people in the U.S. have Latent TB Infection (LTBI). In many cases, LTBI is managed by public health departments. The most effective regimen for LTBI is a 12-dose, 12-week regimen. Directly

Observed Therapy (DOT) is the CDC recommended standard of care. However, other self-administered regimens are often prescribed due to lack of public health department resources to perform DOT. Better methods of easing the burden of DOT-based medication regimens are needed.

5 [0005] With advances in computer technology and the Internet, home verification systems have been devised. For example, U.S. Pub. 20160259911 “Automated Medication Adherence System” describes the use of real time video to verify a patient taking medication: “In application, the patient faces the video camera so that the operator at the central computer can witness the patient administering the medication. Further, during the entire administering
10 session, neither the medication container nor the dosage is ever removed from the view of the camera and the operator stationed at the central computer so that while the prescribed medication is being administered by the patient, the medication remains in front of the camera until completely administered by the patient.” (Abstract).

[0006] U.S. Pub. 20080076973 “Remote Health Care System With Treatment Verification”
15 describes a similar system: “The patient presents the pill to the video camera 102 such that the medical professional is able to confidently identify it. The patient is then instructed to ingest the pill. The patient ingests the pill. The medical professional then optionally requests that the patient open their mouth to clearly show that the pill is not in their mouth. Further optionally, the patient shows the hand that held the pill before the pill was ingested. In this
20 way the medical professional is able to confidently establish that the patient has swallowed the pill.” (paragraph 0028).

[0007] U.S. Pub. 20150061832 “Directly Observed Thearpy [sic] Using Mobile Technology” describes using video in combination with unlocking a compartment of a medication dispensing device: “The device may be used to acquire video data showing the
25 identity of the patient, and to transmit that data to a first computing device at a control center for verification of the patient's identity, as described above. After the patient's identity has been verified, the device may receive a signal from the control center causing the solenoid to rotate the dispenser until a chamber (1-7) is positioned adjacent the retractable window. Medication within that chamber can then be removed by the patient. An application running
30 on the device subsequently may cause the touch screen to display instructions for acquiring video of the administration or ingestion of the medication, and subsequently transmitting that

video to the control center to verify that the patient has complied with their therapy.” (paragraph 0026).

[0008] While the above described systems eliminate the need for travel to monitor a patient taking medication, it would be desirable to further limit the burden on medical personnel.

5

SUMMARY

[0009] The present invention provides a system and method for asynchronous, remote monitoring of a patient taking medication that satisfies the requirements for Directly Observed Therapy (“DOT”). The present invention also provides a technological triage system for remotely monitoring and intervening with DOT patients using an Internet based
10 DOT program that insures patients most needing attention are addressed first.

[0010] In one embodiment, patient dosage data and a corresponding medication regimen are stored in a patient profile. A patient securely accesses the profile and is prompted to record a video file showing the patient taking the medication according to the regimen. The video file is encrypted and uploaded to a secure database. A medical provider is notified of
15 video files awaiting review, prioritized according to a triage method that ranks review urgency based on a patient’s demonstrated regimen adherence history. The medical provider securely accesses the video file to verify adherence, and indicates acceptance or rejection of the video file as proof of the patient taking a correct dosage of the medication as defined in the medication dosage regimen. A medication regimen adherence value is calculated based
20 on the medication dosage regimen and the approval data. The degree of monitoring of the medication dosage regimen by the medical provider is modified based on the medication regimen adherence value.

[0011] In one embodiment, a patient is progressed through multiple stages based on whether or not they submit compliant videos. As the patient demonstrates continuing
25 adherence to the protocol, the time period within which the medical provider is required to review the video is relaxed (e.g., from 6 hours to 24 hours to 48 hours). Also, the intensity of intervention is relaxed with demonstrated adherence, such as not requiring a phone call to the patient for a single missed video or non-compliant video.

[0012] In one embodiment, a patient progresses through at least 3 stages. The first stage,
30 App Download, requires the patient to successfully download the application and record and upload a test video. If the patient fails after multiple tries, they become ineligible for the

Internet based DOT program. Upon successful completion of the App Download stage, the patient enters an Onboarding stage with high intervention intensity. The patient is required to demonstrate 100% compliance of at least two video recordings to move onto the third stage. In the third stage, less than 100% compliance is required, and the intervention intensity is reduced after a period of demonstrated compliance. The intervention intensity is increased if there is a faltering in the demonstrated compliance. In one embodiment, the third stage is itself composed of 3 stages, the Habit Building stage, Performance stage and Autopilot stage, with different degrees of required compliance and intervention intensity.

BRIEF DESCRIPTION OF THE DRAWINGS

10 **[0013]** FIG. 1 shows a simplified method 100 for enabling asynchronous appointments for securing medication adherence, according to certain embodiments.

[0014] FIG. 2 is a simplified block diagram of a security architecture according to certain embodiments.

15 **[0015]** FIG. 3 is a block diagram of a program architecture according to certain embodiments.

[0016] FIG. 4 is a block diagram of an infrastructure architecture according to certain embodiments.

[0017] FIG. 5 is a table of the various intervention intensities and compliance criteria according to certain embodiments.

20 **[0018]** FIG. 6 is a table of the requirements for various stages for a 5-7 day regimen according to certain embodiments.

[0019] FIG. 7 is a table of the requirements for various stages for a 3 day regimen according to certain embodiments.

25 **[0020]** FIG. 8 is a table of the requirements for various stages for a 1 day regimen according to certain embodiments.

[0021] FIGS. 9A-B are a high level flow chart of the stages according to certain embodiments.

[0022] FIG. 10 is a more detailed flow chart of one of the stages according to certain embodiments.

[0023] FIG. 11 is a diagram of a medical provider triaged review interface according to certain embodiments.

[0024] FIG. 12 is a simplified block diagram of a computing system and client computing system according to an embodiment.

5

DETAILED DESCRIPTION

[0025] In the following description, various embodiments of systems and methods for providing mobile-based, computer-aided medical care will be described. For purposes of explanation, specific configurations and details are set forth in order to provide a thorough understanding of the embodiments. However, it will also be apparent to one skilled in the art that the embodiments may be practiced without the specific details. Furthermore, well-known features may be omitted or simplified in order not to obscure the embodiment being described. For example, although a mobile internet-based Directly Observed Therapy platform is described, access need not be through a mobile device, and could use a desktop computer, smart television, game console, or any other computing device with a camera, or connectable to a camera or media from a camera.

[0026] In certain embodiments, asynchronous appointments may be used to secure medication adherence for patients requiring directly observed care. Using asynchronous video DOT, asynchronous video-based direct observation allows for the patient and the healthcare worker to engage in the activities of a face-to-face appointment with each party performing their aspect of the appointment at different times, independent of one another. In some embodiments, the purpose of such appointments can be for the healthcare worker to verify ingestion, inhalation, or infusion of medication through observation. While a live, in-person appointment may be replicated nearly exactly through a live video observation, asynchronous video DOT enables a non-live appointment, which would not be possible without the use of the technology. The patient is free to take their medication at any time during a “check in window,” while the healthcare worker is able to assess the video with the assistance of the technology at any time thereafter.

[0027] In some embodiments, many different permutations of asynchronous appointments can be supported. For example, a patient may be required to take their medication (if there are multiple pills) at many times throughout the day. The healthcare worker can assess the entire episode at a later time, reviewing each video separately or as single compiled video (referred to as “batching”), and assess all of them together as one episode or “dose.”

Medication adherence can then be calculated accordingly. In another scenario, a patient can take their medication at one or more times throughout the day, and several healthcare workers can review and accept the dosage, as if in-person, each at different times (i.e., asynchronous direct observed care) in the day.

5 **[0028]** In a typical operation, a patient can record a video of themselves taking their prescribed medication via asynchronous video DOT software on their mobile computing device (e.g., smart phone, laptop computer, smart watch, etc.). If the patient has internet access, the recorded videos can be sent immediately to the asynchronous video DOT server. The video files can be sent individually or may be batched, as noted above. In situations
10 where internet access is sparse or intermittent, or in areas with very slow data rates, portions of the individual videos may be sent, whenever possible, from the patients computing device and may be reassembled at the asynchronous video DOT server side.

[0029] In situations where a patient may have extended periods of time with no internet access, the patient can operate their asynchronous video DOT software offline and continue
15 to take their prescribed medication(s) and record a video. The videos will continue to be stored on the patient's mobile computing device until an internet connection becomes available. The videos may be stored in any suitable format on the patient's computing device, and may be saved individually or batched, and individual video files may be saved as a number of pieces or portions of the entire video entry (in consecutive or non-consecutive
20 order) and reassembled at a later time by the asynchronous video DOT server(s) when transferred. Once their computing device establishes an internet connection, the stored videos can be sent to the asynchronous video DOT server for medical provider access. In that way, the medical provider may then review all of the videos at once and approve or disapprove each video in their own time – asynchronously with the actual time that the
25 medication was administered, but still within the guidelines of typical programs requiring DOT-based verification.

[0030] In certain embodiments, each recorded video may be encrypted to prevent unintended parties from accessing and viewing them. The videos can be encrypted while on the patient's mobile computing device, while they are transmitted from the mobile device to
30 the asynchronous video DOT server computer(s), and while saved on the asynchronous video DOT server computer(s). Different types of encryption may be used or combined. For instance, the video files may be encrypted on patient's mobile device and further encrypted

during transmission to the asynchronous video DOT server(s). In some embodiments, the video recordings are not accessible while they are stored on the patient's mobile phone. For example, the patient cannot access the videos on their mobile device using their standard operating system media library that may store other photos, videos, audio recordings, and the like. If a user accesses or copies the files using directory management software (e.g., Windows Explorer), the files can still be encrypted to prevent access to unauthorized viewers.

[0031] In certain embodiments, a dose-by-dose adherence calculation using asynchronous direct observation can be performed with specialized asynchronous video DOT-based software. The software provides workflow and visualization to bring the two independently-performed activities together in such a way as to allow for an extremely accurate, dose-by-dose calculation of the medication adherence rate. This calculation would not be possible for patients who are not under direct observation for every single dose. As such, medication adherence as a dose-by-dose statistic is not currently available in medical care without direct observation. The implementation of asynchronous video DOT can solve this problem.

[0032] Conventional methods may use other calculations currently used as proxies for the actual dose-by-dose adherence rate. For example, a currently accepted medical standard is called Proportion of Days Covered and calculates medication adherence based on the timeliness of the patient picking up their medication from the pharmacy. There are a few exceptions, such as Tuberculosis (TB), where the standard of care is direct observation of ingestion. In TB care, the patient travels to the clinic, or a healthcare worker travels to the patient, nearly every day. The healthcare worker verifies several aspects of care, as required by the CDC: 1) identification of the medication; 2) capture of any side effects experienced by the patient since the last dose; 3) medication ingestion; and 4) document the visit.

[0033] It should be noted that the video-based asynchronous appointments for securing medication adherence, as described herein, can be applied to any suitable medication. For instance, applications of the embodiments described herein can work equally well for infections like TB, chronic conditions like Hepatitis C or congestive heart failure, or other conditions like hemophilia, asthma, and more, as would be appreciated by one of ordinary skill in the art. Also, multiple prescriptions can be applied to the various embodiments presented in this disclosure. For instance, asynchronous video DOT software can manage the administering of multiple medications in separate patient-recorded video files, or in the same

video file (e.g., the patient records taking a dose of two medications at the same time on the same video).

[0034] In some embodiments, an assessment of video(s) to calculate adherence using asynchronous video DOT can include the patient submitting a video of themselves, which includes sound and images. Unlike a “smart pill” bottle, which may provide information that the medicine bottle was opened, the adherence calculation is driven by both a video being submitted and the healthcare worker(s) reviewing the video and determining that the medication was taken. By the healthcare worker(s) accepting or acknowledging that a prescribed dose of medication was properly taken, based on the video(s), the adherence calculation is increased by a dose. By rejecting or denying the fact that a prescribed dose of medication was taken, the number of doses taken does not increase, but the healthcare worker may fill out a report explaining the rejection.

[0035] In some implementations, asynchronous video DOT software can capture visual evidence that medication was taken, or can be used to infer that medication was “missed” or not taken. When a dose is not taken, the patient’s regimen can be automatically extended by one day into the future. Side effects can be captured and reported through a questionnaire via a asynchronous video DOT software interface. If the patient or the healthcare worker chooses, the side effects as well as all application instructions can be displayed in another language, or as icons/images for those who cannot read one of the languages available. In some embodiments, asynchronous video DOT software can generate notifications and sent using any suitable communication protocol including SMS, email, or in-application notifications. The asynchronous video DOT software may provide notifications that can be directed to the patient or the healthcare worker and may inform of side effect reports, missed doses, or patients determined to be at risk of missing a dose in the near future.

[0036] FIG. 1 shows a simplified method 100 for enabling asynchronous appointments for securing medication adherence, according to certain embodiments. Method 100 can be performed by processing logic that may comprise hardware (circuitry, dedicated logic, etc.), software operating on appropriate hardware (such as a general purpose computing system or a dedicated machine), firmware (embedded software), or any combination thereof. In certain embodiments, method 100 can be performed at least by the systems shown and described in the appendices.

[0037] At step 110, method 100 includes receiving, by a processor, dosage data corresponding to a medication dosage regimen for a medication prescribed to a patient. The dosage data may include a type of medication to be administered, a frequency that the medication is to be administered, and a dosage that the medication is to be administered.

5 [0038] At step 120, method 100 includes receiving, by the processor from a remote mobile device, one or more video data files including video of the patient administering the medication at intervals defined by the medication dosage regimen. The remote mobile device can be one of a smart phone, personal digital assistant, a smart watch, a smart headset, a laptop computer, a desktop computer, or a tablet computer. The one or more video data files
10 each include a corresponding date and time stamp.

[0039] At step 130, method 100 includes receiving a request from a medical provider to access the one or more video data files. In some implementations, a request for video data files may require the medical provider to provide credentials to prove that they are an approved medical provider that can access the video data files. At step 140, method 100
15 includes providing the medical provider access to the one or more video data files.

[0040] In some embodiments, a medical provider can be a primary care provider or staff thereof, or may be a referred care provider (i.e., third party). asynchronous video DOT can be configured to allow any approved medical provider or individual access to view and/or evaluate (accept/reject) a patient's video data files.

20 [0041] At step 150, method 100 includes receiving approval data corresponding to the medical provider's acceptance or rejection of the one or more video data files as proof of the patient taking a correct dosage of the medication as defined in the medication dosage regimen.

[0042] At step 160, method 100 includes calculating a medication regimen adherence value
25 based on the medication dosage regimen and the approval data, and, if necessary, extending the length of the regimen if appropriate (e.g., extending by a day, week, etc. depending on how many doses were missed) (step 170).

[0043] It should be appreciated that the specific steps illustrated in FIG. 1 provides a particular method 100 for enabling asynchronous appointments for securing medication
30 adherence, according to certain embodiments. Other sequences of steps may also be performed according to alternative embodiments. For example, alternative embodiments may

perform the steps outlined above in a different order. Moreover, the individual steps illustrated in FIG. 1 may include multiple sub-steps that may be performed in various sequences as appropriate to the individual step. Furthermore, additional steps may be added or removed depending on the particular applications. One of ordinary skill in the art would
 5 recognize and appreciate many variations, modifications, and alternatives of the method 100.

Security Architecture

[0044] The asynchronous video DOT platform is a suite of patient engagement and medication adherence applications, with both mobile (iOS / Android) and web components. Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the United States of
 10 America legislation that dictates the rules and provisions around data security and privacy to safeguard medical information. The asynchronous video DOT platform complies with HIPAA regulations on how to handle Protected Health Information (PHI), including but not limited to secure encryption of data, access controls, and industry-standard best practices. HIPAA has specific rules around how data should be handled and secured; for the purposes
 15 of the Cloud, the following apply:

HIPAA Privacy Rule

[0045] HIPAA Privacy rule defines Protected Health Information as any information that can identify a patient:

- Name, Address, Birth Date, Social Security Number
- 20 • An individual's health or mental condition
- Any care provided to the individual
- Information concerning payment for services

ADMINISTRATIVE REQUIREMENTS TO SATISFY THE HIPAA PRIVACY RULE

INCLUDE:

- 25 • Assignment of a privacy official
- Employee training
- Technical and Physical Safeguards
- Process for complaints
- If PHI is disclosed, mitigation

HIPAA Security Rule

[0046] HIPAA security rule requires covered entities to maintain reasonable and appropriate administrative, technical and physical safeguards to protect PHI. Specifically,

- Ensure the confidentiality, integrity and availability of all PHI created, received, maintained and transmitted
- Identify and protect against reasonably anticipated threats to the security and integrity of information
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by workforce

HIPAA enforcement

[0047] Technical and Physical Safeguards used for the present invention are listed below:

- Data is stored encrypted-at-rest
- Data is encrypted-in-flight
- All events are audit-logged
- All system access and keys are safeguarded and established according to a process
- All systems are highly-available and have disaster recovery protocols
- All system configurations are documented
- All data access is on a need-to-know basis
- Technical safeguards are in-place (such as anti-virus, anti-malware)
- Patients have the right to access their data at any time

[0048] FIG. 2 is a simplified block diagram of a security architecture according to certain embodiments. A user device 202 has an application loaded for secure access with a password and encryption capability. A web interface device 204 for a medical provider similarly has an application with secure access capability. Both user device 202 and web interface device 204 use an SSL tunnel, such as SSL tunnel 206, to communicate over the Internet 208 and through SSL tunnel 210 to a secure database 212 and file system 214.

Access

[0049] In one embodiment, access to the system is managed via password-protected user accounts. User passwords are never stored in clear text, only as a one-way encrypted digest, and are never visible to any user including asynchronous video DOT system administrators.

The system includes rules to require that users create a complex password (with configurable minimum length, and requirements for special characters, numbers, etc.), and requires that user passwords be changed periodically. All access attempts, successful or otherwise, are logged. Repeated failed attempts result in the account being locked, and may only be
5 unlocked by an administrator.

User roles and administration

[0050] In one embodiment, user accounts are defined by a set of role-based permissions and only users with elevated permissions are capable of modifying a user's access. The system's position towards any user action is "default-deny" - unless a user has specifically
10 been granted the right to perform an action via a permission they've been explicitly granted by an administrator, the action is not permitted. An interface is provided both to add and remove roles from user accounts, to define new roles, and to add and remove permissions from existing roles. Multiple roles can be assigned to the same user.

Input validation

[0051] In one embodiment, all input to the system is checked for validity before being processed into data structures. Validation is done on both the client and server side; client-side as a user-experience convenience and data input validation, and server-side for data validation. The data validation processes are required to run all inputs before any data is stored. The validation involves but is not limited to formatting, length, range, data type
20 validations, along with general malicious attack checks such as Cross-Site Scripting (XSS) attacks and Structured Query Language (SQL) injection attacks. If any validation fails, the whole request is declined and data is not stored.

Authentication & Authorization

[0052] In one embodiment, authentication is managed with a username and password.
25 Users are authorized to perform only the actions explicitly granted to them by the roles they have been assigned. Before allowing any user interaction with the system (for instance viewing patient information, creating a new user account, scheduling an appointment), the user's permissions are checked to determine if they have the privileges to perform the specified action and whether they're allowed to access the object in question. A given user
30 may be configured to only be allowed access to view or modify certain patients. In the event that a user has forgotten their password, they can request a password reset for their username.

This will generate a message to the email address associated with that account containing a time-limited link which can be used to enter a new password.

Session Management & Timeouts

[0053] In one embodiment, most interactions within the system require a valid, recent, session token which is returned as part of a successful authentication. Session identifiers are stored as encrypted cookies on the device or browser and chosen from a large, random, address space. These are not predictable and any modification of the local value will invalidate the session. No user-provided data (other cookies, roles/permissions, etc.) is used by the system and is ignored if provided. The platform only trusts the platform's database as the trusted source of information for authentication and session management. Sessions time out after a configurable period of inactivity, for which the default is 5 minutes. When timeout happens, the user must re-authenticate to continue interacting with the system.

Encryption

[0054] In one embodiment, the asynchronous video DOT platform uses two main kinds of encryption: in-flight and at-rest. In-flight encryption refers to the encryption of all data while being transmitted. Data being sent from a client, whether web-based or a mobile application, is sent over a secure HTTPS connection secured by a 2048-bit Transport Layer Security (TLS) certificate. The system audits the TLS configuration regularly, ensuring that system configuration is as up-to-date as possible. All connections between the database and application servers are made over TLS as well, utilizing the same 2048-bit certificate.

[0055] At-rest encryption means that all Protected Health Information (PHI) in the database and disk is always stored encrypted. This includes any record of a user, anything in the error log or audit log tables, any patient data, and all information submitted including video files or GPS coordinates. The encryption scheme uses the Advanced Encryption Standard (AES) algorithm of at least 256 bits, with the ability to revoke and issue new keys as needed.

[0056] Key Management for the encryption / decryption keys is accomplished through a separate server and only accessible through a highly-restrictive API through defined methodologies. Keys are only stored in-memory on the application server and never in permanent files written to disk. Effectively, the database cannot decrypt its own data; even in the event of the server being compromised and a malicious party acquiring an export of the data, PHI will remain secure. Each customer application's data (patients, check-ins,

laboratory test result data) resides in a separate database and is completely invisible to other customers.

Audit logs

[0057] Any view or edit of the system configuration or data is logged in a persistent and unmodifiable database. Audit trail records include but are not limited to the action being taken, the user who initiated the action, the date and time of the action, and in the case of modifications, both the old and new values. These logs are accessible through the administrative interface.

Infrastructure, Hosting Environment and Backups

[0058] In one embodiment, asynchronous video DOT platform's servers are hosted "in the cloud" at secure data centers. Physical access to servers are limited; all servers are single-tenant; and there is no shared hardware between asynchronous video DOT platform and any other entity. Network access to any server is limited to the specific port and IP ranges needed for the platform to function. For instance, the front-facing load balancers allow access via HTTPS from anywhere but the database servers only allow TLS access over port 3306 from the application servers they specifically support, and SSH access is only permitted from the asynchronous video DOT platform offices. Login credentials are managed by a combination of a strong authentication (username / password) and private keys. Login passwords are required to adhere to the asynchronous video DOT Password Policy, explained above. Access to production servers is only given to employees with a demonstrable need for access, mostly to provide support & maintenance for the platform.

[0059] In one embodiment, remote console access, where these settings are managed, requires a two-factor authentication token in addition to a strong password. Accounts used to connect to servers are per-user rather than a shared "root" account. This allows for individual users to be managed, or access revoked, without compromising other accounts. Backups are taken regularly; nightly backups are made of the entire encrypted database and snapshots of the entire server disk are taken, including any encrypted file uploads. These are kept available across a rolling 30-day window in case they need to be rolled back to. All data is replicated across multiple servers, in near real-time, to ensure availability. We also run monitoring software that checks, at all times, whether the service is available and functioning, and have a system in place to page on-call support personnel if needed. In addition, nothing is ever

deleted in the system; data is “soft-deleted” via marking with a flag that will hide the record during normal operations, but leave it easily recoverable if needed.

Design Overview

5 [0060] FIG. 3 is a block diagram of a program architecture according to certain embodiments. A universal RESTful API is provided, communicating entirely over HTTPS and in the JSON format (JavaScript Object Notation), and serves as the means of interaction with both the web interface and the mobile application. Full role-based user permissions are required, as is strict validation of all user input, useful error codes. Both the web interface and
10 mobile apps handle errors dynamically.

[0061] An incoming request 302 is provided to server.py 304. The main services logic lives in server.py 304 and lib/services/base.py, and handles routing specific URLs to the right services class. Debugging, error and other information is logged by logger 308. Base service module 306 sets the headers, validates inputs, checks permissions, gets any needed data and
15 sends a response. Validate module 310 validates messages. FooService module 312 performs specific functions as noted under control of Base Service module 306. FooService module 312 itself uses FooModel 314, BaseModel 316, and database module 320. Server.py 304 can also directly access the database using database module 320 and memory cache module 318.

20 [0062] Other libraries include the memcached driver, encryption wrapper (encrypted fields are defined in the model, and the field data consist of key_version, initialization vector, and encrypted value, all concatenated together), and base database connection class. The DB and memcached drivers are capable of handling multiple connections and re-connecting in the case of a temporary outage. There's a logging class, lib/logger.py, and one to send email,
25 lib/mailer.py.

[0063] Service URLs are defined in each service class, as a list with each element consisting of a dictionary with the following keys:

- method (GET, POST, PUT, or DELETE)
- uri (regex pattern)
- 30 - required (list of field names that, if missing or mis-formatted, will result in an error)

- optional (list of field names that, if present and mis-formatted, will result in an error)
- require_auth (whether to allow un-authorized requests)

Which gets compiled into a list of usable route/method combinations in server.py, with the required/optional/require_auth values used to validate the request input.

5 **[0064]** Required and optional fields are validated by methods in lib/validate.py, as defined in “Input Validation” above, and available to the service in self.inputs. The service classes themselves descend from EموchaBaseService, and implement a subset of the following methods: get, post, put, delete (each called when the URL is reached by the relevant HTTP method).

10 **[0065]** Service methods themselves are small and often involve simple permissions checks, often secondary validation, and calling a select/update/list wrapper around a model function. In more complex cases such as transactions that update multiple tables, they can be lengthier. Each method is a self-contained piece of functionality in order to maintain logical separation of architecture.

15 **Infrastructure**

[0066] There are two main software scripts at the core of the services layer. They may be run on the same machine, or each on their own instance type.

- server.py, which listens on ports 8001-8004, running one process per CPU core available, and serving the JSON over REST.

20 ○ Model: Database layer

 ○ Controller: Eموcha services modules, routed through Python Tornado Web Server.

 ○ View: JSON

25 - frontend.py, which listens on ports 8801-8804, running one process per CPU core, and serving the HTML templates for the frontend.

 ○ Model: Requests to the services AP.

 ○ Controller: Two main URI handler types:

- Web Handlers: Checks the session cookie, uses the Tornado templating engine to render the HTML template, including JS blocks to handle all dynamic content.
- JSAPI Handlers: Pass-through proxy that makes requests to services, solving AJAX same-origin issues and provides an additional layer of validation.

- View: Tornado HTML templates.

[0067] Both of these processes run behind a local nginx instance, running in proxy/load-balance configuration to route traffic across processes and handle SSL termination. Nginx listens on two ports - 80 and 443. HTTPS/443 is used for all normal traffic, and the only function of the HTTP/80 listener is to redirect traffic over to the HTTPS listener.

[0068] There are also a set of worker processes that run via cron to handle scheduled jobs for a few things:

- Data interchange with third-parties, often for test result processing.

- API-based: if the third-party has an API we can use to send/receive data, these workers will encapsulate all operations against it.
- SFTP-based: via secure File Transfer Protocol (sFTP), a third party may drop a file-based data dump to be ingested by the asynchronous video DOT platform.

- Notification engine

- Set up to run as many copies as needed
- Load configuration (which messages to send, and to whom, and when - either on a schedule or event-based) from client database.
- Send messages out via SMS, email, or in-app notifications, depending on client configuration.

- Check-in processing engine

- Updates a closed/passed/timed-out (a time window that's ended) check-in window to modify the check-in status appropriately.

- Active patients have their check-ins moved to status "MISSED"
- Paused patients have their check-ins moved to status "PAUSED"

[0069] FIG. 4 is a block diagram of an infrastructure architecture according to certain embodiments. Separate database servers are provided, with a Read-replicate database server 402 and a write-master database server 404. These communicate through one or more services servers 406 and website servers 408. Load balancers 410 and 412 distribute the communications to balance the load, and are in communication, through Internet 414, with user devices 416, 418, 420, 422 and web interface 424. In one embodiment, the Services and Website load balancers 410, 412 are actually the same piece of equipment, but logically separate. In an alternate embodiment, they may run on different hardware, pointing at different clusters of app servers, to provide scalability.

Notifications

[0070] The apps can send notifications to users/patients. A notification is defined by a few criteria:

- Who? This is a role, ebola_patient_sms, administrator_sms (essentially just a role with a single permission - GET_SMS - it can't be rolled into the regular role because people might opt out).
- Where? The business unit that the role is attached to - ebola_patient_sms for _____ County, etc.
- What? The message content. This needs to be brief (SMS has a 160-character limit) and cannot include any identifiable information (such as patient name, medical record number, etc.).
- When or Why?
 - o When? Proactive messages are sent out on a schedule - eg, a daily reminder to take your pills.
 - o Why? Notifications may be sent based on an event - eg, a check-in with positive symptoms results in a message being sent to the healthcare workers as a notification.
- How? SMS, Email, or In-app notification.

[0071] A log is kept of all messages sent, and there is a mechanism in place to send messages that may have failed during their original sending window

Web Applications

[0072] In one embodiment, the web application functions as a thin software layer around asynchronous video DOT platform core services - essentially there are two kinds of requests this handles. One is regular web pages, containing templated static HTML/CSS, with a JavaScript layer that handles all dynamic data. The second kind of "page" is the JavaScript API, essentially a proxy pass-through to a) work around AJAX Same-Origin issues, and b) hide the location of the services API from the client for additional security. The web application uses the same error logging endpoints as the mobile applications for ease of debugging.

Mobile Applications

[0073] Mobile apps can be broadly divided into two categories: data collection / enrollment / linkage (clinician-facing: SA-PHC, COMBIND), and adherence (patient-facing: midot, ebola). In either case, owing to the places deployed and the importance of data integrity, apps assume a store-and-upload model, rather than an attempt-fail-retry model. While failed transmissions need to be handled, the paradigm is more in terms of a hierarchical database that occasionally syncs, and less of an always-online app that only caches things in the event of a connection issue. Apps should not assume that a connection is available, and any operation communicating with the server should check and confirm connection availability before trying to send any data. This system deals with using mobile applications in a connection-less environment. Common issues and patterns:

- Local Storage
 - o SQLite is utilized on iOS and Android devices as a durable and structured data store.
 - o Pertinent local data storage is also utilized for storing data such as videos temporarily before an upload.
- Login credentials are cached on the device, and as best as possible to allow for a "login" even if the server is unavailable due to lack of connection.
 - o Best practice is to, on successful login against services APIs, cache the credentials by concatenating username and password (from the request being sent), and hashing (MD5, SHA1, etc) and storing the result in the SQLite database.

- On following logins, if the server is unreachable, this local table can be utilized to authenticate the user
- Data transmission.
 - Any data to be transmitted - patient enrollment, adherence check-ins, etc, are temporarily stored on a local database table before attempting to send to the server.
 - Timestamps are sent with entered records, and refer to the date/time of device entry, not the time of server receipt.
 - Re-transmission logic is presented in as clear a manner as possible, and react intelligently to specific error codes, to keep things from getting stuck in the cache and repeatedly bouncing them off of the services.
 - The guiding principle is over-transmission of data, as data loss in any amount is unacceptable.
- File uploads
 - Due to recorded video files being large in size, the video data is broken into “chunks” and transmitted to the server incrementally from the mobile device.
 - These videos are part of the adherence check-in events and are sent with timestamps and text data, along with some information on file uploads:
 - Total file size
 - Number of "chunks"
 - Size of each chunk
 - Filename
 - Server returns a file upload ID along with the success message.
 - Each chunk uploads independently, as connection is available, and sends:
 - file upload ID
 - chunk size
 - chunk position in order ("part 1 of 3", eg)
 - binary data
- Encryption
 - All data, whether it's being stored on the device or being sent to services APIs, is encrypted as soon as possible. This uses the AES algorithm, and generates a random Initialization Vector to be prepended to the encrypted payload.

- Any request that uses a session token is encrypted with the API key for the user attached to that session.

[0074] Core functionality (roles and user accounts, common lookup tables) are managed in a central public schema, but each client has their own database, created via scripts as part of the deployment process in order to house their patient information (patient PHI, monitoring check-ins, lab test results, etc).

[0075] Audit and error logs are rotated on a monthly basis, out to archive tables (eg, md.audit_logs_04_2015) for performance reasons.

[0076] Most "delete" operations are soft-deletes (that is, set the boolean field is_deleted to true, which hides the records in all queries) rather than hard-deletes (actual SQL delete statements). Patients, Users, Checkins, etc must be soft deletes, but other data - sessions, user -> role mappings, can be deleted.

Multi-stage Compliance progression

[0077] In some embodiments, the platform progresses a patient through multiple stages of compliance. The terms used in the following description are described in Table 1 below:

Term	Definition and Comments
Intervention Intensity	Level of responsiveness by the healthcare worker(s) charged with monitoring the patient. There are three levels: high, medium, low. Each level of intensity has differing requirements for (1) maximum time elapsed between video submission and review, (2) action required in the case of non-compliance; (3) patient performance required to proceed to next stage
Compliance Criteria	All criteria assessed by a User to determine whether a patient-submitted video can be accepted as successful Directly Observed Therapy. Criteria can be broken into two categories: General Process and Critical Criteria. A particular Intervention Intensity or Stage may require that non-compliance relate to a Critical Criteria in order to trigger certain actions.
Duration	The number of days of therapy, or doses, required for a Stage. For example, if a Regimen requires 3x per week medication (MWF), a Stage with a duration of 3 will take 5 calendar days if started on Monday.
Stage	The first few weeks are critical for the healthcare worker to develop strong adherence habits by the patient. This time is broken into four stages. Each stage may have differing Intervention Intensity, duration, Adherence Requirements.
Adherence Requirement	For each regimen, a Stage will have a certain minimum % of successful doses observed in order for the patient to progress to the next Stage.

Regimen	Regimen refers to the number of days per 7-day week a patient is expected to take medication. Regimen also refers to the specific medications that are expected to be observed. Different Regimens may have different Stage durations.
Range	Regimens have a Range which determines up to how many days late an observation can occur. These Ranges are fixed. For a 7-day regimen, the Range = 0. For a 5-day regimen, the range = 2. For a 3-day regimen the Range is 2. For a 1-day regimen the Range is -1 or 3. Example #1: a 3-day regimen requires medication to be taken M-W-F. A patient takes each of these three doses 2 days late: W-F-Sun. The patient has completed 3 doses in 7 days. Example #2: a 5-day regimen. Example #2: A 5-day regimen requires a patient to take medication M-T-W-Th-F. The patient instead takes medication W-Th-F-Sa-Su. The patient has completed 5 doses in a 7-day period. Example #3: a patient has a 1x per week regimen (LTBI) and is required to take their medication every Thursday for 12 weeks total with 4 days minimum in between doses. The medication can be taken as early as Wednesday and as late as Sunday.
Target Day	The Target Day is the specific day a dose is expected. It is possible to achieve 100% adherence while missing the Target Day, provided that doses are taken within the Range.

Table 1

[0078] FIG. 5 is a table of the various intervention intensities and compliance criteria according to certain embodiments. As a patient progresses and shows the ability to meet the compliance criteria, the intervention intensity is lowered from high to medium to low. The intervention intensity, as can be seen in FIG. 5, dictates how soon a medical provider needs to review a video for compliance after a patient video is submitted. At high intensity, 4-6 business hours is required, medium intensity requires review within 24 hours and low intensity within 48 hours. These time periods may be varied, with the amount of time being extended for lower intensity interventions. In addition, the intensity level dictates whether a medical provider needs to call the patient after any missed or noncompliant video, only after two errors, etc. Positive feedback to the patient is also provided in the form of a congratulatory call or message upon 100% compliance.

[0079] FIG. 6 is a table of the requirements for various stages for a 5-7 day regimen according to certain embodiments. Five stages are shown, (1) app download, (2) onboarding, (3) habit building, (4) performance and (5) autopilot. The adherence requirement starts at 100% for the patient to demonstrate the ability to use the system. The adherence requirement then drops to 80% over a larger number of doses, allowing the patient an occasional slip. In the last stage, the adherence requirement is raised back to 90%, since the intervention

intensity will be low. Thus, the patient is required to maintain a high adherence score in order to be trusted to properly take the medication without prompt monitoring by a medical provider.

[0080] FIG. 7 is a table of the requirements for various stages for a 3 day regimen according to certain embodiments.

[0081] FIG. 8 is a table of the requirements for various stages for a 1 day regimen according to certain embodiments.

App Download Stage

[0082] FIGS. 9A-B are a high level flow chart of the stages according to certain embodiments. As shown in FIG. 9A, a disease state (902) and a regimen (904) are selected. The regimen may be the 1, 3 or 5-7 day regimens shown in FIGS. 6-8. This is typically done by the medical provider for a patient. The patient then downloads the app (908) and enters a login and password for access. The patient is prompted to record a test video for upload. It is determined if the patient was successful (910). If the patient fails to properly complete the test upload or otherwise fails to download an operate the app, the patient will be eligible to try again (912). The patient is indicated as unsuitable for using the app (914) after a number of failures, such as 3 failures.

Onboarding Stage

[0083] In the onboarding stage (916), the patient is required to record and upload 1-3 videos depending on the regimen. The patient is typically required to read a script, such as identifying themselves by name and/or birthdate, identifying the medication and dosage, etc. The patient needs to be 100% successful for 1-2 doses, but can be 2/3 successful for 3 doses or more in this stage. Intervention and escalation (918) is administered as needed. It is determined if the patient was successful (920). If the patient fails to properly complete the video upload or otherwise fails to adhere to the protocol (e.g., the video doesn't show the pill going into the patient's mouth, or the patient didn't correctly read the script), the patient will be eligible to try again (922). The patient is indicated as unsuitable for using the app (924) after a number of failures, such as 3 failures.

[0084] Through the use of an adequate patient script, the asynchronous review of the video is made possible, without the real-time need for a medical provider to prompt and correct the

user. Also, an adequate script enables a simple interaction, without requiring specialized, locking pill containers or other special apparatus. One embodiment of a script is set forth below:

1. State your name and today's date.
- 5 2. State the name of the medication.
3. Hold the medication bottle or other packaging up to the camera, showing the label.
4. Open the bottle in view of the camera.
- 10 5. Place the medication in your mouth in view of the camera, then drink water or other liquids to show washing it down and swallowing.

Habit Forming Stage

[0085] In the habit forming stage (926), since the patient has already demonstrated the capability to adhere to the regimen, only 80% adherence is required over a larger number of doses, such as 5 doses. Intervention and escalation (928) is administered as needed, per the
 15 above-described schedule. It is determined if the patient was successful (930). If the patient fails to properly complete the test upload or otherwise fails to download and operate the app, the patient will be eligible to try again (932). The patient is indicated as unsuitable for using the app (934) after a number of failures, such as 3 failures.

Performance Stage

20 [0086] As shown in FIG. 9B, the user then enters the performance stage (936). The performance stage can be considered a continuation of the habit forming stage, but with the intervention intensity lowered to medium, as defined above. The adherence requirement remains at 80%. The patient may then complete the performance stage if the regimen criteria is satisfied (940). Although the steps are not shown in FIG. 9B, the user can remain in the
 25 performance stage or be disqualified depending on the number of failures, as for the previous stages.

Performance Stage

[0087] Upon completion of the performance stage, the patient is assigned a score or grade and placed in an appropriate intervention group (942). The grade provides an estimate of

future adherence rates based on past performance. A patient with 100% adherence will be placed in a low intensity intervention group, while patients with lower adherence will be placed in medium or high intensity intervention groups. The grade can also be used to determine eligibility (944) instead of allowing the patient multiple tries at passing the performance stage. If the grade is too low, the patient is removed from the program (946). Otherwise, the patient enters the autopilot stage (948) at the assigned intervention level. Interventions and escalations are administered according to the medical provider's engagement level (950). If the patient successfully completes the autopilot stage (952), the patient treatment is complete (954). Otherwise, the patient is unqualified for intervention (946) and is removed from the program.

[0088] FIG. 10 is a more detailed flow chart of a generic stage according to certain embodiments. FIG. 10 illustrates the recurring process for the example between app download and onboarding, but is applicable to the process, which recurs, between other stages. A trigger occurs (1002) in the stage, such as a video being submitted, or a video being missed and the time period has expired for submitting the video. Upon review by a medical provider, it is determined whether provider intervention or engagement is required (1004). If engagement is required, it is determined whether stage repetition is required (1006). If repetition is required, it is determined if the patient has failed the maximum allowed number of times (1008). If not, the stage is restarted (1010), with the system automatically restarting or resetting the onboarding or other stage. If the maximum number of failures has been reached, the patient is not suitable for intervention (1012).

[0089] If no stage repetition is required (1006), it is determined if escalation of intervention intensity is required (1014). If no intervention is administered and the patient continues the stage (1018). If escalation is required, the provider engagement level is escalated and intervention is administered accordingly (1016). The patient then continues the stage.

Medical Provider Interface

[0090] FIG. 11 is a diagram of a medical provider triaged review interface 1102 according to certain embodiments. This diagram illustrates some concepts, and a variety of different interfaces could be used, with different manners of arranging and displaying the data. The interface shows uploaded patient videos ready for review, with a first video 1104 being the one triaged to be the most important to review first. Where a patient has multiple videos for

review, this is indicated by multiple video camera icons for patients videos 1106 and 1108. A number of patients are overdue submitting videos, and thus no video icon is shown for patients 1110, 1112 and 1114. In addition, the border of these boxes may be highlighted in red, or another form of emphasis can be provided. Videos for different patients are thus
 5 queued up for review based on the patient adherence intensity level. The queue is updated in real time as missing or late patient videos are received, or as partial video uploads are completed. The order of the presented videos are thus continuously updated, invisibly to the medical provider, so that when the medical provider logs on and starts reviewing the videos, they are in the real-time, appropriately triaged order.

10 **[0091]** The PROVIDER ENGAGEMENT INTENSITY (PEI) varies automatically based on the patient's performance. The PEI has three categories: high, medium, low. Actions and interventions are programmed for each category. Sample pre-determined actions:

- o review patient video within X hours
- o call patient in certain circumstances
- 15 ☐ failure to submit a video
- ☐ submitting a non-compliant video
- ☐ good performance

- Providers are prompted by the system to interact with the patient at certain times

On the provider interface, videos are sorted based on the PEI level. Because the PEI level
 20 determines the maximum delay between video submission and video review, the videos can be sorted in order of time left for the provider to review, which will usually mirror the PEI.

[0092] In one embodiment, additional information is provided on a medical provider interface, with the ability to drill down for more information. For example, an interface display can set forth a list of the patient videos needing review. The list includes patients
 25 who have not uploaded a video in the designated time period. The list can be dynamically modified as patient videos come in later, with a high priority patient being re-categorized as lower priority with a late arriving video. The interface can indicate the time the video was recorded, the time of submission, any side effects indicated by the patient, the numerical progress through the dosage regimen, the current adherence percentage and raw numbers
 30 (e.g., 2/5). The interface will also indicate when videos have been reviewed.

[0093] In one embodiment, based on the medical provider's inputs, the medical provider is prompted to undertake certain interactions depending upon the stage and adherence as described above. For example, if a video is marked as non-compliant, the medical provider may be prompted to call the patient depending on the patient's adherence record, stage, and the type of non-compliance. For a major non-compliance, such as the wrong medication, or the wrong patient name, the medical provider may be prompted to call the patient immediately. For a minor non-compliance, such as a minor error in reading the script, the medical provider may not be prompted to call, or may be prompted to call within the next week as opposed to immediately.

Computer Systems for Client Server System

[0094] Various operations described herein may be implemented on computer systems. FIG. 12 shows a simplified block diagram of a representative computing system 1202 and client computing system 1204 usable to implement certain embodiments of the present invention. In various embodiments, computing system 1202 or similar systems may implement the remote server, or any other computing system described herein or portions thereof. Client computing system 1204 or similar systems may implement user devices such as a smartphone or other user device.

[0095] Computing system 1202 may be one of various types, including processor and memory, a handheld portable device (e.g., an iPhone® cellular phone, an iPad® computing tablet, a PDA), a wearable device (e.g., a Google Glass® head mounted display), a personal computer, a workstation, a mainframe, a kiosk, a server rack, or any other data processing system.

[0096] Computing system 1202 may include processing subsystem 1210. Processing subsystem 1210 may communicate with a number of peripheral systems via bus subsystem 1270. These peripheral systems may include I/O subsystem 1230, storage subsystem 1268, and communications subsystem 1240.

[0097] Bus subsystem 1270 provides a mechanism for letting the various components and subsystems of server computing system 1204 communicate with each other as intended.

Although bus subsystem 1270 is shown schematically as a single bus, alternative embodiments of the bus subsystem may utilize multiple buses. Bus subsystem 1270 may form a local area network that supports communication in processing subsystem 1210 and

other components of server computing system 1202. Bus subsystem 1270 may be implemented using various technologies including server racks, hubs, routers, etc. Bus subsystem 1270 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. For example, such architectures may include an Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnect (PCI) bus, which may be implemented as a Mezzanine bus manufactured to the IEEE P1386.1 standard, and the like.

[0098] I/O subsystem 1230 may include devices and mechanisms for inputting information to computing system 1202 and/or for outputting information from or via computing system 1202. In general, use of the term “input device” is intended to include all possible types of devices and mechanisms for inputting information to computing system 1202. User interface input devices may include, for example, a keyboard, pointing devices such as a mouse or trackball, a touchpad or touch screen incorporated into a display, a scroll wheel, a click wheel, a dial, a button, a switch, a keypad, audio input devices with voice command recognition systems, microphones, and other types of input devices. User interface input devices may also include motion sensing and/or gesture recognition devices such as the Microsoft Kinect® motion sensor that enables users to control and interact with an input device, the Microsoft Xbox® 360 game controller, devices that provide an interface for receiving input using gestures and spoken commands. User interface input devices may also include eye gesture recognition devices such as the Google Glass® blink detector that detects eye activity (e.g., “blinking” while taking pictures and/or making a menu selection) from users and transforms the eye gestures as input into an input device (e.g., Google Glass®). Additionally, user interface input devices may include voice recognition sensing devices that enable users to interact with voice recognition systems (e.g., Siri® navigator), through voice commands.

[0099] Other examples of user interface input devices include, without limitation, three dimensional (3D) mice, joysticks or pointing sticks, gamepads and graphic tablets, and audio/visual devices such as speakers, digital cameras, digital camcorders, portable media players, webcams, image scanners, fingerprint scanners, barcode reader 3D scanners, 3D printers, laser rangefinders, and eye gaze tracking devices. Additionally, user interface input

devices may include, for example, medical imaging input devices such as computed tomography, magnetic resonance imaging, position emission tomography, medical ultrasonography devices. User interface input devices may also include, for example, audio input devices such as MIDI keyboards, digital musical instruments and the like.

- 5 **[0100]** User interface output devices may include a display subsystem, indicator lights, or non-visual displays such as audio output devices, etc. The display subsystem may be a cathode ray tube (CRT), a flat-panel device, such as that using a liquid crystal display (LCD) or plasma display, a projection device, a touch screen, and the like. In general, use of the term “output device” is intended to include all possible types of devices and mechanisms for
- 10 outputting information from computing system 1202 to a user or other computer. For example, user interface output devices may include, without limitation, a variety of display devices that visually convey text, graphics and audio/video information such as monitors, printers, speakers, headphones, automotive navigation systems, plotters, voice output devices, and modems.
- 15 **[0101]** Processing subsystem 1210 controls the operation of computing system 1202 and may comprise one or more processing units 1212, 1214, etc. A processing unit may include one or more processors, including single core processor or multicore processors, one or more cores of processors, or combinations thereof. In some embodiments, processing subsystem 1210 may include one or more special purpose co-processors such as graphics processors,
- 20 digital signal processors (DSPs), or the like. In some embodiments, some or all of the processing units of processing subsystem 1210 may be implemented using customized circuits, such as application specific integrated circuits (ASICs), or field programmable gate arrays (FPGAs). In some embodiments, such integrated circuits execute instructions that are stored on the circuit itself. In other embodiments, processing unit(s) may execute instructions
- 25 stored in local storage, e.g., local storage 1222, 1224. Any type of processors in any combination may be included in processing unit(s) 1212, 1214.

- [0102]** In some embodiments, processing subsystem 1210 may be implemented in a modular design that incorporates any number of modules (e.g., blades in a blade server implementation). Each module may include processing unit(s) and local storage. For
- 30 example, processing subsystem 1210 may include processing unit 1212 and corresponding local storage 1222, and processing unit 1214 and corresponding local storage 1224.

[0103] Local storage 1222, 1224 may include volatile storage media (e.g., conventional DRAM, SRAM, SDRAM, or the like) and/or non-volatile storage media (e.g., magnetic or optical disk, flash memory, or the like). Storage media incorporated in local storage 1222, 1224 may be fixed, removable or upgradeable as desired. Local storage 1222, 1224 may be physically or logically divided into various subunits such as a system memory, a ROM, and a permanent storage device. The system memory may be a read-and-write memory device or a volatile read-and-write memory, such as dynamic random access memory. The system memory may store some or all of the instructions and data that processing unit(s) 1212, 1214 need at runtime. The ROM may store static data and instructions that are needed by processing unit(s) 1212, 1214. The permanent storage device may be a non-volatile read-and-write memory device that may store instructions and data even when a module including one or more processing units 1212, 1214 and local storage 1222, 1224 is powered down. The term “storage medium” as used herein includes any medium in which data may be stored indefinitely (subject to overwriting, electrical disturbance, power loss, or the like) and does not include carrier waves and transitory electronic signals propagating wirelessly or over wired connections.

[0104] In some embodiments, local storage 1222, 1224 may store one or more software programs to be executed by processing unit(s) 1212, 1214, such as an operating system and/or programs implementing various server functions such as functions of UPP system 102, or any other server(s) associated with UPP system 102. “Software” refers generally to sequences of instructions that, when executed by processing unit(s) 1212, 1214 cause computing system 1202 (or portions thereof) to perform various operations, thus defining one or more specific machine implementations that execute and perform the operations of the software programs. The instructions may be stored as firmware residing in read-only memory and/or program code stored in non-volatile storage media that may be read into volatile working memory for execution by processing unit(s) 1212, 1214. In some embodiments the instructions may be stored by storage subsystem 1268 (e.g., computer readable storage media). In various embodiments, the processing units may execute a variety of programs or code instructions and may maintain multiple concurrently executing programs or processes. At any given time, some or all of the program code to be executed may be resident in local storage 1222, 1224 and/or in storage subsystem including potentially on one or more storage devices. Software may be implemented as a single program or a collection of separate programs or program modules that interact as desired. From local storage 1222, 1224 (or

non-local storage described below), processing unit(s) 1212, 1214 may retrieve program instructions to execute and data to process in order to execute various operations described above.

[0105] Storage subsystem 1268 provides a repository or data store for storing information that is used by computing system 1202. Storage subsystem 1268 provides a tangible non-transitory computer-readable storage medium for storing the basic programming and data constructs that provide the functionality of some embodiments. Software (programs, code modules, instructions) that when executed by processing subsystem 1210 provide the functionality described above may be stored in storage subsystem 1268. The software may be executed by one or more processing units of processing subsystem 1210. Storage subsystem 1268 may also provide a repository for storing data used in accordance with the present invention.

[0106] Storage subsystem 1268 may include one or more non-transitory memory devices, including volatile and non-volatile memory devices. As shown in FIG. 12, storage subsystem 1268 includes a system memory 1260 and a computer-readable storage media 1252. System memory 1260 may include a number of memories including a volatile main RAM for storage of instructions and data during program execution and a non-volatile ROM or flash memory in which fixed instructions are stored. In some implementations, a basic input/output system (BIOS), containing the basic routines that help to transfer information between elements within computing system 1202, such as during start-up, may typically be stored in the ROM. The RAM typically contains data and/or program modules that are presently being operated and executed by processing subsystem 1210. In some implementations, system memory 1260 may include multiple different types of memory, such as static random access memory (SRAM) or dynamic random access memory (DRAM). Storage subsystem 1268 may be based on magnetic, optical, semiconductor, or other data storage media. Direct attached storage, storage area networks, network-attached storage, and the like may be used. Any data stores or other collections of data described herein as being produced, consumed, or maintained by a service or server may be stored in storage subsystem 1268.

[0107] By way of example, and not limitation, as depicted in FIG. 12, system memory 1260 may store application programs 1262, which may include client applications, Web browsers, mid-tier applications, relational database management systems (RDBMS), etc., program data 1264, and one or more operating systems 1266. By way of example, an

example operating systems may include various versions of Microsoft Windows®, Apple Macintosh®, and/or Linux operating systems, a variety of commercially-available UNIX® or UNIX-like operating systems (including without limitation the variety of GNU/Linux operating systems, the Google Chrome® OS, and the like) and/or mobile operating systems such as iOS, Windows® Phone, Android® OS, BlackBerry® 10 OS, and Palm® OS operating systems.

[0108] Computer-readable storage media 1252 may store programming and data constructs that provide the functionality of some embodiments. Software (programs, code modules, instructions) that when executed by processing subsystem 1210 a processor provide the functionality described above may be stored in storage subsystem 1268. By way of example, computer-readable storage media 1252 may include non-volatile memory such as a hard disk drive, a magnetic disk drive, an optical disk drive such as a CD ROM, DVD, a Blu-Ray® disk, or other optical media. Computer-readable storage media 1252 may include, but is not limited to, Zip® drives, flash memory cards, universal serial bus (USB) flash drives, secure digital (SD) cards, DVD disks, digital video tape, and the like. Computer-readable storage media 1252 may also include, solid-state drives (SSD) based on non-volatile memory such as flash-memory based SSDs, enterprise flash drives, solid state ROM, and the like, SSDs based on volatile memory such as solid state RAM, dynamic RAM, static RAM, DRAM-based SSDs, magnetoresistive RAM (MRAM) SSDs, and hybrid SSDs that use a combination of DRAM and flash memory based SSDs. Computer-readable media 1252 may provide storage of computer-readable instructions, data structures, program modules, and other data for computing system 1202.

[0109] In certain embodiments, storage subsystem 1268 may also include a computer-readable storage media reader 1250 that may further be connected to computer-readable storage media 1252. Together and, optionally, in combination with system memory 1260, computer-readable storage media 1252 may comprehensively represent remote, local, fixed, and/or removable storage devices plus storage media for storing computer-readable information.

[0110] In certain embodiments, computing system 1202 may provide support for executing one or more virtual machines. Computing system 1202 may execute a program such as a hypervisor for facilitating the configuring and managing of the virtual machines. Each virtual machine may be allocated memory, compute (e.g., processors, cores), I/O, and networking

resources. Each virtual machine typically runs its own operating system, which may be the same as or different from the operating systems executed by other virtual machines executed by computing system 1202. Accordingly, multiple operating systems may potentially be run concurrently by computing system 1202. Each virtual machine generally runs independently of the other virtual machines.

[0111] Communication subsystem 1240 provides an interface to other computer systems and networks. Communication subsystem 1240 serves as an interface for receiving data from and transmitting data to other systems from computing system 1202. For example, communication subsystem 1240 may enable computing system 1202 to establish a communication channel to one or more client computing devices via the Internet for receiving and sending information from and to the client computing devices.

[0112] Communication subsystem 1240 may support both wired and/or wireless communication protocols. For example, in certain embodiments, communication subsystem 1240 may include radio frequency (RF) transceiver components for accessing wireless voice and/or data networks (e.g., using cellular telephone technology, advanced data network technology, such as 3G, 4G or EDGE (enhanced data rates for global evolution), WiFi (IEEE 802.11 family standards, or other mobile communication technologies, or any combination thereof), global positioning system (GPS) receiver components, and/or other components. In some embodiments communication subsystem 1240 may provide wired network connectivity (e.g., Ethernet) in addition to or instead of a wireless interface.

[0113] Communication subsystem 1240 may receive and transmit data in various forms. For example, in some embodiments, communication subsystem 1240 may receive input communication in the form of structured and/or unstructured data feeds, event streams, event updates, and the like. For example, communication subsystem 1240 may be configured to receive (or send) data feeds in real-time from users of social media networks and/or other communication services such as Twitter® feeds, Facebook® updates, web feeds such as Rich Site Summary (RSS) feeds, and/or real-time updates from one or more third party information sources.

[0114] In certain embodiments, communication subsystem 1240 may be configured to receive data in the form of continuous data streams, which may include event streams of real-time events and/or event updates, that may be continuous or unbounded in nature with no explicit end. Examples of applications that generate continuous data may include, for

example, sensor data applications, financial tickers, network performance measuring tools (e.g. network monitoring and traffic management applications), clickstream analysis tools, automobile traffic monitoring, and the like.

[0115] Communication subsystem 1240 may also be configured to output the structured and/or unstructured data feeds, event streams, event updates, and the like to one or more databases that may be in communication with one or more streaming data source computers coupled to computing system 1202.

[0116] Communication subsystem 1240 may provide a communication interface 1242, e.g., a WAN interface, which may provide data communication capability between the local area network (bus subsystem 1270) and a larger network, such as the Internet. Conventional or other communications technologies may be used, including wired (e.g., Ethernet, IEEE 802.3 standards) and/or wireless technologies (e.g., Wi-Fi, IEEE 802.11 standards).

[0117] Computing system 1202 may operate in response to requests received via communication interface 1242. Further, in some embodiments, communication interface 1242 may connect computing systems 1202 to each other, providing scalable systems capable of managing high volumes of activity. Conventional or other techniques for managing server systems and server farms (collections of server systems that cooperate) may be used, including dynamic resource allocation and reallocation.

[0118] Computing system 1202 may interact with various user-owned or user-operated devices via a wide-area network such as the Internet. An example of a user-operated device is shown in FIG. 12 as client computing system 1204. Client computing system 1204 may be implemented, for example, as a consumer device such as a smart phone, other mobile phone, tablet computer, wearable computing device (e.g., smart watch, eyeglasses), desktop computer, laptop computer, and so on.

[0119] For example, client computing system 1204 may communicate with computing system 1202 via communication interface 1242. Client computing system 1204 may include conventional computer components such as processing unit(s) 1282, storage device 1284, network interface 1280, user input device 1286, and user output device 1288. Client computing system 1204 may be a computing device implemented in a variety of form factors, such as a desktop computer, laptop computer, tablet computer, smart phone, other mobile computing device, wearable computing device, or the like.

[0120] Processing unit(s) 1282 and storage device 1284 may be similar to processing unit(s) 1212, 1214 and local storage 1222, 1224 described above. Suitable devices may be selected based on the demands to be placed on client computing system 1204; for example, client computing system 1204 may be implemented as a “thin” client with limited processing capability or as a high-powered computing device. Client computing system 1204 may be provisioned with program code executable by processing unit(s) 1282 to enable various interactions with computing system 1202 of a message management service such as accessing messages, performing actions on messages, and other interactions described above. Some client computing systems 1204 may also interact with a messaging service independently of the message management service.

[0121] Network interface 1280 may provide a connection to a wide area network (e.g., the Internet) to which communication interface 1240 of computing system 1202 is also connected. In various embodiments, network interface 1280 may include a wired interface (e.g., Ethernet) and/or a wireless interface implementing various RF data communication standards such as Wi-Fi, Bluetooth®, or cellular data network standards (e.g., 3G, 4G, LTE, etc.).

[0122] User input device 1286 may include any device (or devices) via which a user may provide signals to client computing system 1204; client computing system 1204 may interpret the signals as indicative of particular user requests or information. In various embodiments, user input device 1286 may include any or all of a keyboard, touch pad, touch screen, mouse or other pointing device, scroll wheel, click wheel, dial, button, switch, keypad, microphone, and so on.

[0123] User output device 1288 may include any device via which client computing system 1204 may provide information to a user. For example, user output device 1288 may include a display to display images generated by or delivered to client computing system 1204. The display may incorporate various image generation technologies, e.g., a liquid crystal display (LCD), light-emitting diode (LED) including organic light-emitting diodes (OLED), projection system, cathode ray tube (CRT), or the like, together with supporting electronics (e.g., digital-to-analog or analog-to-digital converters, signal processors, or the like). Some embodiments may include a device such as a touchscreen that function as both input and output device. In some embodiments, other user output devices 1288 may be provided in

addition to or instead of a display. Examples include indicator lights, speakers, tactile “display” devices, printers, and so on.

[0124] Some embodiments include electronic components, such as microprocessors, storage and memory that store computer program instructions in a computer readable storage medium. Many of the features described in this specification may be implemented as processes that are specified as a set of program instructions encoded on a computer readable storage medium. When these program instructions are executed by one or more processing units, they cause the processing unit(s) to perform various operation indicated in the program instructions. Examples of program instructions or computer code include machine code, such as is produced by a compiler, and files including higher-level code that are executed by a computer, an electronic component, or a microprocessor using an interpreter. Through suitable programming, processing unit(s) 1212, 1214 and 1282 may provide various functionality for computing system 1202 and client computing system 1204, including any of the functionality described herein as being performed by a server or client, or other functionality associated with message management services.

[0125] It will be appreciated that computing system 1202 and client computing system 1204 are illustrative and that variations and modifications are possible. Computer systems used in connection with embodiments of the present invention may have other capabilities not specifically described here. Further, while computing system 1202 and client computing system 1204 are described with reference to particular blocks, it is to be understood that these blocks are defined for convenience of description and are not intended to imply a particular physical arrangement of component parts. For instance, different blocks may be but need not be located in the same facility, in the same server rack, or on the same motherboard. Further, the blocks need not correspond to physically distinct components. Blocks may be configured to perform various operations, e.g., by programming a processor or providing appropriate control circuitry, and various blocks might or might not be reconfigurable depending on how the initial configuration is obtained. Embodiments of the present invention may be realized in a variety of apparatus including electronic devices implemented using any combination of circuitry and software.

[0126] While the invention has been described with respect to specific embodiments, one skilled in the art will recognize that numerous modifications are possible. Embodiments of

the invention may be realized using a variety of computer systems and communication technologies including but not limited to specific examples described herein.

[0127] Embodiments of the present invention may be realized using any combination of dedicated components and/or programmable processors and/or other programmable devices.

5 The various processes described herein may be implemented on the same processor or different processors in any combination. Where components are described as being configured to perform certain operations, such configuration may be accomplished, e.g., by designing electronic circuits to perform the operation, by programming programmable electronic circuits (such as microprocessors) to perform the operation, or any combination thereof. Further, while the embodiments described above may make reference to specific hardware and software components, those skilled in the art will appreciate that different combinations of hardware and/or software components may also be used and that particular operations described as being implemented in hardware might also be implemented in software or vice versa.

15 **[0128]** Computer programs incorporating various features of the present invention may be encoded and stored on various computer readable storage media; suitable media include magnetic disk or tape, optical storage media such as compact disk (CD) or DVD (digital versatile disk), flash memory, and other non-transitory media. Computer readable media encoded with the program code may be packaged with a compatible electronic device, or the
20 program code may be provided separately from electronic devices (e.g., via Internet download or as a separately packaged computer-readable storage medium).

[0129] Thus, although the invention has been described with respect to specific embodiments, it will be appreciated that the invention is intended to cover all modifications and equivalents within the scope of the following claims.

25 **[0130]** While certain exemplary embodiments have been described in detail and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not intended to be restrictive of the broad invention, and that this invention is not to be limited to the specific arrangements and constructions shown and described, since various other modifications may occur to those with ordinary skill in the art.

30 **[0131]** Other variations are within the spirit of the present disclosure. Thus, while the disclosed techniques are susceptible to various modifications and alternative constructions,

certain illustrated embodiments thereof are shown in the drawings and have been described above in detail. It should be understood, however, that there is no intention to limit the disclosure to the specific form or forms disclosed, but on the contrary, the intention is to cover all modifications, alternative constructions and equivalents falling within the spirit and scope of the disclosure, as defined in the appended claims.

[0132] The use of the terms “a” and “an” and “the” and similar referents in the context of describing the disclosed embodiments (especially in the context of the following claims) are to be construed to cover both the singular and the plural, unless otherwise indicated herein or clearly contradicted by context. The terms “comprising,” “having,” “including,” and “containing” are to be construed as open-ended terms (i.e., meaning “including, but not limited to,”) unless otherwise noted. The term “connected” is to be construed as partly or wholly contained within, attached to, or joined together, even if there is something intervening. The phrase “based on” should be understood to be open-ended, and not limiting in any way, and is intended to be interpreted or otherwise read as “based at least in part on,” where appropriate. Recitation of ranges of values herein are merely intended to serve as a shorthand method of referring individually to each separate value falling within the range, unless otherwise indicated herein, and each separate value is incorporated into the specification as if it were individually recited herein. All methods described herein can be performed in any suitable order unless otherwise indicated herein or otherwise clearly contradicted by context. The use of any and all examples, or exemplary language (e.g., “such as”) provided herein, is intended merely to better illuminate embodiments of the disclosure and does not pose a limitation on the scope of the disclosure unless otherwise claimed. No language in the specification should be construed as indicating any non-claimed element as essential to the practice of the disclosure.

WHAT IS CLAIMED IS:

1 1. A computer-implemented method comprising:
2 receiving, by a processor, dosage data corresponding to a medication dosage
3 regimen for a medication prescribed to a patient;
4 receiving, by the processor from a remote mobile device, one or more video
5 data files including video of the patient administering the medication at intervals defined by
6 the medication dosage regimen;
7 receiving a request from a medical provider to access the one or more video
8 data files;
9 providing the medical provider access to the one or more video data files;
10 receiving approval data corresponding to the medical provider's acceptance or
11 rejection of the one or more video data files as proof of the patient taking a correct dosage of
12 the medication as defined in the medication dosage regimen;
13 calculating a medication regimen adherence value based on the medication
14 dosage regimen and the approval data; and
15 wherein the medical provider is able to review multiple video data files at a
16 time, thus requiring fewer interactions than physical Direct Observed Therapy.

1 2. The method of claim 1 wherein the calculating a medication regimen
2 adherence value is performed by a system program separate from a medical provider program
3 on a medical provider device.

1 3. The method of claim 1 wherein the video data files each include a time
2 and date stamp of a time and date of recording.

1 4. The method of claim 1 further comprising:
2 modifying a medical provider intervention intensity based on the medication
3 regimen adherence value, wherein the intervention intensity comprises an amount of time
4 after receipt of the patient video at the secure patient database for the medical provider to
5 review the patient video.

1 5. The method of claim 4 wherein modifying a medical provider
2 intervention intensity based on the medication regimen adherence value comprises advancing

the patient to a subsequent monitoring stage, wherein a final monitoring stage requires a lesser intensity of intervention.

6. The method of claim 5 wherein a first stage comprises:
indicating successful downloading of the patient program,
verifying a patient password,
capturing a patient test video,
encrypting the patient test video,
establishing a secure connection over the network to the secure patient
database, and
uploading an encrypted patient test video to the secure patient
database.

7. The method of claim 5 wherein a first stage comprises
receiving a medical provider input verifying an adherence by the
patient to the medication dosage regimen for a predetermined number of dosages, and
indicating an advancement of the patient to a subsequent stage.

8. The method of claim 5 wherein the operations include advancing a
patient through multiple stages requiring high, medium and low values of medical provider
intervention intensity.

9. The method of claim 1 further comprising:
encrypting the video data file,
establishing a secure connection over a network to a secure patient
database,

uploading an encrypted video data file to the secure patient database.

10. A system for securing medication adherence remotely over a network
in communication with a patient computing device and a medical provider computing device,
comprising:

at least one secure patient database storing
encrypted patient profiles including medication descriptions,
medication dosages, and dosage regimens,
encrypted patient videos of patients taking medications;

8 a patient program non-transitory computer-readable storage medium
9 containing instructions configured to cause a processor in the patient computing
10 device to perform operations including
11 verifying a patient password,
12 capturing a patient video showing the patient taking a medication,
13 encrypting the patient video,
14 establishing a secure connection over the network to the secure patient
15 database,
16 uploading an encrypted patient video to the secure patient database;
17 a medical provider program non-transitory computer-readable storage medium
18 containing instructions configured to cause a processor in the medical provider
19 computing device to perform operations including
20 verifying a medical provider password,
21 establishing a secure connection over the network to the secure patient
22 database,
23 displaying information relating to multiple patients in a triaged order,
24 accessing an encrypted patient video in the secure patient database in
25 response to a selection by a medical provider,
26 decrypting the encrypted patient video,
27 receiving approval data corresponding to the medical provider's
28 acceptance or rejection of the one or more video data files as proof of the patient
29 taking a correct dosage of the medication as defined in a medication dosage regimen;
30 a system program non-transitory computer-readable storage medium
31 containing instructions configured to cause a processor to perform operations
32 including
33 calculating a medication regimen adherence value based on the
34 medication dosage regimen and the approval data; and
35 modifying a medical provider intervention intensity based on the
36 medication regimen adherence value.

1 11. The system of claim 10 wherein the system program non-transitory
2 computer-readable storage medium is part of the medical provider program non-transitory
3 computer-readable storage medium.

1 12. The system of claim 10 wherein the patient videos each include a time
2 and date stamp of a time and date of recording.

1 13. The system of claim 10 wherein the intervention intensity comprises an
2 amount of time after receipt of the patient video at the secure patient database for the medical
3 provider to review the patient video.

1 14. The system of claim 10 wherein modifying a medical provider
2 intervention intensity based on the medication regimen adherence value comprises advancing
3 the patient to a subsequent monitoring stage, wherein a final monitoring stage requires a
4 lesser intensity of intervention.

1 15. The system of claim 14 wherein a first stage comprises instructions in
2 the patient program non-transitory computer-readable storage medium configured to
3 cause the processor in the patient computing device to perform operations including
4 indicating successful downloading of the patient program,
5 verifying a patient password,
6 capturing a patient test video,
7 encrypting the patient test video,
8 establishing a secure connection over the network to the secure patient
9 database,
10 uploading an encrypted patient test video to the secure patient database.

1 16. The system of claim 14 wherein a first stage comprises instructions in
2 the medical provider program non-transitory computer-readable storage medium
3 configured to cause the processor in the medical provider computing device to
4 perform operations including
5 receiving a medical provider input verifying an adherence by the
6 patient to the medication dosage regimen for a predetermined number of dosages,
7 indicating an advancement of the patient to a subsequent stage.

1 17. The system of claim 14 wherein the operations include advancing a
2 patient through multiple stages requiring high, medium and low values of medical provider
3 intervention intensity.

1 18. The system of claim 10 wherein the network comprises the internet
2 and the secure connection over the network comprises an SSL tunnel.

1 19. A system for securing medication adherence remotely over a network
2 in communication with a patient computing device and a medical provider computing device,
3 comprising:

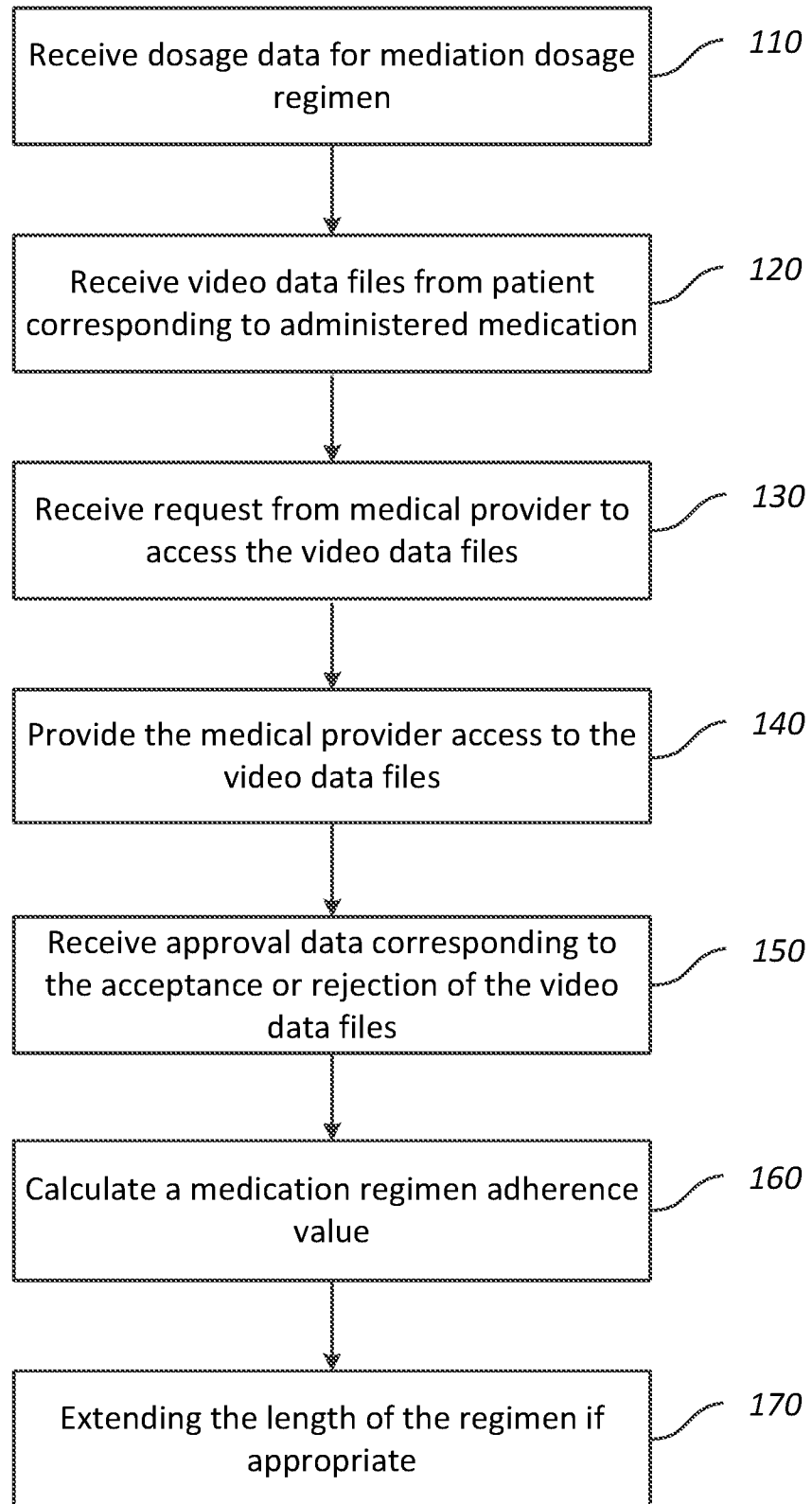
4 at least one secure patient database storing
5 encrypted patient profiles including medication descriptions,
6 medication dosages, and dosage regimens,
7 encrypted patient videos of patients taking medications;
8 a patient program non-transitory computer-readable storage medium
9 containing instructions configured to cause a processor in the patient computing
10 device to perform operations including
11 verifying a patient password,
12 capturing a patient video showing the patient taking a medication,
13 wherein the patient video includes a time stamp of a time of recording,
14 encrypting the patient video,
15 establishing a secure an SSL tunnel connection over the network to the
16 secure patient database,
17 uploading an encrypted patient video to the secure patient database;
18 a medical provider program non-transitory computer-readable storage medium
19 containing instructions configured to cause a processor in the medical provider
20 computing device to perform operations including
21 verifying a medical provider password,
22 establishing a secure an SSL tunnel connection over the network to the
23 secure patient database,
24 displaying information relating to multiple patients in a triaged order,
25 accessing an encrypted patient video in the secure patient database in
26 response to a selection by a medical provider,
27 decrypting the encrypted patient video,
28 receiving approval data corresponding to the medical provider's
29 acceptance or rejection of the one or more video data files as proof of the patient
30 taking a correct dosage of the medication as defined in a medication dosage regimen;

31 a system program non-transitory computer-readable storage medium
32 containing instructions configured to cause a processor to perform operations
33 including
34 calculating a medication regimen adherence value based on the
35 medication dosage regimen and the approval data; and
36 modifying a medical provider intervention intensity based on the medication
37 regimen adherence value, wherein the intervention intensity comprises an amount of
38 time after receipt of the patient video at the secure patient database for the medical
39 provider to review the patient video, wherein the modifying comprises advancing the
40 patient to a subsequent monitoring stage, wherein a final monitoring stage modifies
41 the intensity of intervention,
42 wherein a first stage comprises instructions in the patient program non-
43 transitory computer-readable storage medium configured to cause the processor in the
44 patient computing device to perform operations including
45 indicating successful downloading of the patient program,
46 verifying a patient password,
47 capturing a patient test video,
48 encrypting the patient test video,
49 establishing a secure connection over the network to the secure patient
50 database,
51 uploading an encrypted patient test video to the secure patient
52 database.

1 20. The system of claim 19 wherein the network comprises the
2 internet.

1

1

**FIG. 1**

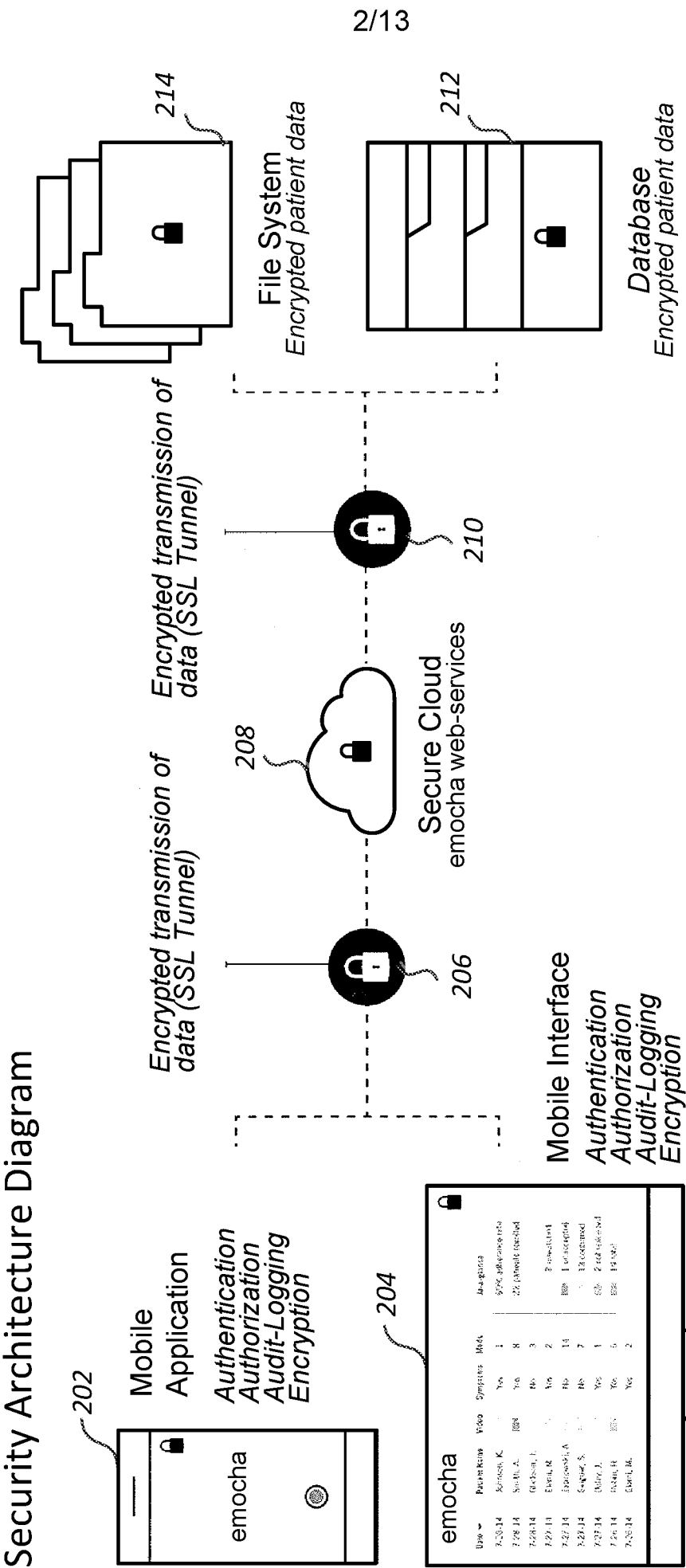
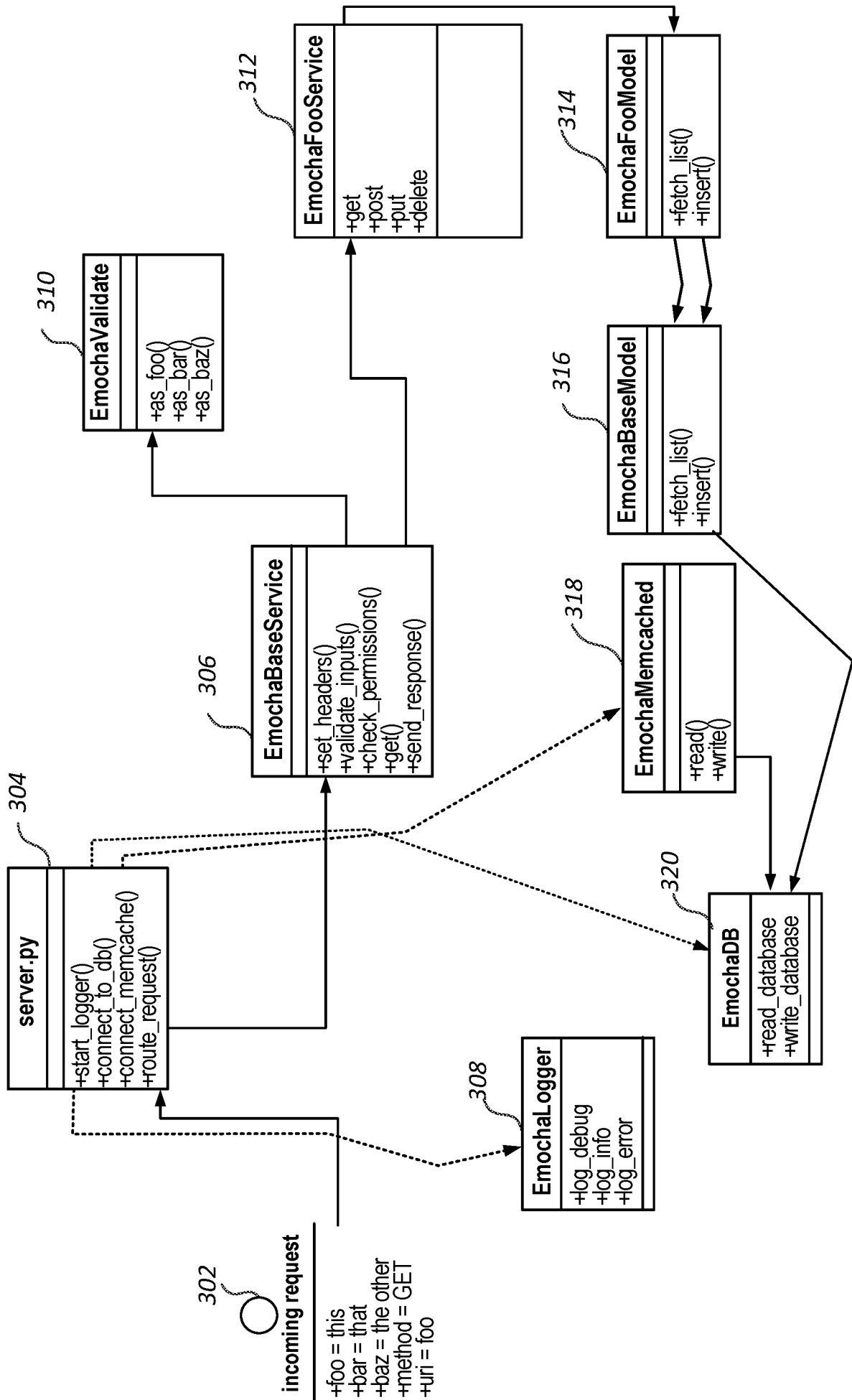


FIG. 2



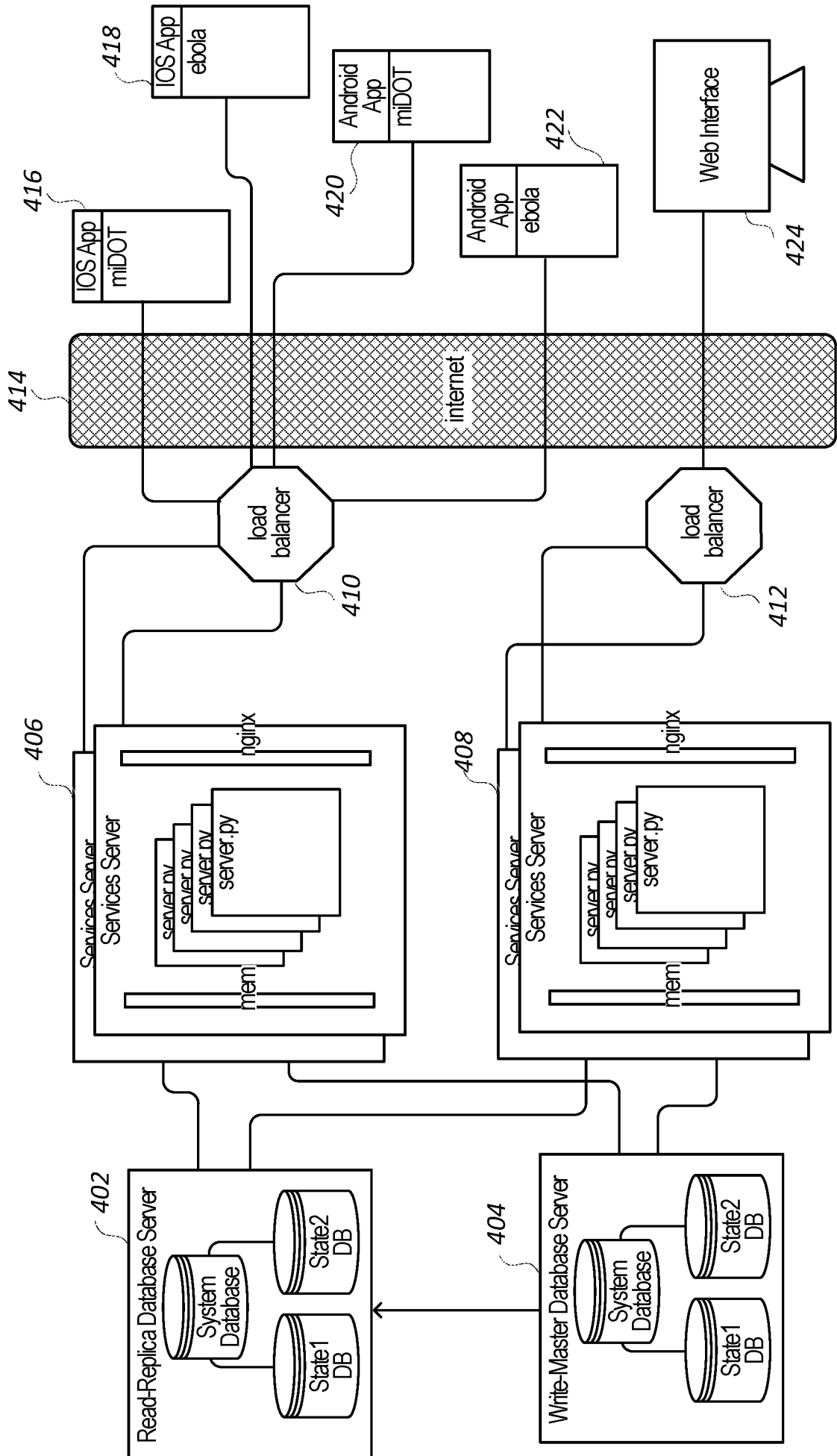


FIG. 4



<u>Intervention Intensity</u>	<u>Intervention Requirements for Healthcare worker (User)</u>	<u>Special Requirements for 1x per week Regimens</u>
High Intensity	Review and assessment of videos within 4 business hours Phone call to patient at video miss or ANY non-compliance with procedure Congratulatory call/message at 100% compliance of stage	Review and assessment of videos within 6 business hours Phone call to patient at video miss or ANY non-compliance with procedure Congratulatory call/message at 100% compliance of stage Reminder call/message to patient at T-1 and T+1
Medium intensity	Review of videos within 24 hours Phone call to patient at video miss or any CRITICAL non-compliance with procedure Congratulatory call/message at 100% compliance of stage	Review of videos within 24 hours Phone call to patient at T+1 Congratulatory call/message at 100% compliance of stage
Low intensity	Review of videos within 48 hours Phone call to patient at video miss or any CRITICAL non-compliance with procedure Congratulatory call/message at weeks with 100% compliance	Low intensity not possible given impact of a miss
<u>Compliance Criteria</u>	<u>General Process</u> Patient identifies self Patient states the date Patient states medication pill-by-pill Patient shows medication in mouth Patient drinks water after each pill	<u>Critical non-compliance</u> Patient does not take medication Patient does not appear to take medication Patient not identifiable Video cut short before process complete
<u>Regimens</u>	Daily Regimen is 5 or 7 days per week 3x weekly is M-W-F 1x weekly is once a week with a specified Target day Target -1 is the day before the target Target +1 is the day after the target	
<u>Stages</u>	App Download Onboarding Stage Habit Building Stage Performance Stage Autopilot	

FIG. 5

Protocol for 5-day or 7-day regimen

Stage	App Download	Onboarding	Habit Building	Performance	Autopilot
Duration	1	2	5	5	NA
Dose	Test Video	1 2	3 4 5 6 7	8 9 10 11 12	Dose 13 onwards
Adherence Requirement	100%	100%	need 80%	need 80%	90%
Intervention Intensity	High	High	High	Medium	Low
Escalation				revert to high upon 2 failures	revert to medium at any failure: revert to high after 2 failures in any calendar week
Stage Repetition	prerequisite to use app	2x max	Repeat upon 2+ misses (2x max)		

FIG. 6

Protocol for 3-day regimen

Stage	App Download	Onboarding	Habit Building	Performance	Autopilot
Duration	1	3	3	6	NA
Dose	Test	1 2 3	4 5 6	7 8 9 10 11 12	Dose 13 onwards
Adherence Requirement		need 2/3	need 100%	need 100%	90%
Intervention Intensity		High	High	Medium	Low
Escalation				revert to High upon 2 failures	revert to Medium at any failure: revert to High after 2 failures in any calendar week
Stage Repetition			Repeat upon 1+ miss. Max 3 repeats	Repeat upon 2+ misses	

FIG. 7

Protocol for 1-day regimen

Stage	App Download	Onboarding	Habit Building	Performance	Autopilot											
Duration	1	1	2	2	6											
Dose	Test	1	1 2	3 4	6	7	8	9	10	11	12	Dose 13 onwards				
Adherence Requirement			need 100%		need 100%											
Intervention Intensity			High	High	Medium											
Escalation				Progress to next stage at “High” if one of these two doses is missed, progress to “medium” next stage if this stage is completed with 100% of doses	revert to High after 1 miss											
Stage Repetition			Repeat upon 1+ miss	No repetitions												

FIG. 8

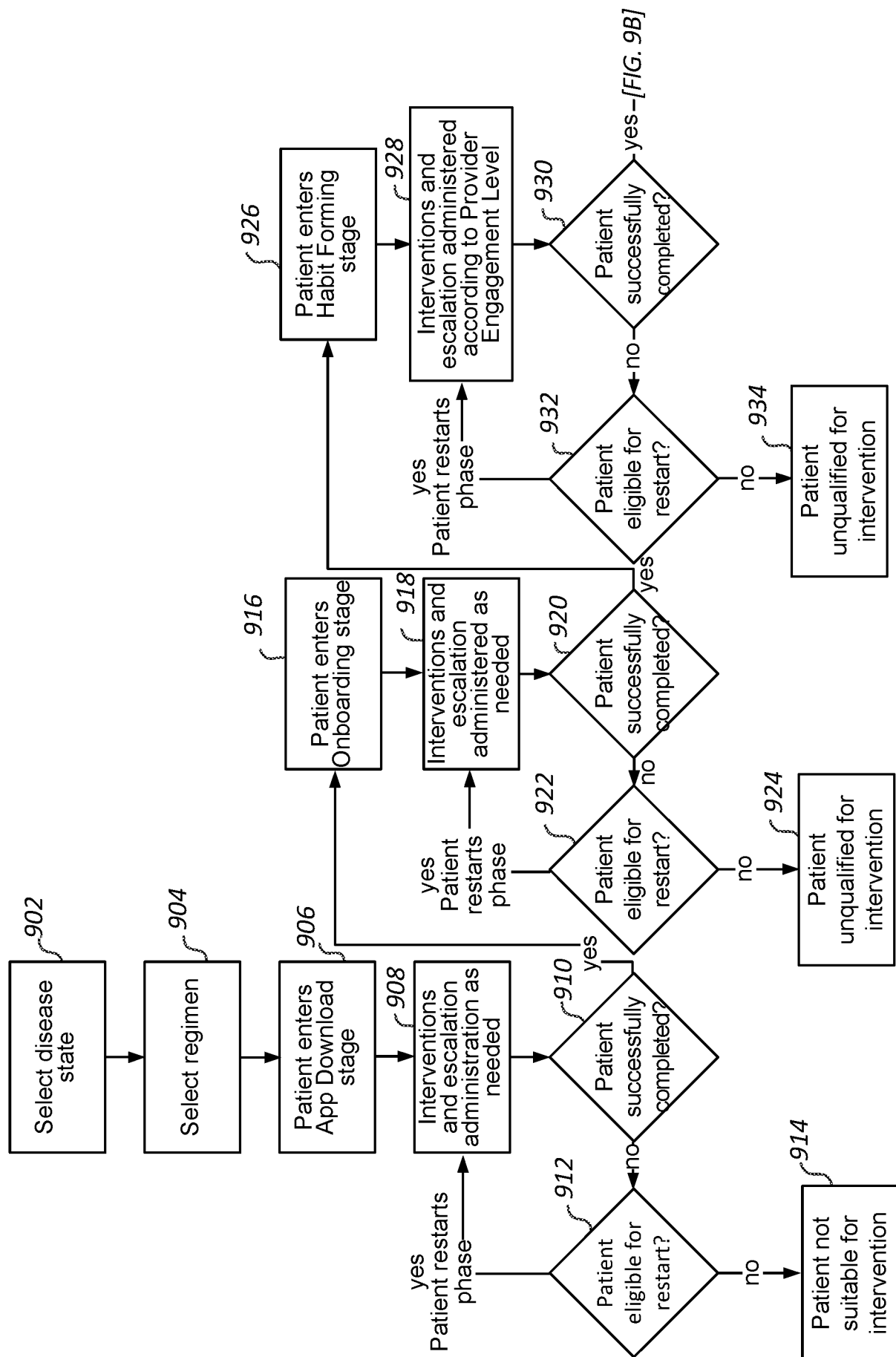


FIG. 9A

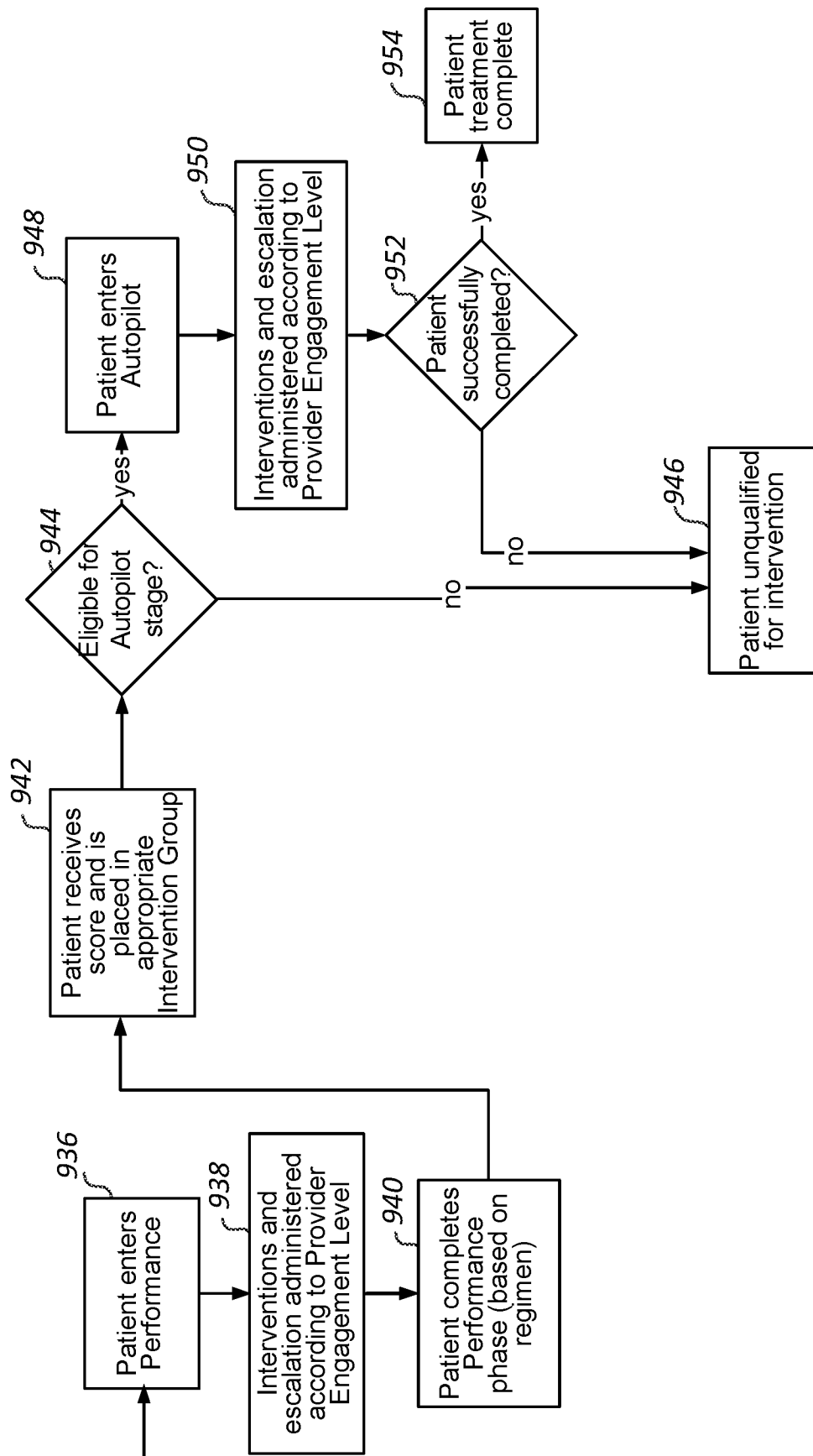


FIG. 9B

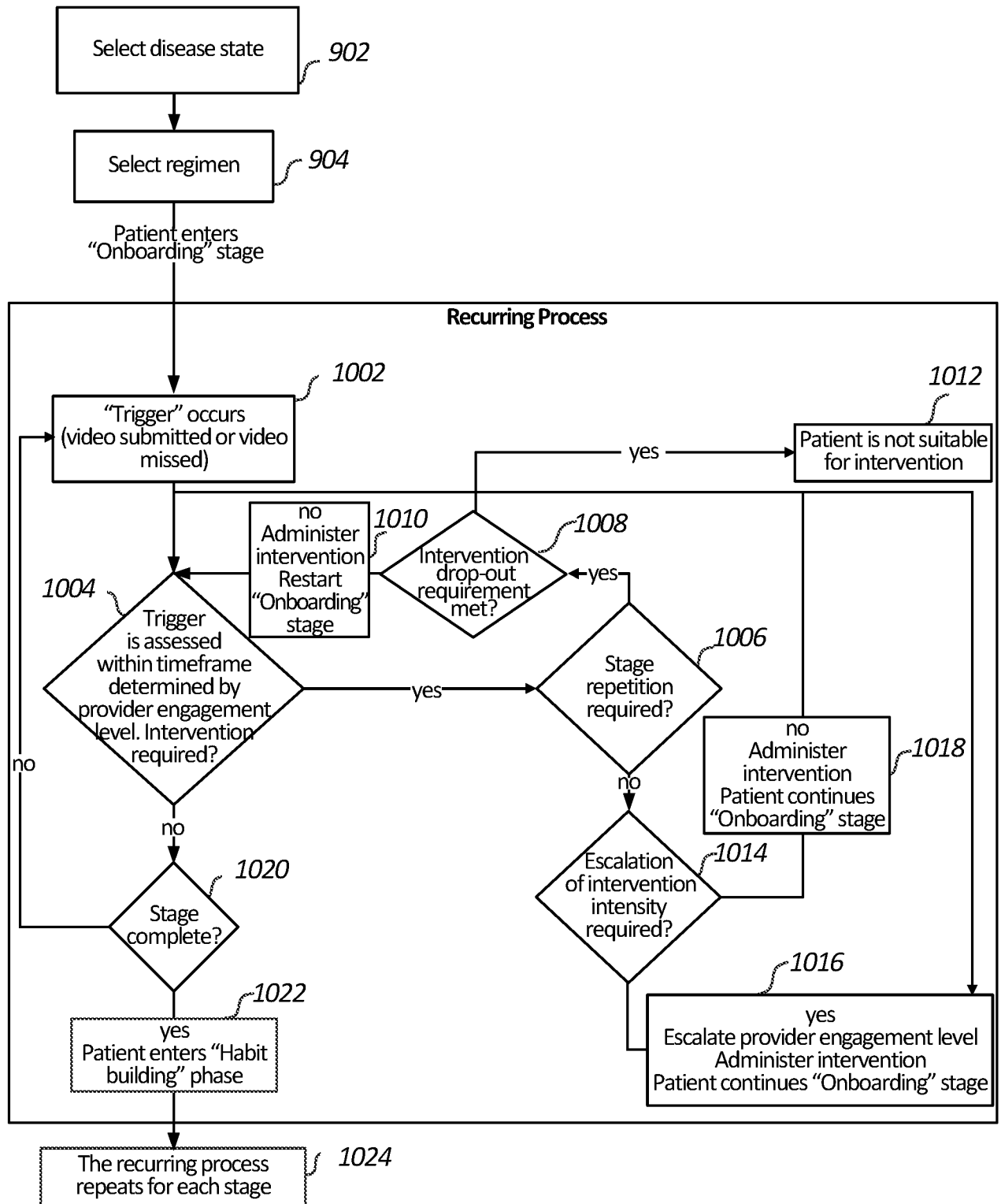


FIG. 10

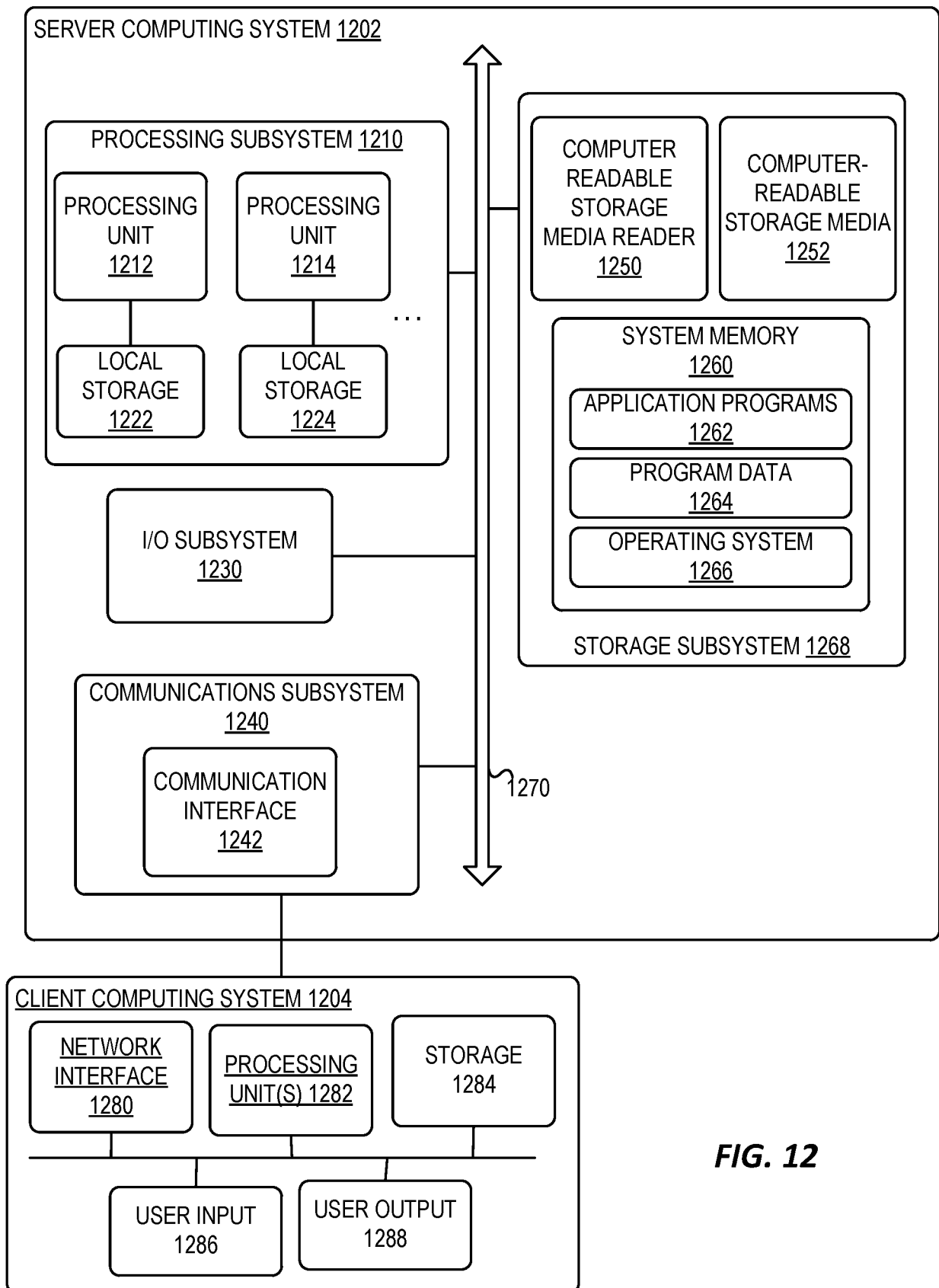


1102

NEED REVIEW			
Bamburg, Laura July 12 <u>1104</u> ...	Chiasson, Greg July 12 ...	Daniel, Rob July 12 ...	Elliot, Sean July 12 <u>1106</u> ...
Bamburg, Laura July 12 ...	Chiasson, Greg July 12 <u>1110</u> ...	Daniels, Rob July 12 <u>1108</u> ...	Elliot, Sean July 12 ...
Bamburg, Laura July 12 <u>1112</u> ...	Chiasson, Greg July 12 ...	Daniels, Rob July 12 ...	Elliot, Sean July 12 <u>1114</u> ...

FIG. 11



**FIG. 12**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 17/26851

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06Q 40/00 (2017.01)

CPC - G06Q 50/24, G06Q 50/22, G06F 19/322, G06Q 40/08, G06Q 10/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

See Search History Document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

See Search History Document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

See Search History Document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014/0055589 A1 (Bangera et al.) 27 February 2014 (27.02.2014) entire document (especially Abstract, para [0126], para [0130]-[0132], para [0138], para [0153], para [0192], para [0198])	1-20
Y	US 2012/0316897 A1 (Hanina et al.) 13 December 2012 (13.12.2012) entire document (especially para [0016], para [0038]-[0039], para [0046], para [0054])	1-20
Y	US 2011/0275051 A1 (Hanina et al.) 10 November 2011 (10.11.2011) entire document (especially para [0028], para [0041])	6, 9
Y	US 2015/0281949 A1 (Laborde) 01 October 2015 (01.10.2015) entire document (especially para [0030], para [0078]-[0080], cl. 31, cl. 35)	10-20
Y	US 2012/0041788 A1 (Wons et al.) 16 February 2012 (16.02.2012) entire document (especially para [0037])	18-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

23 June 2017 (23.06.2017)

Date of mailing of the international search report

17 JUL 2017

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-8300

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774