31st Annual International Conference of the IEEE EMBS
Minneapolis, Minnesota, USA, September 2-6, 2009

Legitimate Data in Remote Monitoring

J. D. Schilling, *Member, IEEE*

***Abstract*—An approach for ensuring legitimate data transfers of an individual within a remote healthcare solution. Biometric traits and networking are discussed for clarification of the approach. In this approach, a biometric solution is identified as a fingerprint scanner for use in a personal area network of the patient's home. Secure data exchange is acknowledged as a potential weakness in the transferring of patient data within this network. Some options are discussed to ensure security of data for the review by the caregiver. Example approaches regarding legitimacy are identified using a pulse oximeter [1], a blood pressure meter, and a weight scale as the remote patient devices in the remote healthcare solution.**

I. Introduction

In determining a remote healthcare solution, questions are asked in response to the legitimacy of the data that is transacted between an acquiring patient device and the computer reaching the caregiver's eyes (see Fig. 1).

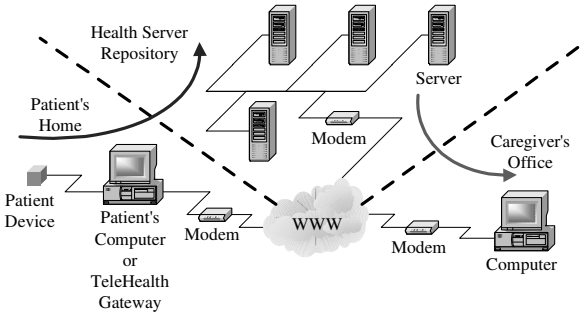

Fig. 1. An example of a typical network for remote healthcare monitoring.

Legitimacy of patient data benefits: the caregiver by continued use of remote monitoring for a treatment plan [2], the third-party service provider by reducing any misdiagnosis and associated liability [3], the insurance company reimbursements and the patient's wellness [4].

Secure websites attempt to ensure that data passed from the patient's computer to the caregiver's computer is not intercepted; however, the focus of this approach will be from the input of the patient device to the output of patient's computer. The patient's computer could be a TeleHealth Gateway such as proprietary hub for collecting remote devices or a cell phone. For this example, a pulse oximeter will be described as the patient's device connected to a computer.

Manuscript received April 7, 2009. This work was part of a Fingerprint Sensor project funded by Nonin Medical, Inc.

J. D. Schilling is a Design Engineer at Nonin Medical, Inc., Plymouth, MN 55441 USA (phone: 763-553-9968; fax: 763-553-7807; e-mail: josh.schilling@nonin.com).

Three reasons legitimacy of the measurements are in question from the computer/gateway and earlier are:

1) *Lack of skill.* While obtaining the measurement by the patient there is risk in improper handling, placement, care of device, and management of the device. An example could be that the user doesn't leave a thermometer in the mouth and under the tongue for the appropriate length of time. A potential solution is the thermometer determines the appropriate time to record and send a single measurement through a cabled or wireless connection to the patient's computer.
2) *Data Manipulation.* While obtaining the measurement by the patient there is risk in the patient's intentional or unintentional act of adjusting the results. An example could be the weight listed on a driver's license. A potential solution is to electronically record the measurement and allow the data transaction to occur only once, but often enough to develop a trend. Additionally, a potential weakness occurs when the patient has access to locally stored files, which have not been uploaded to the server, and are still pending a successful upload. In this weakness, the system designer should observe additional means of encryption.
3) *Patient substitution.* While obtaining the measurement by the patient there is risk that the patient may not the actual patient and that substitution has occurred. An example could be drug screening for sports players requiring clean results for continued involvement in the sport. A potential solution is to embed a biometric fingerprint scanner in the patient device to enable it to record or associate the data to a user's ID for authentication. This advancement helps ensure the data collected is indeed the patient's. As example approaches to patient substitution: a pulse oximeter, a blood pressure meter, and a weight scale are reviewed as a method for patient identification with the inclusion of a biometric sensor.

II. Background

Entrusting that the network extending outside of the patient's home is secure, the legitimacy of data is now a higher concern for networks confined to the patient's living space as the patient provides direct influence to the patient device.

Remote healthcare monitoring is constructed into 4 levels of networks for data collection: the highest level shown as the **W**ide **A**rea **N**etwork representing the **W**orld **W**ide **W**eb or the cloud; the next level down is the **L**ocal **A**rea **N**etwork

representing the telehealth device or Computer/Gateway and Modem; following this is a **P**ersonal **A**rea **N**etwork representing the telehealth or Computer/Gateway and the Patient Device; and at the lowest level is the **B**ody **A**rea **N**etwork representing multiple Patient Devices that are interconnected.

At the point that the network enters the home and breaks into small networks like a PAN or BAN is where identity access management for data collection becomes the concern.

Biometrics as it relates to identity access management is the gathering and recognition of intrinsic behavioral or physical traits.

TABLE I
RANKING OF BIOMETRIC TRAITS

Biometric	Unique	Permanent
DNA	High	High
Fingerprint	High	High
Iris	High	High
Odor	High	High
Retinal Scan	High	Medium
Facial Thermograph	High	Low
Ear Canal	Medium	High
Hand Geometry	Medium	Medium
Hand Veins	Medium	Medium
Face	Low	Medium
Gait	Low	Low
Keystrokes	Low	Low
Signature	Low	Low
Voice	Low	Low

Four traits stand out as potential candidates for identity access management. These traits are Iris, Odor, DNA, and Fingerprint. At the time of this article's writing, DNA has not undergone automation as is too lengthy of a process for use as an immediate recognition [6]. Odor is still in investigation as well [7]. As individuals age, conditions such as glaucoma [8] and obstructions like eyelashes [6] may make it more difficult for scanning of the Iris. Fingerprint scanning is unique and permanent [5] and relatively simple [6] for patient's to learn.

III. CONSIDERATIONS

Unencrypted objects from the patient device may leave room for security risk. While security is provided for the transfer protocol, a trait such as a fingerprint if linked to the patient information object could act as a key for transmission of the patient information from the patient device to the patient's computer. If the data isn't encrypted by the patient device, then the patient's computer could encrypted the data as it is received alternatively.

Encryption may help in preventing the data from being modified locally in the event that the pathway isn't available from the patient's computer to the WAN. The fingerprint itself could be used as the key, thus allowing the fingerprint to be secret upon delivery of the data to the caregiver's computer (Fig. 2). The caregiver would require the patient's fingerprint to successfully unlock the patient's data stored on the web server's repository.

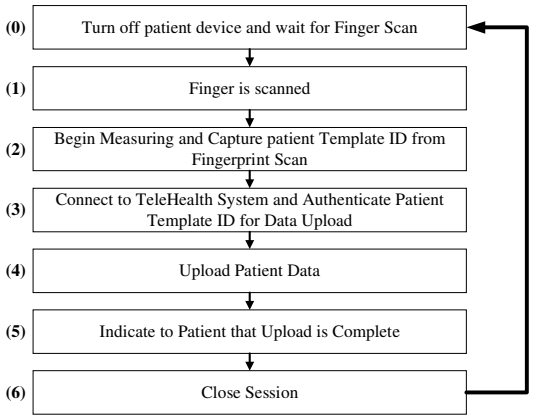

Fig. 2. An example flow of the authentication for a patient's device.

Though patient substitution may not always impossible to counteract even with biometrics, some key points will make patient substitution more difficult.

A camera connected to the telehealth device could assist the nurse or caregiver in helping further identify that the patient is actually taking the measurement after a successful scan of the finger. The camera may feel like an invasion of privacy to some, so some other methods are further discussed here in regards to the design and implementation.

Assuming there is risk, the issues are mitigated by:

1) *Reaction time.* This will be the time that the patient is given between scanning their finger and recording data. Once the finger has been scanned, if the patient is not recording data or breaks the recording of data with a slight pause or delay in measurements then the patient must rescan the finger.
2) *Sign In / Sign Out.* The patient is required to take a measurement by inserting their finger into a scanner and not allowed to remove it until after the measurement. The sensor could contain a capacitive sensor that recognizes when the finger is resting on the scanner and when it has been removed.
3) *Location.* The sensor is placed in a location that is most accessible to the patient using the patient device. The fingerprint sensor could be placed on a blood pressure cuff, on a thermometer, on a remote sensor placed for a weight scale, or inside or outside of a pulse oximeter sensor.

IV. BIOMETRIC INTEGRATION EXAMPLES

A. Pulse Oximeter

Homecare monitoring of chronic obstructive pulmonary disease (COPD) patients and long term oxygen therapy (LTOT) patients may result in a pulse oximeter being used. A pulse oximeter measures the percentage of oxygen bound to the hemoglobin in red blood cells by the circulation of the blood. A pulse oximeter can be used on multiple sites like the ear lobes, forehead, tongue, and the fingers. For TeleHealth, the finger is typically used for ease of use to the

patient.

The oximeter sensor and fingerprint sensor can be separate from the processing unit or attached as a dual sensor. As noting from the considerations in section III, the fingerprint sensor could be on the inside of the sensor design. This would help simplify the instructions to user, and provide a reliable method of ensuring the patient retains the sensor after authentication.

Fig. 3. A typical pulse oximeter sensor.

A pulse oximeter, when used with the finger (Fig. 3), could be placed on any of the patient's fingers. This is unique to a pulse oximeter as other patient devices typically do not rely on the finger and could be specific to one as it relates to biometrics. To make a versatile pulse oximeter, templates for each finger would need to be stored. Because the fingerprint scanner scans as the finger is inserted and un-inserted, the image is reversed upon removal of the finger from the sensor (Fig. 4). Thus, if dual authentication was required then two templates minimum would be required for every finger.

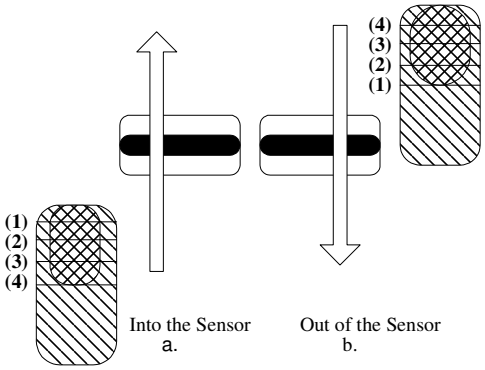

Fig. 4. The image acquisition process as the finger enters and exits the sensor. a) Into the Sensor - as the finger slides across the biometric scanner, the image is read starting at 1 (tip of the fingerprint) as the first part of the image. b) Out of the Sensor - as the finger slides across the biometric scanner, the image is read starting at 1 (base of the fingerprint) as the first part of the image.

Each image could increase cost because of the increase in the amount of templates is directly related to the increase the amount of memory required for data storage. The device could be limited to one finger, but if a deformity occurs such as the user cuts their finger then another sensor site might increase usability.

To ease the implementation, these templates could be stored on the TeleHealth or computer device in addition or as an alternate option to the pulse oximeter. If this was in addition, then this would just require the connecting device to transmit the image identifier (possibly a patient identification number) for finger placement and whether or not the finger was being inserted. Assuming direction was known from a power-up state, one of the images could be interpolated and checked against the other. Due to potential increases in power consumption, image analysis could be done at the TeleHealth or computer system.

For a wireless device with external storage only versus internal storage, might also decrease overall battery life due to the patient device transmission of the full fingerprint image. In this case, a local analysis may be better suited with a patient identifier for transmission depending on how often the sensor is used.

As each finger contains a specific biometric template, a determination of which finger being measured for pulse oximetry reading may prove useful. The caregiver would be able to control where the measurements are taken from if certain sites proved difficult.

B. Blood Pressure

Homecare monitoring of congestive heart failure (CHF), hypertension (high arterial pressure) or hypotension (low arterial pressure) may result in an electronic sphygmomanometer (blood pressure meter) being used. A blood pressure meter (Fig. 5) measures the pressure in the veins by the circulation of the blood. For TeleHealth, this is typically the brachial artery in the upper arm.

Fig. 5. Blood pressure meter.

Similar to the Pulse Oximeter, a blood pressure meter typically will have the probing instrument separate from the meter. Unlike the pulse oximeter, the finger is not the site required for the measurement.

The finger would need to be lifted from the sensor to complete the capture of the fingerprint. This is more of a concern for this example as there is no way to prevent the finger from being removed during the measurement; however, a solution might be to place the fingerprint scanner on the surface of the meter and provide two capacitive sensors.

One capacitive sensor could be part of the fingerprint sensor and a second part of the button for enabling the blood pressure measurement. As the finger slid over one it would land on the second and the measurement would start. The

meter would cancel the measurement in process if the finger was removed early.

C. Weight Scale

Homecare monitoring of congestive heart failure (CHF) may result in a weight scale (Fig. 6) being used. A weight scale is used to measure a patient's weight.

Fig. 6. Typical weight scale.

Similar to a Blood Pressure the finger is not the site required for the measurement. Unlike the Blood Pressure, the weight scale is the meter and performs the measurement.

As it would not be convenient for the patient to kneel down to swipe their finger, a remote sensor connected wirelessly or wired to the weight scale may help in operation. The patient would be required to hold their finger in place similar to the blood pressure meter to acquire a measurement.

Though the toes could be used for fingerprinting, this assumes that the patient is barefoot. Fingerprinting of the patient's finger should result in a larger amount of use cases where the patient is required to take their weight midday.

V. Conclusion

Overall the concept of biometrics provides an added confidence to the legitimacy of the transferred data and a potential mechanism for patient privacy of health information between the patient and the clinician. Its simplicity, given the right mechanical design should be easiest enough that a large learning curve by the patient isn't required. This concept can be applied to any patient device in a remote healthcare solution to a TeleHealth gateway.

References

[1] G. Tschautscher; J. Parthasarathy;"Sensor and system providing physiologic data and biometric identification" U.S. Patent Pending, Application 20090043180, August 8, 2007

[2] L. Schlachta-Fairchild, V. Elfrink, A. Deickman "Patient Safety, Telenursing, and Telehealth", Patient Safety and Quality: An Evidence-Based Handbook for Nurses: Vol. 3

[3] F. F. Rahman , Healthcare – Research Analyst, Frost & Sullivan (24 Jan 2005) "Keys Issues of Remote Patient Monitoring", Frost & Sullivan Market Insight (http://www.frost.com/prod/servlet/market-insight-print.pag?docid=31225662)

[4] R. E. Litan , October 24, 2008 "VITAL SIGNS VIA BROADBAND: REMOTE HEALTH MONITORING TRANSMITS SAVINGS, ENHANCES LIVES" Better Health Care Together (www.betterhealthcaretogether.org)

[5] A.K. Jain; A. Ross; S. Prabhakar (January 2004), "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology 14th (1): 4 – 20

[6] National Science & Technology Council's (NSTC) Subcommittee on Biometrics (Sept. 7 2006). "Biometrics Frequently Asked Questions" National Science & Technology Council's (NSTC) (http://www.biometrics.gov/Documents/FAQ.pdf)

[7] Z. Korotkaya "Biometric Person Authentication: Odor" Department of Information Technology, Laboratory of Applied Mathematics, Lappeenranta University of Technology (http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf)

[8] A. Davis, (July 1997) "The Body as Password" Wired Magazine (http://www.wired.com/wired/archive/5.07/biometrics_pr.html)

[9] P.S. Seibert, T.A. Whitmore, C. Patterson, P.D. Parker, C. Otto, J. Basom, N. Whitener, and C.G. Zimmerman (Oct. 28 2007). "Telemedicine Facilitates CHF Home Health Care for Those with Systolic Dysfunction" Internation Journal of Telemedicine and Application (http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2274890)