Provided is a collecting apparatus and a collecting method for recording medical transactions designed to protect patient privacy when necessary to record private biometric individual data. This collecting apparatus and collecting method can improve patient privacy when using a biometric signature such as fingerprints, face scans and related characteristics when recorded into a computing system.
COLLECTING APPARATUS AND COLLECTING METHOD

CROSS-REFERENCE TO RELATED APPLICATIONS
This application claims priority to US non-provisional application Ser. No. 15/707,431 filed on Sep. 18, 2017.

FIELD OF THE INVENTION
The present invention relates to a collecting apparatus and a collecting method which reads, records, and encodes patient biometric data.

BACKGROUND OF THE INVENTION
Medical device technology and the systems providing health-care service to public populations have progressed exponentially during recent years following computing revolution in the early 1970's and personal computing revolutions since the 1980's.

This is well-known history and the public health benefits deriving from these technical and informational advancements are very important and significant for citizens of many countries. However, along with this progress, there are unanticipated challenges created by the complexity and inter-connectedness of medical and health-care industry systems.

One recent risk has been the proliferation of 'hacker' activity with purpose of causing damage and disruption to others based upon personal, political, nation-state and economic objectives. For medical industry, this means patients have valid concerns about the privacy, accuracy and disclosure of their very sensitive health-related and person-related information.

Current industry trends address these problems with ubiquitous security solutions focused on applications, databases, firewalls, and activity alarm systems. One part of the solution is, for example, proprietary encrypting hard drives which are manufactured and installed in servers and workstations to protect against unauthorized disclosure. And, in short, there is a public problem that requires multiple solutions to protect privacy of individuals and patients. Privacy expectations are extremely
sensitive in medical health-care.

SUMMARY OF THE INVENTION
The object of the present invention is to overcome above deficiencies by providing a collecting apparatus and a collecting method which improves patient privacy when using a biometric signature such as fingerprints, face scans and related characteristics when recording patient information into a computing system.

A first aspect of the present invention relates to a collecting apparatus. The collecting apparatus reads, records, and encodes patient biometric data, and including:

- an input module configured to input patient information;
- a photo collecting module including a display unit configured to display countdown timer instructions for taking photos, a camera unit configured to take photos and store the photos in a temporary storage device, an encoder unit combines and hashes the photos into a combined data set and forwards the combined data set (encoded photos) to a privacy encoder temporary storage;
- a fingerprint collecting module including a display unit configured to display instructions for fingerprint capture, a fingerprint scan unit configured to actuate fingerprint scan, a processing unit that processes fingerprint scan into fingerprint template data set, a privacy encoder unit configured to combine and encrypt all data acquired into an encrypted data set,
- a purging module configured to purge all temporary data acquired by the photo collecting module and the fingerprint collecting module; and
- a casing module in which the photo collecting module, the fingerprint collecting module, and the purging module are arranged, including filter vents, an exhaust vent screen, and an intake vent filter configured to remove particulate matter and improve reliability of apparatus.

The collecting apparatus deletes original biometric data before delivery to a computing main board and software. The collecting apparatus delivers resulting biometric data in an encoded and encrypted data set to a computing main board for permanent storage.
With this collecting apparatus, the private information is scrambled and encoded in a manner that cannot be deciphered outside of the apparatus. This therefore allows for permanent storage of such biometric information (scrambled without external cipher keys) without risk of viruses, theft and loss of system data from cloud, private network, or insurance industry data warehouse systems. There are numerous possibilities, variations and vendors in the medical and finance marketplace with biometric reader equipment.

Further, the camera unit may include two cameras. One of the two cameras is for normal visible light and the other is for non-visible light, and the two cameras may be aligned to take a photo in the same direction.

Further, the fingerprint scan unit may include two fingerprint readers, one of the two fingerprint readers is for one finger, for example, a thumbprint reader, and the other is for multiple fingers, for example, a fingerprint bar reader, and the two fingerprint readers may be located proximate to each other.

A sixth aspect of the present invention provides a collecting method for recording a medical transaction declaration. The method includes the steps of:

- inputting private information of a patient;
- requiring two immediate and simultaneous fingerprints;
- displaying prompts for camera photograph;
- acquiring camera photos;
- recording an affirmative or negative response through apparatus display and user-selectable response;
- prompting for a biometric reader activation;
- recording biometric fingerprints from two persons on two physical reader devices;
- time-stamping a first fingerprint and a second fingerprint and electronically determines that the two fingerprints are recorded within a certain time period;
- computing an electronic decision about the physical proximity of the two persons based upon a time-stamp of the first fingerprint and a time-stamp of the second fingerprint;
- merging biometric signatures, from the two persons, with an "agreement document".
generating a "signed agreement document"; and
outputting "signed agreement document" to a computing main board.

A collecting method of a seventh aspect of the present invention is the collecting
method according to the sixth aspect, wherein
the private information including last name, first name and initial of patient,
identifying medical number of patient, and date of birth of patient, and wherein
the response including an affirmative response and a negative response.

A collecting method of an eighth aspect of the present invention is the collecting
method according to the sixth or the seventh aspect, wherein
the certain time period is, for example, 10 seconds.

A collecting method of a ninth aspect of the present invention is the collecting method
according to the eighth aspect, wherein
the two persons including a patient and a witness.

With this collecting apparatus and collecting method described above, patient privacy
can be protected while recording some highly private and personal data about an
individual. This is a challenging solution considering the high-level government and
insurance industry goals, in a systematic way, demand collecting biometric
information (i.e. fingerprints, photographs, other data based upon personal
characteristics of an individual).

The present invention has been briefly described above. Details of the present
invention will be further described in the embodiments below with the accompanied
drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig.1 is a perspective view schematically showing an overall construction of a
collecting apparatus of a preferred embodiment of the present invention.
Fig.2 is a schematic diagram showing hardware mechanisms in the collecting
apparatus of Fig.1.
Fig. 3 is a flowchart showing a collecting method of a preferred embodiment of the present invention.

In the figures:

DETAILED DESCRIPTION OF THE INVENTION

Referring to Fig. 1, a collecting apparatus is described. Fig. 1 is a perspective view schematically showing an overall construction of a collecting apparatus of a preferred embodiment of the present invention.

The collecting apparatus comprises: a casing module 1 with filtered vents; an exhaust vent screen 2; an intake vent filter 3 which is necessary to remove particulate matter and improve reliability of apparatus in imperfect and hot field conditions; an display screen 4 which displays instructions provided to the patient; a metal heat-sink casing 5 for camera heat; two camera modules 6, of which normal visible light for one camera and thermal, infrared or non-visible light spectrum for the other; a fingerprint bar reader 7 for multiple-finger scanning; and a thumbprint reader 8 used for single-finger scanning.

The collecting apparatus has a trapezoidal shape in its side view and a substantially rectangular shape in its front view. An exhaust vent screen 2 is formed in the top part and side part of the collecting apparatus, through which air flows out; while an intake vent filter 3 is formed at the bottom part of the collecting apparatus, through which the air flows in.

The display screen 4 is provided in the front face of the apparatus and has a rectangular shape. A camera module is provided below the display screen 4, in the camera module, there are two different cameras aligned in the height direction, one of the two cameras is for visible light and the other is for non-visible light.

The casing 5 is made of material that is easy to dissipate the heat generated by the
camera module, preferably, made of metals.

A fingerprint collecting module is provided in the bottom part of the collecting apparatus. The fingerprint collecting module includes two fingerprint readers, a fingerprint reader 7 and a fingerprint reader 8 that are provided adjacent to each other. Among the two fingerprint readers, one fingerprint reader which is elongated shape is used for multiple-finger scanning, while the other fingerprint reader is used for single-finger scanning, for example, thumb scanning.

Inside the casing module, there is provided a purging module configured to purge all temporary data acquired by the photo collecting module and the fingerprint collecting module.

Hardware mechanisms in the collecting apparatus of Fig.1 will be described with reference to Fig.2. Fig.2 is a diagram showing hardware mechanisms in the collecting apparatus of Fig.1.

As shown, this diagram indicates the relationship and order of hardware mechanisms in the collecting apparatus in Fig.1. The process begins at the top with an acquisition hardware (two camera modules 6), where raw biometric data is input. This unprotected data is encoded by hardware before delivery to temporary storage on an encryption chip mechanism. The collecting apparatus utilizes a private encryption key which is known only to the apparatus. And the hardware encryption mechanism is marked privacy encoder chip to illustrate this final step.

A collecting method of a preferred embodiment of the present invention is described with reference to Fig.3. Fig.3 is a flowchart showing a collecting method of a preferred embodiment of the present invention. This flowchart demonstrates how a private biometric signature can be used to confirm a real-time medical transaction. For medical fraud prevention, these steps demonstrate how a patient can review a document and then certify with a witness, using a real-time apparatus, with hardware encryption.
In the first step, an agreement document is input and displayed.

Then, the collecting apparatus of the present invention prompts for acceptance or non-acceptance. In this step, if the patient acknowledges and accepts the document, the apparatus prompts for photo, and the patient waits 3-5 seconds for photo; and, if the patient does not accept the document, the process returns back to the first step.

After taking the photo successfully, the process goes on to the next step, where biometric fingerprints are required to confirm the identities of the patient and the witness, wherein, the fingerprints from two persons are recorded on two physical reader devices.

Next, the collecting apparatus time-stamps each biometric fingerprints and electronically determines that the fingerprints are recorded within a certain time period, for example, 10 seconds; then computing an electronic decision about the physical proximity of one person and one witness based upon the first fingerprint reader time-stamp and the second fingerprint reader time-stamp. If it is determined that the fingerprints are recorded within 10 seconds, the apparatus merges biometric signatures, from two persons, with an "agreement document", generating a "signed agreement document"; and if it is determined that the fingerprint are not recorded within 10 seconds, the process returns to the fingerprint scan step.

Then the process goes on to the last step where the "signed agreement document" is output to a computing main board, and the process is finished by now.

Heretofore, the invention is described with reference to specific embodiment, however, the invention is not limited to this. The above embodiment according to the invention may be subjected to various modifications and improvements on the basis of common knowledge of persons skilled in the art.
CLAIMS

We claim:

1. A collecting apparatus for recording a medical transaction declaration, comprising:
   an input module for inputting patient information:
      a photo collecting module including
         a display unit configured to display countdown timer instructions for taking
         photos, a camera unit configured to take photos and store the photos in a temporary
         storage device, an encoder unit combines and hashes the photos into a combined data
         set and forwards the combined data set to a privacy encoder temporary storage;
      a fingerprint collecting module including a display unit configured to display
         instructions for fingerprint capture;
         a fingerprint scan unit configured to actuate fingerprint scan,
         a processing unit that processes fingerprint scan into fingerprint template data set,
      a privacy encoder unit configured to combine and encrypt all data acquired into
         an encrypted data set,
      a purging module configured to purge all temporary data acquired by the photo
         collecting module and the fingerprint collecting module; and
      a casing module in which the photo collecting module, the fingerprint collecting
         module, and the purging module are arranged, including filter vents, an exhaust vent
         screen, and an intake vent filter configured to remove particulate matter and improve
         reliability of apparatus;
   wherein the collecting apparatus deletes original biometric data before delivery to
   a computing main board and software; and the collecting apparatus delivers resulting
   biometric data in an encoded and encrypted data set to a computing main board for
   permanent storage.

2. The collecting apparatus of claim 1, wherein the camera unit includes two cameras,
   one of the two cameras is for normal visible light and the other is for non-visible light.

3. The collecting apparatus of claim 2, wherein the two cameras are aligned to take a
   photo in the same direction.
4. The collecting apparatus of any one of claims 1 to 3, wherein the fingerprint scan unit includes two fingerprint readers, one of the two fingerprint readers is for one finger and the other is for multiple fingers.

5. The collecting apparatus of claim 4, wherein the two fingerprint readers are located proximate to each other.

6. A collecting method for recording medical transaction declaration, comprising:
   - inputting private information of a patient;
   - requiring two immediate and simultaneous fingerprints;
   - displaying prompts for camera photograph;
   - acquiring camera photos;
   - recording a response through apparatus display and user-selectable response;
   - prompting for biometric reader activation;
   - recording biometric fingerprints from two persons on two physical reader devices;
   - time-stamping a first fingerprint and a second fingerprint and electronically determines that the two fingerprints are recorded within a time period;
   - computing an electronic decision about the physical proximity of the two persons based upon a time-stamp of the first fingerprint and a time-stamp of the second fingerprint;
   - merging biometric signatures, from the two persons, with an "agreement document", generating a "signed agreement document"; and
   - outputting the "signed agreement document" to a computing main board.

7. The collecting method of claim 6, wherein the private information includes last name, first name and initial of patient, identifying medical number of patient, and date of birth of patient; and the response includes an affirmative response and a negative response.

8. The collecting method of claim 6 or 7, wherein the time period is 10 seconds.

9. The collecting method of claim 8, wherein the two persons includes a patient and a
witness.
FIG. 1

FIG. 2

camera for visible light

camera for non-visible light

fingerprint scan unit

camera encoder unit

fingerprint template encoder

device key chip

privacy encoder chip

computing main board
Start

Input: Agreement document

Display document

Patient reads agreement document on screen

Prompt for acceptance or non-acceptance

Patient accepts document?

Y

Prompt for photo

Patient waits 3-5 seconds for photo

Prompt for fingerprint confirmation

Prompt for witness fingerprint confirmation

N

Both patient and witness provide fingerprint signatures within 1000ms?

Y

merge signatures from two persons with an "agreement document", and generate a "signed agreement document"

Output a "signed agreement document"

FIG. 3