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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 October 2021 (21.10.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/211375 A1

(51) International Patent Classification:
G06Q 10/00 (2012.01) *G06Q 50/00* (2012.01)
G06Q 10/06 (2012.01) *G16H 10/60* (2018.01)

(21) International Application Number:
PCT/US2021/026580

(22) International Filing Date:
09 April 2021 (09.04.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/009,133 13 April 2020 (13.04.2020) US

(72) Inventors; and
(71) Applicants: **RAJAGOPAL, Dhiren** [US/US]; 1252 Swims Valley Drive, Atlanta, Georgia 30327 (US). **RAJAGOPAL, Deven** [US/US]; 1252 Swims Valley Drive, Atlanta, Georgia 30327 (US).

(74) Agent: **MUELLER, Craig**; 10162 E. 29th Ave., Denver, Colorado 80238 (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, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

(54) Title: SYSTEMS AND METHODS FOR VERIFYING PATIENT IMMUNITY

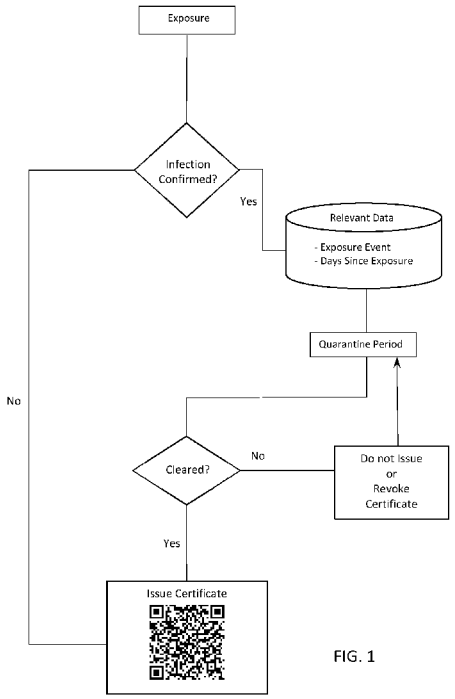


FIG. 1

(57) Abstract: A system and method for verifying a patient's immunity to a predetermined pathogen are provided. The contemplated system relies on at least one of patient-specific and exposure data, which could include immunization or vaccination data, to assess the patient's immunity to a predetermined pathogen. If immunity is verified, the patient is selectively issued a digital certificate real-time and/or on-demand used to allow access to a building, gain authorization to conduct predetermined activities, work, travel freely, etc. The immunity certificate may be renewed or revoked if predetermined events occur, such as a rise in body temperature over a predetermined level.

WO 2021/211375 A1

[Continued on next page]

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

SYSTEMS AND METHODS FOR VERIFYING PATIENT IMMUNITY

[0001] This application claims the benefit of U.S. Provisional Patent Application Serial No. 63/009,133, filed April 13, 2020, the entirety of which is incorporated by reference herein.

FIELD OF THE INVENTION

[0002] Embodiments of the present invention are generally related to providing a selectively accessible database that allows patients, doctors, or third parties to access predetermined medical records. In one embodiment, access to medical records is used to verify a user, e.g., a patient, has immunity to one or more pathogens.

BACKGROUND OF THE INVENTION

[0003] Coronaviruses are well-known and are endemic in humans and animals. Most coronaviruses, such as those that cause the common cold, are minor, but some strains can cause severe illness. In particular, SARS-Co-V caused the SARS pandemic in 2003, and in 2019 a new strain of the coronavirus (SARS-CoV-2) was identified and quickly infected large portions of populations of many countries, causing the coronavirus disease 2019 (COVID-19) pandemic. The COVID-19 pandemic is expected to continue and will likely cause many deaths until vaccines or efficient treatment protocols are tested and implemented.

[0004] Because of its ease of transmission, including from asymptomatic carriers, countries affected by COVID-19 take steps to curb infection rates. These steps include requesting/requiring social distancing, wherein individuals are asked to remain a predetermined distance from each other; shelter-in-place orders whereby bars/restaurants and other businesses deemed nonessential are closed; reminding individuals not to touch their faces; reminding individuals to wash their hands consistently; wearing masks in public; etc.

[0005] Business and school closings adversely affect the economy and parents/' 'children's mental health. More importantly, the virulent nature and manifest symptoms caused by some viruses also take a tremendous toll on healthcare workers, often overwhelming the healthcare system's capacity. More specifically, although the COVID-19 virus, for example, causes many patients to exhibit mild flu-like symptoms, some patients, particularly the elderly or those with co-morbidities, require enhanced medical care that may call for the use of ventilators and other breathing and patient

monitoring equipment. The machines and other devices required by some patients, in turn, increase the demand for skilled individuals to treat patients. Accordingly, one major issue identified during the treatment of the COVID-19 virus is that hospitals can be quickly overwhelmed with patients, resulting in longer hospital stays or increased mortality and limited care for patients with other conditions that require hospitalization.

[0006] Patients afflicted by COVID-19, like those afflicted by other diseases caused by coronaviruses and other viruses, will naturally create antibodies to the pathogen. These antibodies give the patient some degree of immunity for a predetermined time. More importantly, the antibodies can be taken from the formerly-infected patient and be used to create a serum for retreating currently infected patients. Formerly infected individuals are also unlikely to transmit the virus to others after a predetermined time post-infection. The presence of antibodies also would allow the patient to be "cleared" to work in jobs that formerly were off-limits as the chances of infection are high or to patronize any business (e.g., restaurants, bars, movie theaters, stores) that might otherwise be off-limits. For example, one of ordinary skill in the art will appreciate that healthcare workers are extremely vulnerable to be affected by many viruses, especially COVID-19, and it would be desirable to employ previously-infected or vaccinated individuals to maintain the needed hospital workforce. Business owners, such as those in the hotel, entertainment, bar, restaurant, etc., businesses, would also be desirous of hiring individuals that will not transmit the virus to customers and might desire to be open to immune customers.

[0007] It is foreseen that state, local, and foreign governments may mandate verification systems as a form of "immunity passport" to allow individuals to leave their homes, to gather in large groups, forgo mask-wearing, forgo social distancing rules, to work in certain industries, etc. Indeed, the U.S. government imposed strict vaccination guidelines to address a smallpox epidemic occurring in the early 1900s, so it reasonable to believe that the COVID-19 pandemic will force (or continue to force) entities to restrict civil liberties for the greater good of preserving life. It is also foreseen that individuals may be more willing to give up their civil liberties to be tracked with their mobile phone, randomly tested, etc. Notwithstanding any mandate, it is also foreseen that individuals may be willing to have their immunity status recorded in a voluntary database if it facilitates their ability to work, travel, and/or frequent businesses or other public places.

[0008] The following disclosure describes systems and methods for storing data related to pathogen exposure or vaccination. The data can be later used to verify immunity or provide a real-time certification that the patient is free of the pathogen and, thus, can perform certain tasks, be employed in certain locations, etc.

SUMMARY OF THE INVENTION

[0009] It is one aspect of some embodiments of the present invention to provide a system for storing patient-specific data that is accessible by the patient, physician, or a third party upon request. The patient-specific data stored in one embodiment of the present invention is very top-level – 1) last name, 2) access code, 3) if the patient was exposed to a pathogen, and when exposure occurred, 4) if the patient was vaccinated against the pathogen, 5) whether the patient has been tested for antibodies. It is contemplated that the information obtained and stored is minimal such that compliance with data security rules, e.g., such as the California Consumer Privacy Act (CCPA) and European Union's General Data Protection Regulation (GDPR), are met. In some embodiments, however, the "owner" of the information, such as the patient, may opt in to provide more information, such as their complete health records and/or biometric information. This enhanced data may be included with the minimal data needed for embodiments of the present invention to function or accessed upon the input of additional patient-identifying codes or passwords to provide a heightened security level. As one of ordinary skill in the art will appreciate, dual-factor authentication or biometric data (e.g., facial recognition, fingerprints, retinal scans, etc.) may be used. The end-user may also choose to indicate their willingness to be a serum donor if needed so their antibodies can be gathered, opt-in for some notifications (some notifications would be mandatory – the vaccine you took was ineffective or corrupted), opt-in for mobile phone tracking, etc.

[0010] In operation, a doctor, healthcare worker, or certified testing facility verifies the patient has been exposed to a pathogen and enters that information into the database. The date of exposure can also be added such that the patient may be contagious can be calculated. For example, some infected patients are contagious at the beginning of exposure, wherein their chances of infecting others with the pathogen decrease over time, sometimes days/weeks after the patient has exhibited symptoms. Maintaining the date of first exposure or symptom will allow the healthcare professional to assess a date whern patient is no longer at risk for contaminating others. The database may also

include vaccination dates, which could also include a future date that indicates the patient is no longer at risk for contaminating others. Finally, to ensure the information is sound, the doctor, for example, may be asked to include identifying information, such as their DEA number, NPI number, or other practice-specific information. Other healthcare workers (e.g., pharmacist, nurse, etc.) or testing centers (e.g., pharmacy, hospital, or ambulatory testing centers) may also be asked to provide specific identifying information. The testing lab associated with an antibody or PCR test, the vaccine lot number, etc. may also be stored in the database and accessed if it is later discovered that the testing procedures were incorrect, the vaccine lot was compromised, etc.

[0011] It is another aspect of some embodiments of the present invention to allow for selective access of data gathered to verify patient immunity. Here, the patient/healthcare professional/third-party can securely access the database through an electrical device, such as a home computer or mobile phone. In the operation of one embodiment, the end-user, the patient in this example, upon prompting by a third party, such as a potential employer, hospital system, airline, cruise ship, restaurant, theater, bar, state or federal health department, etc., can access the database real-time to provide a certification of prior exposure/immunity. The prompt for information may require a digital "handshake" wherein the user provides a portion of a secure code and another individual having access to the information, for example, the physician, application developer, another family member, etc., must input another piece of the code (e.g., dual-factor or better access protocols). Certification can be then delivered to the interested party, in one embodiment, by way of a secure message to a mobile device. Access to the database may require certain biometric information such as fingerprint or facial recognition to confirm that the individual holding the mobile phone, for example, is the individual whose data has been gathered, which will prevent fraud. Indeed, the third-party may also employ fraud-prevention tools, such as state or federal ID databases, to confirm the person touting their immunity status is the person providing the certificate.

[0012] Encryption may also be used. For example, in one embodiment, the user accesses database software by way of a computer or mobile application with a login name and password (dual-factor identification methods, biometrics, etc., could also be used) and, upon request, the database software generates a digital certificate, which may include a UPC code, a QR Code, or any other encrypted code. The digital certificate is then presented to a scanner to verify the user's health status.

[0013] It is another aspect of some embodiments of the present invention to use existing functionality provided by a user's mobile phone to actively communicate a patient's prior exposure, immunity, or non-exposure to the pathogen. For example, many mobile phones employ tools that allow individuals to find their friends or employ Bluetooth functionality that allows mobile phones to communicate with other mobile phones and devices a predetermined distance away. This functionality can be used to create a notice zone around the user's phone. In operation, a user previously exposed to the pathogen would broadcast that fact through their phone using, for example, Bluetooth, or via other signals that a mobile phone or other mobile device could conceivably generate (e.g., cellular, infra- or ultrasound waves). Any individual having access to an application associated with the contemplated database would access an "all clear" or "immune" signal and therefore appreciate why the person is not wearing a mask, not practicing social distancing, or working in a hospital or restaurant. Conversely, those who have not been exposed or those predisposed for re-exposure could broadcast that fact, wherein individuals would be more mindful to give that person a wider berth, for example.

[0014] The signal continuously broadcast or selectively sent by the user's mobile phone indicating immunity could be accessed by external sensors provided in bars, restaurants, movie theaters, hospitals, police stations, places of work or worship, etc., wherein access is only granted if the individual's phone triggers the sensor to indicate immunity. The contemplated sensor may be incorporated into a lock. Anti-fraud protocols can also be employed to ensure the person holding the mobile device is the actual person who is immune. These "safe spaces" protocols can be used to open restaurants, theaters, cruise ships, planes, trains, sections of hospitals, etc., to previously infected or vaccinated individuals. Conversely, other businesses would be reserved for those that have not been exposed to the pathogen. This separation can be used to help contain or monitor the spread of the pathogen. Ideally, all individuals carrying a mobile device will have access to a computer or mobile device would subscribe. For example, subscribers could permit their mobile devices to be tracked such that if some other subscriber (who may be unknown to them) later reported exposure and a probable date of exposure, the subscriber would be notified that their phone was in close proximity to or in the same building as a phone belonging to a person that has been exposed to a pathogen within a date window of highest contamination probability. The subscriber could then be directed to the nearest testing facility so they can be tested and, if infected,

self-quarantine during the time they are the most contagious, which should drastically reduce infection rates.

[0015] It is also one aspect of one embodiment of the present invention provides a system that allows for individuals who have been affected and are now "safe" to work to provide their willingness to work and/or digital resume so that businesses needing previously infected workers to quickly identify a potential workforce. This aspect of some embodiments of the present invention may also allow for the potential employer to quickly review the immunity certificate described above.

[0016] As briefly mentioned above, some embodiments of the present invention provide the ability for notifications to be sent to subscribers of the app-based system that communicates with the database. These notifications can provide information regarding the possible loss of immunity due to time from exposure, an inadequate response to vaccine, testing error, or new data suggesting inaccuracy of a previously approved test. Again, such loss of immunity could be broadcast to other subscribers (friends/strangers), notifying them that they may be exposed because of the patient's loss of immunity. The notifications may also include reminders to receive a booster vaccine if necessary. The notifications may also include reminders to receive other vaccines for the flu, pneumonia, shingles, etc. The notifications may be linked to the patient's physical location. For example, if the patient is near a blood bank that is harvesting antibodies, and the patient had previously indicated a willingness to provide such antibodies, they would receive a notification that they are a predetermined distance from the blood bank with directions included in the notification. A prompt may also be provided that allows the user to make an appointment to receive a vaccine.

[0017] The data gathered by the contemplated systems may be used by health care professionals or public health organizations (e.g., CDC, WHO, etc.) to calculate rates of infection, recovery rates, movement of patients (if they have allowed or have been mandated to allow their mobile device to be tracked) to track possible exposure/immunity to facilitate, as examples, epidemiological research and public health interventions. In some instances, demographic data such as race, national origin, residence information, etc. may be gathered to assess whether a particular pathogen has an affinity to a certain group.

[0018] The mobile application contemplated by some embodiments of the present invention may also employ tools to notify individuals that it is safe to go to certain locations, such as grocery stores that have recently been opened and disinfected. The

system may also provide notifications that the store is only open to those that have been infected, so they don't have to worry about infecting others. Of course, notifications can also include reminders to wash your hands, wash your mask, indicate that your mobile phone is less than a predetermined distance from another's mobile phone, etc. Although mobile phones have been mentioned herein, wearable devices, such as "smart" devices (e.g., smartwatches, fitness trackers, etc.) can perform the functionality described herein.

[0019] Embodiments of the present invention address the problems articulated above by providing a safe and effective way to verify that one is immune to a virus either by prior exposure or vaccination. The certification can be generated in real time and, thus, instantly verified. Again, in one embodiment, the verification is sent to a ''user's mobile device such as an Apple© watch or smartphone. In other instances, the system generates a physical certification of prior exposure and immunity. Ideally, a real-time solution is provided, such that when queried by government officials, for example, a user can quickly prove they are immune.

[0020] The contemplated immunity inquiry may be initiated by a code produced by a third party coupled with a code produced by the user. For example, national or state border patrol authorities can provide a QR request code to a visitor requesting entry. The user would scan the QR code and input a " key." The system would read the QR code coupled with the user key and generate a secure code or authorization to generate a certificate that verifies immunity. The key may be comprised of identifying information such as a retinal scan, facial recognition, a fingerprint, or a unique user-identified pin number or password, which ensures a proper “handshake." The certificate of immunity is forwarded to the ''user's mobile device and/or the requester. Again, this real-time solution may be required during pandemics where pathogens spread very quickly.

[0021] It is one aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of

patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; and generating a digital certificate related to the patient's immunity to the at least one pathogen.

[0022] It is another aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; and wherein data related to patient infection comprises exposure data and/or vaccination data.

[0023] It is one aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; and wherein the digital certificate can only be generated within a predetermined time window.

[0024] It is still yet another aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record

of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; and wherein the validation code includes data specific to the healthcare provider.

[0025] It is one aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; and wherein the character of the digital certificate is altered as a function of the time between exposure and issuance of the digital certificate.

[0026] It is one aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; and wherein exposure is detected through a sensor integrated into an insulin pump or sensor.

[0027] It is another aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data

related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; wherein exposure is detected through a sensor integrated into an insulin pump or sensor, and wherein the at least one security protocol comprises requiring the patient code before the digital certificate is issued.

[0028] It is one aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; wherein exposure is detected through a sensor integrated into an insulin pump or sensor, and wherein the patient code must be coupled with a randomly-generated requestor code before the digital certificate is issued.

[0029] It is one aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; wherein exposure is detected through a sensor integrated into an insulin pump or sensor, and wherein the patient code is biometric.

[0030] It is one aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; and wherein the digital certificate can be revoked by the healthcare professional or if a predetermined event occurs.

[0031] It is still yet another aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; wherein the digital certificate can be revoked by the healthcare professional or if a predetermined event occurs, and wherein the predetermined event comprises body temperature elevation above a predetermined degree, wherein the body temperature measurement comprises: scanning a temperature detector across an artery; providing a peak temperature reading from plural readings obtained during scanning, wherein the temperature detector comprises a radiation sensor that views a target surface area; further comprising computing an internal body temperature as a function of ambient temperature and the peak temperature reading; and wherein the function includes a weighted difference of surface temperature and ambient temperature, the weighting including an approximation of h/pc at an artery where h is a heat transfer coefficient between a target surface and ambient, p is perfusion rate, and c is blood specific heat.

[0032] It is one aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; wherein the digital certificate can be revoked by the healthcare professional or if a predetermined event occurs, and wherein the temperature detector is associated with a smart watch.

[0033] It is one aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; wherein the digital certificate can be revoked by the healthcare professional or if a predetermined event occurs, and further comprising issuing a notice that a certificate has been issued or revoked.

[0034] It is one aspect of some embodiments of the present invention to provide a method for verifying patient immunity to at least one pathogen, comprising: obtaining patent-specific data, comprising at least one patent identifying characteristic; obtaining exposure data related to patent exposure to the at least one pathogen; gathering data related to patient infection; verifying patient immunity; creating a digital record of patient immunity; adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity; forwarding the patent-specific data, exposure data, and digital record of

patient immunity to a database; selectively accessing the database upon compliance with at least one security protocol; generating a digital certificate related to the patient's immunity to the at least one pathogen; wherein the digital certificate can be revoked by the healthcare professional or if a predetermined event occurs, further comprising issuing a notice that a certificate has been issued or revoked, and wherein the notice is forwarded to a digital lock, whereby functionality of a key card or key code is modified depending on the contents of the notice.

[0035] It is yet another aspect of some embodiments of the present invention to provide a system for verifying patient immunity to at least one pathogen, comprising: a database comprising: at least one processor, a patient information module comprised of at least one processor configured to selectively receive at least one patent identifying characteristic; a pathogen exposure module comprised of at least one processor configured to receive data related to patent exposure to the at least one pathogen, the pathogen exposure module also configured to communicate with the patient information module; a verification module that receives input from a healthcare professional regarding patient immunity to the pathogen; a certificate generation module that communicates with the database upon compliance with predetermined security protocols; a notification module that communicates information from the database to an end user; and an input device that communicates with database.

[0036] It is yet another aspect of some embodiments of the present invention to provide a system for verifying patient immunity to at least one pathogen, comprising: a database comprising: at least one processor, a patient information module comprised of at least one processor configured to selectively receive at least one patent identifying characteristic; a pathogen exposure module comprised of at least one processor configured to receive data related to patent exposure to the at least one pathogen, the pathogen exposure module also configured to communicate with the patient information module; a verification module that receives input from a healthcare professional regarding patient immunity to the pathogen; a certificate generation module that communicates with the database upon compliance with predetermined security protocols; a notification module that communicates information from the database to an end user; an input device that communicates with database, and wherein the monitoring module and/or certificate generation module is in communication with a door lock.

[0037] It is still yet another aspect of some embodiments of the present invention to provide a system for verifying patient immunity to at least one pathogen, comprising: a database comprising: at least one processor, a patient information module comprised of at least one processor configured to selectively receive at least one patent identifying characteristic; a pathogen exposure module comprised of at least one processor configured to receive data related to patent exposure to the at least one pathogen, the pathogen exposure module also configured to communicate with the patient information module; a verification module that receives input from a healthcare professional regarding patient immunity to the pathogen; a certificate generation module that communicates with the database upon compliance with predetermined security protocols; a notification module that communicates information from the database to an end user; an input device that communicates with database, and wherein the monitoring module and/or certificate generation module is in communication with an activity or access module that selectively allows or prevents an individual from accessing a structure or participating in an activity.

[0038] It is one aspect of some embodiments of the present invention to provide a system for verifying patient immunity to at least one pathogen, comprising: a database comprising: at least one processor, a patient information module comprised of at least one processor configured to selectively receive at least one patent identifying characteristic; a pathogen exposure module comprised of at least one processor configured to receive data related to patent exposure to the at least one pathogen, the pathogen exposure module also configured to communicate with the patient information module; a verification module that receives input from a healthcare professional regarding patient immunity to the pathogen; a certificate generation module that communicates with the database upon compliance with predetermined security protocols; a notification module that communicates information from the database to an end user; an input device that communicates with database, and further comprising a monitoring module configured to communicate with at least one of the patient information module and the pathogen exposure module.

[0039] It is yet another aspect of some embodiments of the present invention to provide a system for verifying patient immunity to at least one pathogen, comprising: a database comprising: at least one processor, a patient information module comprised of at least one processor configured to selectively receive at least one patent identifying characteristic; a pathogen exposure module comprised of at least one processor

configured to receive data related to patent exposure to the at least one pathogen, the pathogen exposure module also configured to communicate with the patient information module; a verification module that receives input from a healthcare professional regarding patient immunity to the pathogen; a certificate generation module that communicates with the database upon compliance with predetermined security protocols; a notification module that communicates information from the database to an end user; an input device that communicates with database, further comprising a monitoring module configured to communicate with at least one of the patient information module and the pathogen exposure module, and wherein the monitoring module is configured to communicate with a GPS device.

[0040] It is one aspect of some embodiments of the present invention to provide a system for verifying patient immunity to at least one pathogen, comprising: a database comprising: at least one processor, a patient information module comprised of at least one processor configured to selectively receive at least one patent identifying characteristic; a pathogen exposure module comprised of at least one processor configured to receive data related to patent exposure to the at least one pathogen, the pathogen exposure module also configured to communicate with the patient information module; a verification module that receives input from a healthcare professional regarding patient immunity to the pathogen; a certificate generation module that communicates with the database upon compliance with predetermined security protocols; a notification module that communicates information from the database to an end user; an input device that communicates with database, further comprising a monitoring module configured to communicate with at least one of the patient information module and the pathogen exposure module, and wherein the monitoring module is configured to communicate with a temperature monitoring device.

[0041] The Summary of the Invention is neither intended nor should it be construed as being representative of the full extent and scope of the present invention. That is, these and other aspects and advantages will be apparent from the disclosure of the invention(s) described herein. Further, the above-described embodiments, aspects, objectives, and configurations are neither complete nor exhaustive. As will be appreciated, other embodiments of the invention are possible using, alone or in combination, one or more of the features set forth above or described below. Moreover, references made herein to "the present invention" or aspects thereof should be

understood to mean certain embodiments of the present invention and should not necessarily be construed as limiting all embodiments to a particular description. The present invention is outlined in various levels of detail in the Summary of the Invention as well as in the attached drawings and the Detailed Description and no limitation as to the scope of the present invention is intended by either the inclusion or non-inclusion of elements, components, etc. in this Summary of the Invention. Additional aspects of the present invention will become more readily apparent from the Detailed Description, particularly when taken together with the drawings.

[0042] The above-described benefits, embodiments, and/or characterizations are not necessarily complete or exhaustive, and in particular, as to the patentable subject matter disclosed herein. Other benefits, embodiments, and/or characterizations of the present invention are possible utilizing, alone or in combination, as set forth above and/or described in the accompanying figures and/or in the description hereinbelow.

[0043] The phrases "at least one," "one or more," and "and/or," as used herein, are open-ended expressions that are both conjunctive and disjunctive in operation. For example, each of the expressions "at least one of A, B, and C," "at least one of A, B, or C," "one or more of A, B, and C," "one or more of A, B, or C," and "A, B, and/or C" means A alone, B alone, C alone, A and B together, A and C together, B and C together, or A, B, and C together.

[0044] The term "automatic" and variations thereof, as used herein, refers to any process or operation done without material human input when the process or operation is performed. However, a process or operation can be automatic, even though performance of the process or operation uses material or immaterial human input, if the input is received before performance of the process or operation. Human input is deemed to be material if such input influences how the process or operation will be performed. Human input that consents to the performance of the process or operation is not deemed to be "material".

[0045] The term "computer-readable medium", as used herein, refers to any tangible storage and/or transmission medium that participate in providing instructions to a processor for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, NVRAM, or magnetic or optical disks. Volatile media includes dynamic memory, such as main memory. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic

tape, or any other magnetic medium, magneto-optical medium, a CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, and EPROM, a FLASH-EPROM, a solid state medium like a memory card, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read. A digital file attachment to e-mail or other self-contained information archive or set of archives is considered a distribution medium equivalent to a tangible storage medium. When the computer-readable media is configured as a database, it is to be understood that the database may be any type of database, such as relational, hierarchical, object-oriented, and/or the like. Accordingly, the disclosure is considered to include a tangible storage medium or distribution medium and prior art-recognized equivalents and successor media, in which the software implementations of the present disclosure are stored.

[0046] The terms "determine", "calculate" and "compute," and variations thereof, as used herein, are used interchangeably and include any type of methodology, process, mathematical operation or technique.

[0047] The term "module", as used herein, refers to any known or later developed hardware, software, firmware, artificial intelligence, fuzzy logic, or combination of hardware and software that is capable of performing the functionality associated with that element.

[0048] Unless otherwise indicated, all numbers expressing quantities, dimensions, conditions, and so forth used in the specification and drawing figures are to be understood as being approximations that may be modified in all instances as required for a particular application of the novel assembly and method described herein.

[0049] The term "a" or "an" entity, as used herein, refers to one or more of that entity. As such, the terms "a" (or "an"), "one or more" and "at least one" can be used interchangeably herein.

[0050] The use of "including," "comprising," or "having" and variations thereof herein is meant to encompass the items listed thereafter and equivalents thereof as well as additional items. Accordingly, the terms "including," "comprising," or "having" and variations thereof can be used interchangeably herein.

[0051] It shall be understood that the term "means" as used herein shall be given its broadest possible interpretation per 35 U.S.C., Section 112(f). Accordingly, a claim incorporating the term "means" shall cover all structures, materials, or acts set forth herein, and all of the equivalents thereof. Further, the structures, materials, or acts and

the equivalents thereof shall include all those described in the Summary, Brief Description of the Drawings, Detailed Description and in the appended drawing figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0052] The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention and together with the general description of the invention given above and the detailed description of the drawings given below, serve to explain the principles of these inventions.

[0053] Fig. 1 is a process flow of a method of one embodiment of the present invention.

[0054] Fig. 2 is a process flow of a method of another embodiment of the present invention.

[0055] Fig. 3 is an example communications/data processing network system that may be used in conjunction with embodiments of the present invention.

[0056] Fig. 4 is an example computer system that may be used in conjunction with embodiments of the present invention.

[0057] It should be understood that the drawings are not necessarily to scale. In certain instances, details that are not necessary for an understanding of the invention or that render other details difficult to perceive may have been omitted. It should be understood, of course, that the invention is not necessarily limited to the particular embodiments illustrated herein.

DETAILED DESCRIPTION

[0058] Fig. 1 shows system implementation of one embodiment of the present invention. After virus exposure, a user obtains confirmation of infection either by physical examination by a healthcare professional or, more commonly, from a positive test. One of ordinary skill in the art will appreciate that results of such tests may take hours to days. If infection is not confirmed, a certification is issued to the user. The certificate could be in the form of a QR code issued to user's mobile device, which may be scannable by government authorities, employers, guards, airline personnel, etc. Of course, other certificate forms, digital or physical, may be issued without departing from the scope of the invention.

[0059] If an infection is confirmed, relevant data is gathered, which will help healthcare providers and users appreciate how and when the exposure occurred. This data may be important to curb additional pathogen spread. For example, events that may have

caused the exposure, the date of possible exposure, and symptoms that predicated the visit to the healthcare provider may be logged. This information is used to set a quarantine period so the condition can run its course. It is important to note that infection confirmation is not required. More specifically, if exposure is likely, healthcare experts or state protocols may treat the user as being exposed, wherein relevant data is collected.

[0060] After the quarantine period has passed, a healthcare provider will "clear" the patient, which may entail issuing an immunity certificate and/or patient-specific release code that is entered into the contemplated system and used to selectively generate an immunity certificate. The release code may be associated with a physician-specific identifier, patient-specific identifier, or combination thereof. If the physician or other qualified healthcare professional does not believe the patient is immune because of subsequent tests, or lingering symptoms, the certificate is not issued and the patient is returned to quarantine for a predetermined time. This clearance step can be conducted multiple times, wherein previously-issued certificates may be revoked if needed.

[0061] Fig. 2 shows the method of another embodiment of the present invention. Here, patient data is stored in a database that includes patient baseline data. The baseline data is associated with traditional medical records and may include age, weight, ethnic background, medical history, blood type, family history, etc. Coupled with the baseline data is data more relevant to the pathogen of concern. This "relevant data" may include prior infections, date of prior infection, recovery time, symptoms, treatment protocols, etc. It may also include vaccinations and immunity data because immunity may not last for more than a predetermined time.

[0062] The relevant data is also associated with more current, real-time data similar to what was described in Fig. 1. For example, "current data" is related to the patient's temperature, recent test results, etc. This sub-database may receive information from third-party exposure apps. Vital readings from the user's smart device or wearable may also be fed into the current database. The vital data may include temperature, heart rate, etc. In one embodiment, user temperature is obtained by the methods described in U.S. Patent No. 6,292,685 and 7,787,938, which are incorporated by reference herein. The current database may also draw information from social media websites, wherein posts by the user's friends are monitored to identify instances of exposure, which may be communicated to the patient. For example, if a user's friend indicates they were at a party and now have contracted COVID-19, such information is forwarded to the user

or stored, wherein the user could be queried as to their whereabouts during the party. The user's internet search history could also be monitored to assess whether they are searching for information regarding symptoms of a pathogen of concern.

[0063] Upon an immunization or immunity inquiry from a third-party, the system will assess whether such inquiry has been authorized. Prior authorization can come from the user or may be mandated. If the inquiry was not approved, the certification of immunity is not issued. If the inquiry comes from the user, no preauthorization to access patient data and immunity validation is needed.

[0064] Next, the patient's health is validated, which entails drawing information from the patient database and may include input by a healthcare professional. The healthcare professional's approval may have been pre-obtained if, for example, a prior certificate has been issued. In some instances, prior certificates may become "stale" after a predetermined amount of time, wherein healthcare professionals may need to reassess patient data to re-recommend the issuance of a certificate. If the patient's health is validated, a certificate is issued as described above.

[0065] However, if the patient's immunity status is not validated, issuance of a new certificate is denied or a previously-issued certificate is revoked. Certificate revocation also happens in one embodiment of the present invention if predetermined parameters are exceeded. For example, the current database is continually updated with the user's temperature. If the user's temperature exceeds a predetermined level, the currently-issued certificate is revoked or flagged for further review. Certificate revocation may generate a notification to the user, the doctor, or other third parties, depending on user preferences. This will allow others that are part of the system to be quickly notified of possible exposure because of their friend's infection or reinfection.

[0066] As alluded to above, certificates can be temporal. Commonly, the certificate will sunset over time and expire. In another embodiment, the strength of the certificate may be apparent by a color code or other designation. For example, a green certificate would mean that the validation of immunity has occurred within a predetermined amount of time, e.g., six hours. The certificate color may change or fade over time based on various factors.

[0067] Embodiments of the present invention contemplate the issuance of notices when a certificate is issued, not issued, or revoked. Such information is sent to predefined interested parties. For example, the notification or certificate could be sent to a user's

workplace or employment websites. The certificate can be used to unlock doors, wherein scanning of the certificate acts as a key.

[0068] Referring to Fig. 3, an example network system is provided that may be used in connection with the classification systems and methods disclosed herein. More specifically, Fig. 3 illustrates a block diagram of a system 100 that may use a web service connector to integrate an application with a web service. The system 100 includes one or more user computers 105, 110, and 115. The user computers 105, 110, and 115 may be general-purpose personal computers (including, merely by way of example, personal computers and/or laptop computers running various versions of Microsoft Corp.'s Windows™ and/or Apple Corp.'s Macintosh™ operating systems) and/or workstation computers running any of a variety of commercially-available UNIX™ or UNIX-like operating systems. These user computers 105, 110, 115 may also have any of a variety of applications, including, for example, database client and/or server applications, and web browser applications. Alternatively, the user computers 105, 110, and 115 may be any other electronic device, such as a thin-client computer, Internet-enabled mobile telephone, and/or personal digital assistant, capable of communicating via a network (e.g., the network 120 described below) and/or displaying and navigating web pages or other types of electronic documents. Although the exemplary system 100 is shown with three user computers, any number of user computers may be supported.

[0069] System 100 further includes a network 120. The network 120 may be any type of network familiar to those skilled in the art that can support data communications using any of a variety of commercially-available protocols, including without limitation TCP/IP, SNA, IPX, AppleTalk, and the like. Merely by way of example, the network 120 may be a local area network ("LAN"), such as an Ethernet network, a Token-Ring network and/or the like; a wide-area network; a virtual network, including without limitation a virtual private network ("VPN"); the Internet; an intranet; an extranet; a public switched telephone network ("PSTN"); an infra-red network; a wireless network (e.g., a network operating under any of the IEEE 802.11 suite of protocols, the Bluetooth™ protocol known in the art, and/or any other wireless protocol); and/or any combination of these and/or other networks.

[0070] The system 100 may also include one or more server computers 125, 130. One server may be a web server 125, which may be used to process requests for web pages

or other electronic documents from user computers 105, 110, and 120. The web server can be running an operating system including any of those discussed above, as well as any commercially-available server operating systems. The web server 125 can also run a variety of server applications, including HTTP servers, FTP servers, CGI servers, database servers, Java servers, and the like. In some instances, the web server 125 may publish operations available as one or more web services.

[0071] The system 100 may also include one or more file and/or application servers 130, which can, in addition to an operating system, include one or more applications accessible by a client running on one or more of the user computers 105, 110, 115. The server(s) 130 may be one or more general-purpose computers capable of executing programs or scripts in response to the user computers 105, 110 and 115. As one example, the server may execute one or more web applications. The web application may be implemented as one or more scripts or programs written in any programming language, such as JavaTM, C, C#™ or C++, and/or any scripting language, such as Perl, Python, or TCL, as well as combinations of any programming/scripting languages. The application server(s) 130 may also include database servers, including without limitation those commercially available from Oracle, Microsoft, SybaseTM, IBMTM and the like, which can process requests from database clients running on a user computer 105.

[0072] In some embodiments, an application server 130 may create web pages dynamically for displaying the development system. The web pages created by the web application server 130 may be forwarded to a user computer 105 via a web server 125. Similarly, the web server 125 may be able to receive web page requests, web services invocations, and/or input data from a user computer 105 and can forward the web page requests and/or input data to the web application server 130.

[0073] In further embodiments, the server 130 may function as a file server. Although for ease of description, Fig. 3 illustrates a separate web server 125 and file/application server 130, those skilled in the art will recognize that the functions described with respect to servers 125, 130 may be performed by a single server and/or a plurality of specialized servers, depending on implementation-specific needs and parameters.

[0074] The system 100 may also include a database 135. The database 135 may reside in a variety of locations. By way of example, database 135 may reside on a storage medium local to (and/or resident in) one or more of the computers 105, 110, 115, 125,

130. Alternatively, it may be remote from any or all of the computers 105, 110, 115, 125, 130, and in communication (e.g., via the network 120) with one or more of these. In a particular set of embodiments, the database 135 may reside in a storage-area network ("SAN") familiar to those skilled in the art. Similarly, any necessary files for performing the functions attributed to the computers 105, 110, 115, 125, 130 may be stored locally on the respective computer and/or remotely, as appropriate. In one set of embodiments, the database 135 may be a relational database, such as Oracle 10i™, that is adapted to store, update, and retrieve data in response to SQL-formatted commands.

[0075] Referring to Fig. 4, an example computer system is provided that may be used in connection with the classification systems and methods disclosed herein. More specifically, Figure 2 illustrates one embodiment of a computer system 200 upon which a web service connector or components of a web service connector may be deployed or executed. The computer system 200 is shown comprising hardware elements that may be electrically coupled via a bus 255. The hardware elements may include one or more central processing units (CPUs) 205; one or more input devices 210 (e.g., a mouse, a keyboard, etc.); and one or more output devices 215 (e.g., a display device, a printer, etc.). The computer system 200 may also include one or more storage device 220. By way of example, storage device(s) 220 may be disk drives, optical storage devices, solid-state storage device such as a random access memory ("RAM") and/or a read-only memory ("ROM"), which can be programmable, flash-updateable and/or the like.

[0076] The computer system 200 may additionally include a computer-readable storage media reader 225; a communications system 230 (e.g., a modem, a network card (wireless or wired), an infra-red communication device, etc.); and working memory 240, which may include RAM and ROM devices as described above. In some embodiments, the computer system 200 may also include a processing acceleration unit 235, which can include a DSP, a special-purpose processor and/or the like.

[0077] The computer-readable storage media reader 225 can further be connected to a computer-readable storage medium, together (and, optionally, in combination with storage device(s) 220) comprehensively representing remote, local, fixed, and/or removable storage devices plus storage media for temporarily and/or more permanently containing computer-readable information. The communications system 230 may permit data to be exchanged with the network 220 and/or any other computer described above with respect to the system 200.

[0078] The computer system 200 may also comprise software elements, shown as being currently located within a working memory 240, including an operating system 245 and/or other code 250, such as program code implementing a web service connector or components of a web service connector. It should be appreciated that alternate embodiments of a computer system 200 may have numerous variations from that described above. For example, customized hardware might also be used and/or particular elements might be implemented in hardware, software (including portable software, such as applets), or both. Further, connection to other computing devices such as network input/output devices may be employed.

[0079] It should be appreciated that the methods described herein may be performed by hardware components or may be embodied in sequences of machine-executable instructions, which may be used to cause a machine, such as a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the methods. These machine-executable instructions may be stored on one or more machine-readable mediums, such as CD-ROMs or other type of optical disks, floppy diskettes, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, flash memory, or other types of machine-readable mediums suitable for storing electronic instructions. Alternatively, the methods may be performed by a combination of hardware and software.

[0080] Exemplary characteristics of embodiments of the present invention have been described. However, to avoid unnecessarily obscuring embodiments of the present invention, the preceding description may omit several known apparatus, methods, systems, structures, and/or devices one of ordinary skill in the art would understand are commonly included with the embodiments of the present invention. Such omissions are not to be construed as a limitation of the scope of the claimed invention. Specific details are set forth to provide an understanding of some embodiments of the present invention. It should, however, be appreciated that embodiments of the present invention may be practiced in a variety of ways beyond the specific detail set forth herein.

[0081] Modifications and alterations of the various embodiments of the present invention described herein will occur to those skilled in the art. It is to be expressly understood that such modifications and alterations are within the scope and spirit of the present invention, as set forth in the following claims. Further, it is to be understood that the invention(s) described herein is not limited in its application to the details of construction and the arrangement of components set forth in the preceding description

or illustrated in the drawings. That is, the embodiments of the invention described herein are capable of being practiced or of being carried out in various ways. The scope of the various embodiments described herein is indicated by the following claims rather than by the foregoing description. And all changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope. It is intended to obtain rights which include alternative embodiments to the extent permitted, including alternate, interchangeable and/or equivalent structures, functions, ranges or steps to those claimed, whether or not such alternate, interchangeable and/or equivalent structures, functions, ranges or steps are disclosed herein, and without intending to publicly dedicate any patentable subject matter.

[0082] The foregoing disclosure is not intended to limit the invention to the form or forms disclosed herein. In the foregoing Detailed Description, for example, various features of the invention are grouped together in one or more embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed inventions require more features than expressly recited. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the following claims are hereby incorporated into this Detailed Description, with each claim standing on its own as a separate preferred embodiment of the invention. Further, the embodiments of the present invention described herein include components, methods, processes, systems, and/or apparatus substantially as depicted and described herein, including various sub-combinations and subsets thereof. Accordingly, one of skill in the art will appreciate that would be possible to provide for some features of the embodiments of the present invention without providing others. Stated differently, any one or more of the aspects, features, elements, means, or embodiments as disclosed herein may be combined with any one or more other aspects, features, elements, means, or embodiments as disclosed herein.

What is claimed is:

1. A method for verifying patient immunity to at least one pathogen, comprising:

obtaining patent-specific data, comprising at least one patent identifying characteristic;

obtaining exposure data related to patent exposure to the at least one pathogen;

gathering data related to patient infection;

verifying patient immunity;

creating a digital record of patient immunity;

adding a predefined validation code by a healthcare professional to at least one of the patient-specific data, exposure data, and digital record of patient immunity;

forwarding the patent-specific data, exposure data, and digital record of patient immunity to a database;

selectively accessing the database upon compliance with at least one security protocol; and

generating a digital certificate related to the patient's immunity to the at least one pathogen.

2. The method of claim 1, wherein data related to patient infection comprises exposure data and/or vaccination data.

3. The method of claim 1, wherein the digital certificate can only be generated within a predetermined time window.

4. The method of claim 1, wherein the validation code includes data specific to the healthcare provider.

5. The method of claim 1, wherein the character of the digital certificate is altered as a function of the time between exposure and issuance of the digital certificate.

6. The method of claim 1, wherein exposure is detected through a sensor integrated into an insulin pump or sensor.

7. The method of claim 1, wherein the at least one security protocol comprises requiring the patient code before the digital certificate is issued.

8. The method of claim 7, wherein the patient code must be coupled with a randomly-generated requestor code before the digital certificate is issued.

9. The method of claim 7, wherein the patient code is biometric.

10. The method of claim 1, wherein the digital certificate can be revoked by the healthcare professional or if a predetermined event occurs.

11. The method of claim 10, wherein the predetermined event comprises body temperature elevation above a predetermined degree, wherein the body temperature measurement comprises:

scanning a temperature detector across an artery;

providing a peak temperature reading from plural readings obtained during scanning, wherein the temperature detector comprises a radiation sensor that views a target surface area;

further comprising computing an internal body temperature as a function of ambient temperature and the peak temperature reading; and

wherein the function includes a weighted difference of surface temperature and ambient temperature, the weighting including an approximation of h/pc at an artery where h is a heat transfer coefficient between a target surface and ambient, p is perfusion rate, and c is blood specific heat.

12. The method of claim 10, wherein the temperature detector is associated with a smart watch.

13. The method of claim 10, further comprising issuing a notice that a certificate has been issued or revoked.

14. The method of claim 13, wherein the notice is forwarded to a digital lock, whereby functionality of a key card or key code is modified depending on the contents of the notice.

15. A system for verifying patient immunity to at least one pathogen, comprising:

a database comprising:

at least one processor,

a patient information module comprised of at least one processor configured to selectively receive at least one patent identifying characteristic;

a pathogen exposure module comprised of at least one processor configured to receive data related to patent exposure to the at least one pathogen, the pathogen exposure module also configured to communicate with the patient information module;

a verification module that receives input from a healthcare professional regarding patient immunity to the pathogen;

a certificate generation module that communicates with the database upon compliance with predetermined security protocols;

a notification module that communicates information from the database to an end user; and

an input device that communicates with database.

16. The system of claim 15, wherein the monitoring module and/or certificate generation module is in communication with a door lock.

17. The system of claim 15, wherein the monitoring module and/or certificate generation module is in communication with an activity or access module that selectively allows or prevents an individual from accessing a structure or participating in an activity.

18. The system of claim 15, further comprising a monitoring module configured to communicate with at least one of the patient information module and the pathogen exposure module.

19. The system of claim 18, wherein the monitoring module is configured to communicate with a GPS device.

20. The system of claim 18, wherein the monitoring module is configured to communicate with a temperature monitoring device.

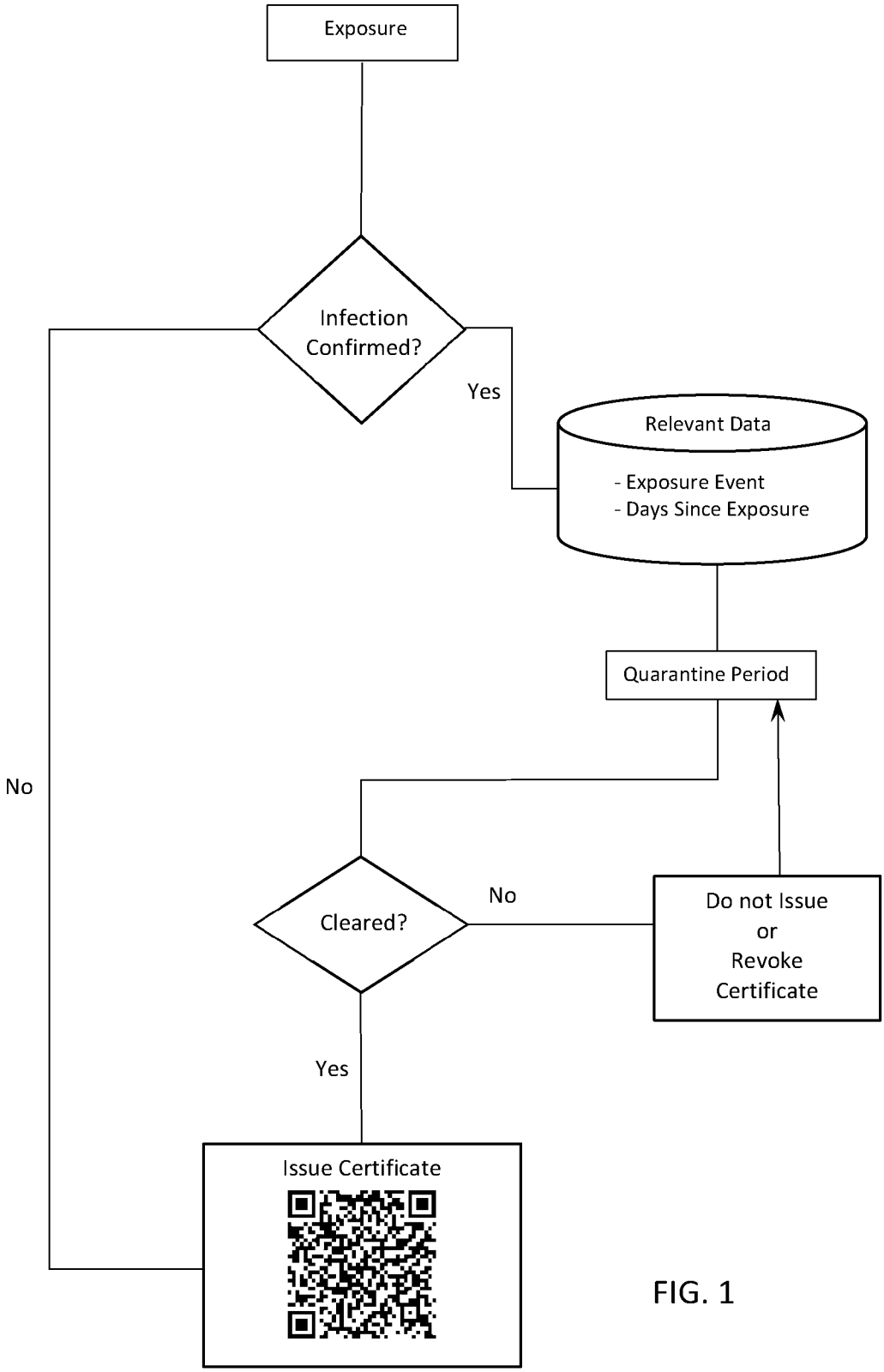

Exposure
Infection Confirmed?
Yes
No
Relevant Data
- Exposure Event
- Days Since Exposure
Quarantine Period
Cleared?
No
Do not Issue or Revoke Certificate
Yes
Issue Certificate

FIG. 1

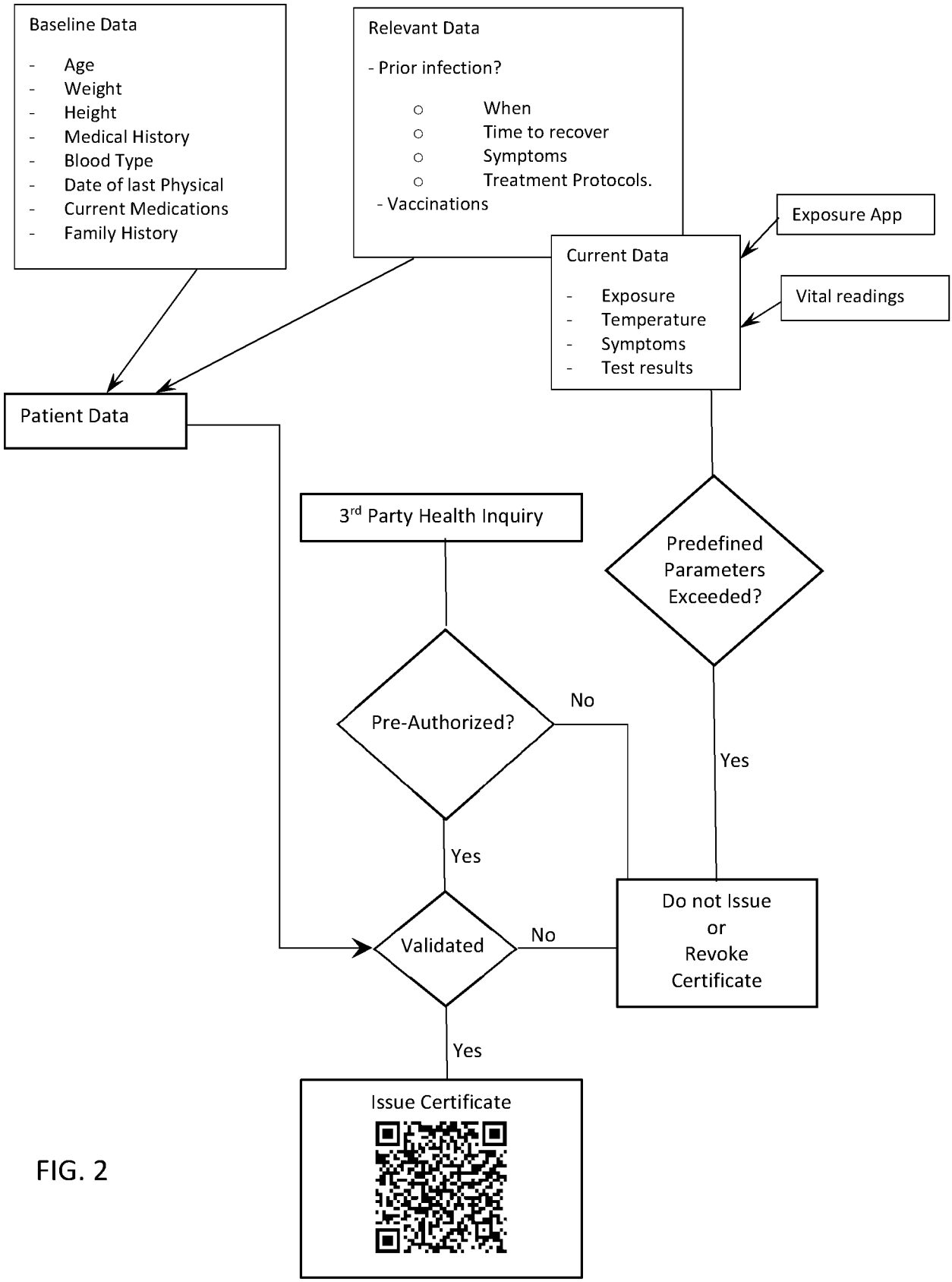

Baseline Data
- Age
- Weight
- Height
- Medical History
- Blood Type
- Date of last Physical
- Current Medications
- Family History
Relevant Data
- Prior infection?
○ When
○ Time to recover
○ Symptoms
○ Treatment Protocols.
- Vaccinations
Exposure App
Current Data
- Exposure
- Temperature
- Symptoms
- Test results
Vital readings
Patient Data
3rd Party Health Inquiry
Predefined Parameters Exceeded?
Pre-Authorized?
No
Yes
Yes
Validated
No
Do not Issue or Revoke Certificate
Yes
Issue Certificate

FIG. 2

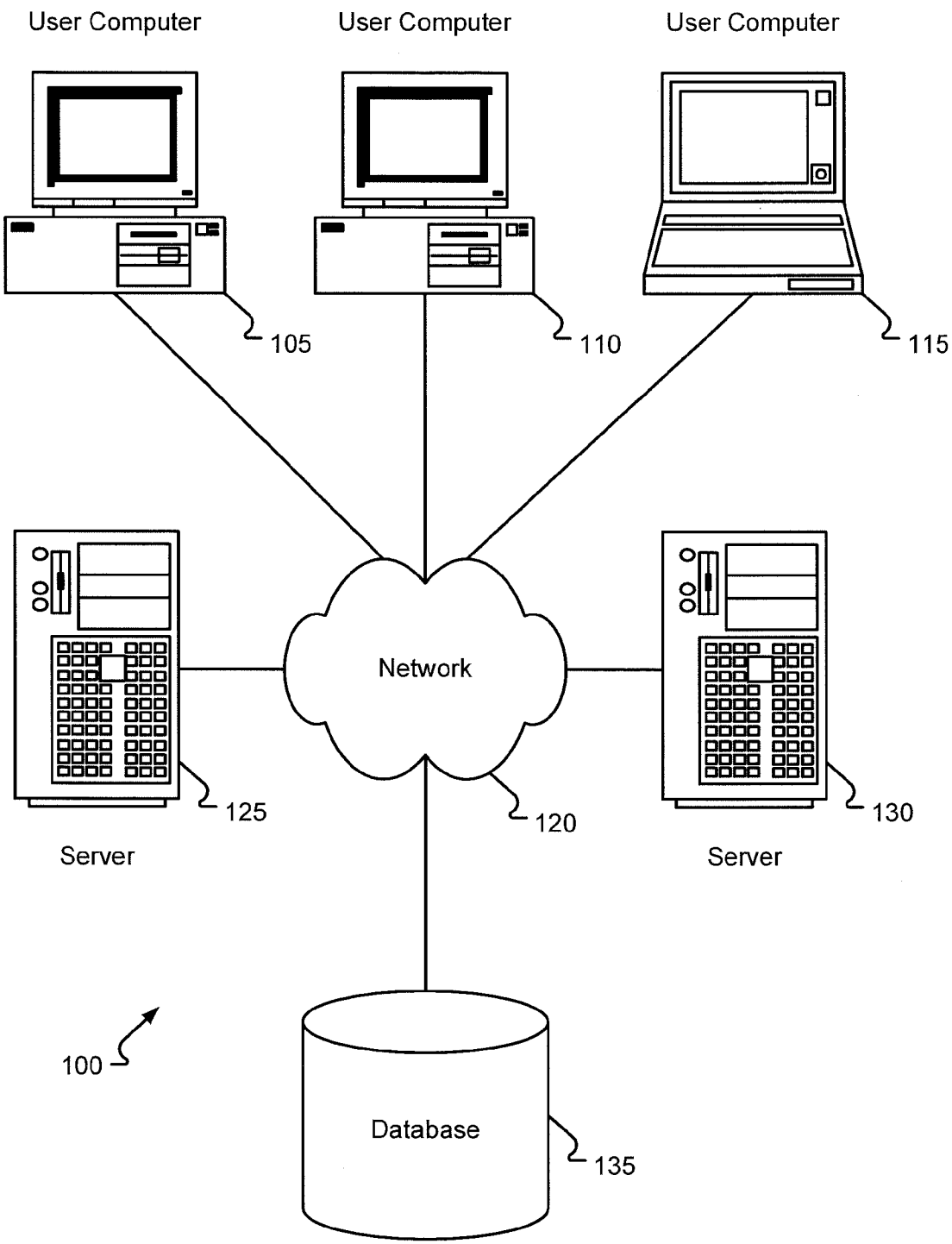

User Computer
User Computer
User Computer
105
110
115
Network
125
120
130
Server
Server
100
Database
135

FIG. 3

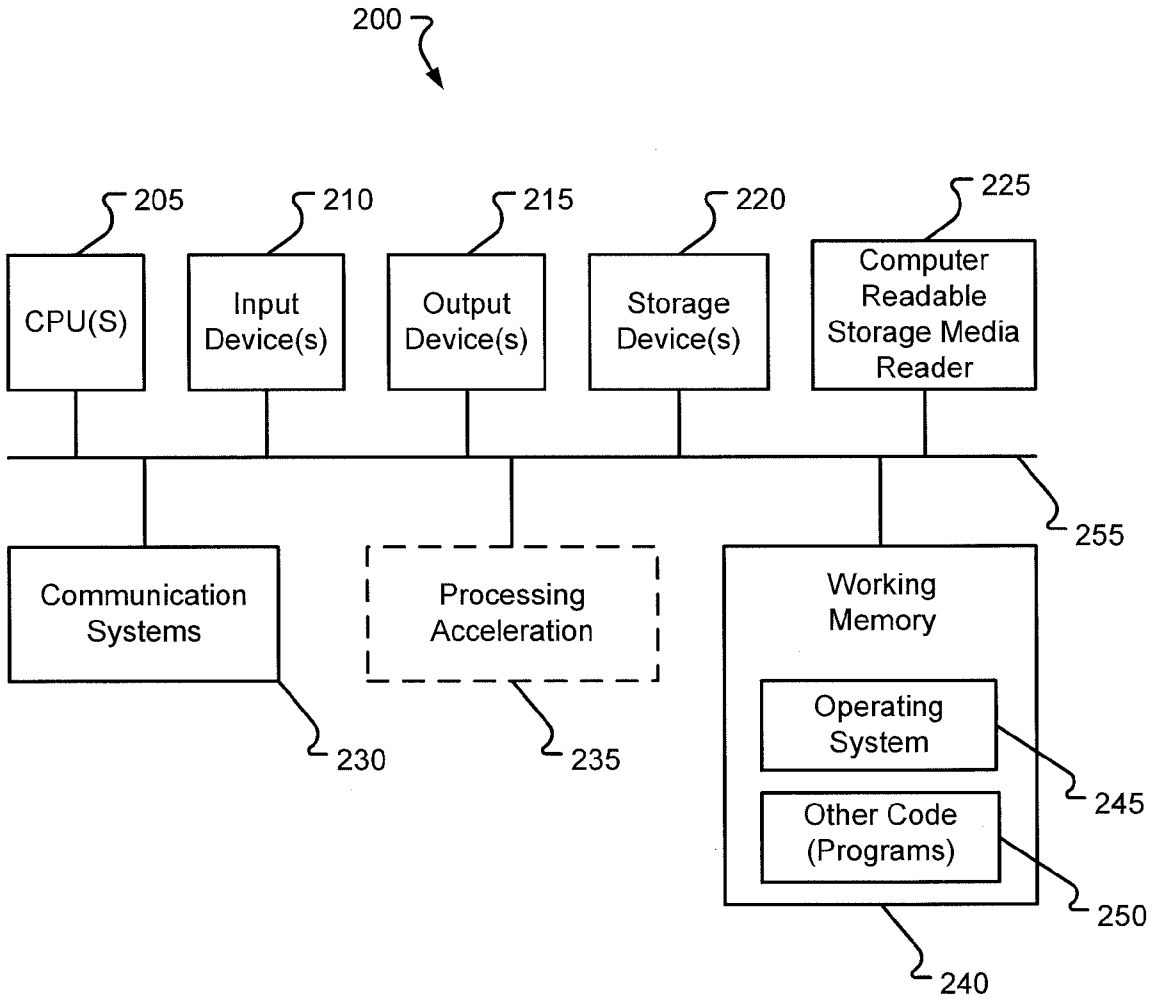

200
205
210
215
220
225
CPU(S)
Input Device(s)
Output Device(s)
Storage Device(s)
Computer Readable Storage Media Reader
255
Communication Systems
Processing Acceleration
Working Memory
Operating System
Other Code (Programs)
230
235
245
250
240

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2021/026580

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06Q 10/00; G06Q 10/06; G06Q 50/00; G16H 10/60 (2021.01)
CPC - G16H 50/80; G06Q 10/06; G16H 10/20; G16H 10/60; G16H 10/65; G16H 15/00; G16H 40/67 (2021.05)

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 2011/0029488 A1 (FUERST et al) 03 February 2011 (03.02.2011) entire document	1, 2, 4, 6, 7, 9, 15, 17
Y	US 7,128,258 B1 (HARPER) 31 October 2006 (31.10.2006) entire document	1, 2, 4, 6, 7, 9, 15, 17
Y	US 2015/0102208 A1 (THE JOAN & IRWIN JACOBS TECHNION-CORNELL INNOVATION INSTITUTE (JACOBS INSTITUTE)) 16 April 2015 (16.04.2015) entire document	6
A	US 2003/0143636 A1 (SIMONSON et al) 31 July 2003 (31.07.2003) entire document	1-20
A	US 2014/0323347 A1 (TRACKER LLC) 30 October 2014 (30.10.2014) entire document	1-20

☐ 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
"D" document cited by the applicant in the international application
"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	Date of mailing of the international search report
21 June 2021	JUL 20 2021
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Harry Kim Telephone No. PCT Helpdesk: 571-272-4300