AHRQ Grant Final Progress Report

Title of Project:

Developing a Medical Biometric Identification System with a Secure Database Network That Can Access Electronic Medical Databases

Principal Investigator

Jason W. Sohn, Associate Professor, Department of Radiation Oncology

Team Members

Haksoo Kim, PhD, Department of Radiation Oncology, Case Western Reserve University

Samuel Park, PhD, Department of Radiation Oncology, Case Western Reserve University

Organization:

Case Western Reserve University

Inclusive Dates of Project: April 1, 2010 – January 31, 2014

Federal Project Officer

Dr. Kerm Henriksen

Acknowledgement of Agency Support: The project described above was supported by grant number 5 R18 HS017424; its contents are the responsibility of the authors and do not necessarily represent the official views of the Agency for Healthcare Research and Quality.

Grant Number: 5 R18 HS017424

Developing a Medical Biometric Identification System with a Secure Database Network That Can Access Electronic Medical Databases

Table of Contents

Developing a Medical Biometric Identification System with a Secure Database Network That Can Access Electronic Medical Databases

Purpose: Our project encompasses developing a patient identification and treatment procedure verification system using fingerprints, which calls up existing hospital applications, such as treatment Record and Verification (R&V) systems or Picture Archiving and Communication (PAC) systems, following correct patient identification without human interactions, thus lowering the possibilities of medical errors.

Scope: The patient identification and procedure verification is a well-known problem in the medical industry. The number of serious or even fatal consequences is growing. The Joint Commission recommends improving the accuracy of patient identification by using at least two patient identification methods. Unfortunately, the most popular identifier, wristbands, is proving to have an unacceptable error rate. These misidentifications can lead to a medical misadministration and fall under the category of a 'sentinel event.' Our developed system can eliminate most problems associated with wristband systems while helping clinics meet the goals set by The Joint Commission.

Methods: Our patient identification system uses an optical fingerprint scanner for biometric data collection, creates a database of fingerprints and images, and interacts with the established clinical patient databases. To create an identification database, our system captures a photograph using a web camera; stores two fingerprints or more; and records brief patient identification information, such as name, date of birth, etc. During an identification process, our system accepts a fingerprint, identifies the patient, verifies with a second fingerprint, and opens the correct patient record in the R&V database.

Results: The system has been successfully developed and implemented in both Radiation Oncology and Surgery. We have currently recruited and processed 73 patients and will continue on to our goal of 600, which we anticipate completing in 2016. For a quality level set to 30%, there is a 33% failure to match and, most importantly, 0% false positives. We tested and recommend using a newer scanner that acquires both fingerprints and finger vein patterns for biometric matching data to reduce the database match failure rate. Older patients (over ~75 years old) tend to have poor-quality fingerprints, as features erode with time. This accounted for most of the failed matches and the enthusiasm for the finger vein scanner and possibly a palm scanner.

Key Words: Patient Identification, Fingerprint

Purpose

The goal of this grant was to develop a fingerprint-based patient identification system to minimize misidentification of patients, particularly for procedure verifications. Optical fingerprint scanners can identify a patient's fingerprints quickly and with exceptional accuracy using proven pattern recognition algorithms. Once a patient is correctly identified, our system can call up existing hospital applications (e.g., treatment Record and Verification (R&V) systems or Picture Archiving and Communication (PAC) systems) to display patient detailed information. Outcomes of this grant include:

- Develop a patient identification system using patient fingerprints for identification and procedure verification
- Develop the multi-layer fingerprint database architecture and construct interfaces between our software and existing hospital databases
- Test the efficacy and accuracy of our system in clinical departments

These outcomes will be of benefit to researchers and hospitals who are directly involved in developing and implementing patient identification system/procedures to minimize misidentification of patients.

Scope

Background and Context: The patient identification and procedure verification is a well-known problem in the medical industry. The number of serious or even fatal consequences is growing. The Joint Commission recommends improving the accuracy of patient identification by using at least two patient identifiers[1]. Unfortunately, the most popular identifier, wristbands, is proving to have an unacceptable error rate. We are proposing a new biometric system using fingerprints to meet The Joint Commission recommendations and minimize error rates. Our system will be designed to interact with established patient databases (e.g., PACS or electronic charts) for highly accurate patient identification and procedure verification.

These misidentifications can lead to a medical misadministration and fall under the category of a 'sentinel event.' A 'sentinel event' is defined by The Joint Commission as "an unexpected occurrence involving death or serious physical or psychological injury, or the risk thereof"[2]. The sentinel report update in December 2001 from The Joint Commission analyzed 126 incidents for root causes and determined that "76% involved surgery on the wrong body part or site; 13% involved surgery on the wrong patient; and 11% involved the wrong surgical procedure." Of the 126 incidents, only 81% were self-reported[2]. The Joint Commission goes on to point out that wrong-site surgery data collected by other organizations suggested a significant amount of under-reporting to The Joint Commission.

The Joint Commission analyzed the causes of misadministration in 2005, as illustrated in Figure 1 [3]. The lack of communication, patient assessment, and availability of information caused 113 'wrong surgeries.' The number of wrong surgeries still increases every year, as shown in Figure 2 [3].

The 'two patient identifiers' specified by The Joint Commission have a two-fold purpose: first, to reliably identify the individual and, second, to match the service or treatment to that individual. The identifiers

may be in the same location, such as a wristband. They must be directly associated with the individual, and the same two identifiers must be directly associated with the treatments or procedure. It is the person-specific information that is the "identifier," not the medium on which that information resides. The 'two-identifier' requirement also applies to an 'order for care' and to report critical test results. Wristbands systems are the most common patient identifier in use. These identifiers play an important role in The Joint Commission protocol to reduce surgical misadministration.

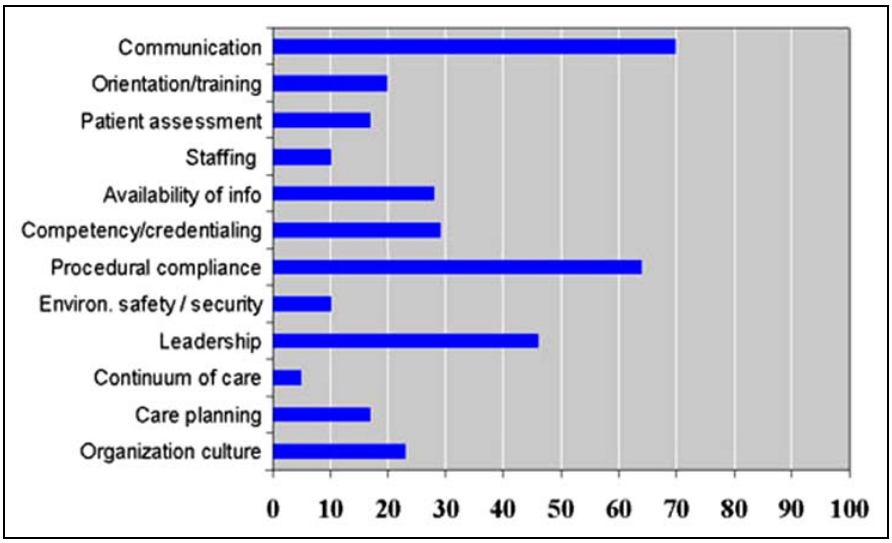


Figure 1. Root causes of wrong-site surgery in 2005, as reported by The Joint Commission

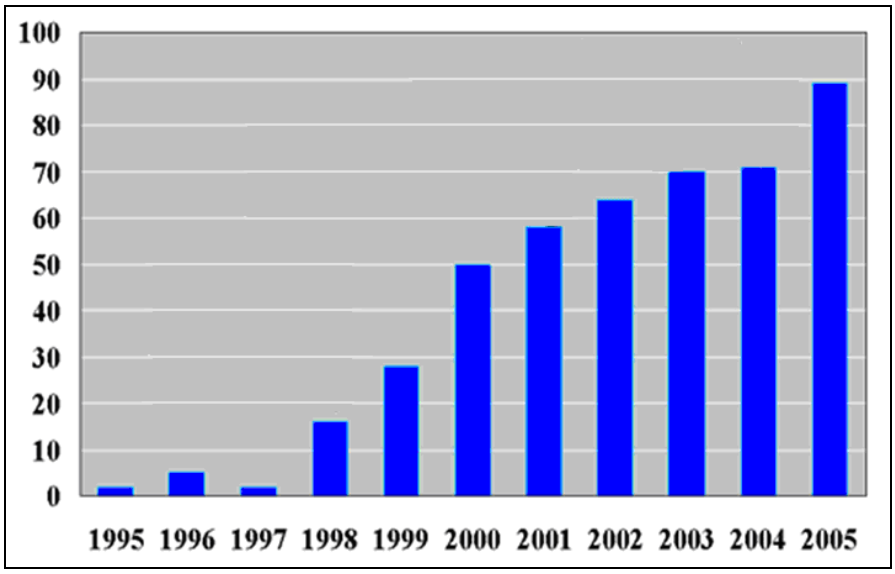


Figure 2. Sentinel event trends report showing the number of wrong surgeries increases every year

Effective July 1, 2004, compliance with the Universal Protocol for Preventing Wrong Site, Wrong Procedure, Wrong Person Surgery has been required of all The Joint Commission accredited organizations, to the extent that these requirements are relevant to the services provided by the organization. An important concept is the "Time Out" quality check now used in procedures. In addition to patient, procedure, and site verification, the "time out" must include verification of correct patient position and availability of correct implants and any necessary special equipment.

The "time out" must be documented. This protocol and its implementation guidelines apply to all operative and other invasive procedures that expose patients to more than minimal risk, including procedures done in settings other than the operating room, such as a special procedures unit, endoscopy unit, or interventional radiology suite. In addition, procedures that involve puncture or incision of the skin, or insertion of an instrument or foreign material into the body, including but not limited to percutaneous aspirations, biopsies, cardiac and vascular catheterizations, and endoscopies, are within the scope of this protocol.

There are a few competing technologies for patient identification, namely barcode and radio frequency identification (RFID) chips. RFID can be used to track the patient's location and extract patient information using a remote scanner [5-7]. However, RFID has a weakness in security, because it can be read with an illegitimate remote scanner. This issue has been reported by experts [8, 9].

Barcode or RFID chips can be taped on patient wristbands. However, their effectiveness of identifying patients is not convincing. There are two critical studies of the barcoded wristbands, which have a significant pool. The first study was reported by the State University of New York, Downstate Medical Center in Brooklyn, NY[10]. The wristband error rates were tracked over a 2-year period. During the 2 years, wristbands were examined 1,757,730 times, and 45,197 wristband errors were found. The mean wristband error rate for the first quarter was 7.4%. However, by the eighth quarter, the mean wristband error rate had fallen to 3.05%. Even with this improvement, sentinel events continued to rise, as shown in Figure 2.

The second study (as mentioned in Specific Aims) was conducted at the Veterans Affairs Medical Center in West Los Angeles, CA, and compared wristband identification errors for 712 hospitals. Phlebotomists checked patient wristbands on 2,463,727 occasions, finding 67,289 errors[10]. Ten percent of the hospital participants had error rates of 10.9% or greater. The researchers found that patient wristbands were missing entirely in 33,308 instances, which represented 49.5% of errors. Multiple wristbands with different information occurred 8.3% of the time; wristbands with incomplete data, 7.5%; wristbands with erroneous data, 8.6%; wristbands with illegible data 5.7%; and patients wearing wristbands with another patient's identifying information, 0.5% of the time.

Proposal

Our proposed biometric identification system will eliminate most of the problems associated with wristband systems while helping clinics meet the goals set by The Joint Commission.

First: Patient misidentification is limited to the failure rate of fingerprint identification, which is approximately one out of a billion (provided the patient can offer two fingerprints).

Second: With our proposed system, procedure verification can be performed biometrically by interacting with the relevant patient database, such as an electronic chart or PACS system.

Third: Fingerprints are not subject to loss, damage, or switching between patients in the same way as plastic wristbands. Multiple records for one patient can be prevented, because there is one set of unique biometric information[11, 12].

Fourth: Patient privacy is maintained, particularly for outpatients who wish to keep their status private by not wearing wristbands.

Fifth: This system can be used to identify and provide patient vital information to clinicians when a patient is not able to provide his/her information. Patients who are suffering from Alzheimer's, unconsciousness, bad hearing, or language difficulty can take advantage of this technology.

Sixth: Our system can be used with other biometric systems (e.g., retinal scanners) by integrating their drivers and pattern recognition algorithms.

Participants: The department of Radiation Oncology and Surgery in University Hospital of Case Western Reserve University participated. There were 73 patients in total at the time of this report.

Methods

Our Biometric Automated Patient Identification Systems (BAPIS) uses an optical fingerprint scanner for biometric data collection, creates a fingerprint database, and interacts with the established clinical patient database. To register a patient, the BAPIS captures a photograph using a web camera, stores at least two fingerprints, and records brief patient information (e.g., name, date of birth, allergic information, etc.). During an identification process, the BAPIS accepts a fingerprint, identifies the patient, verifies with a second fingerprint, and opens the correct patient record in the R&V database, as shown in Figure 3.

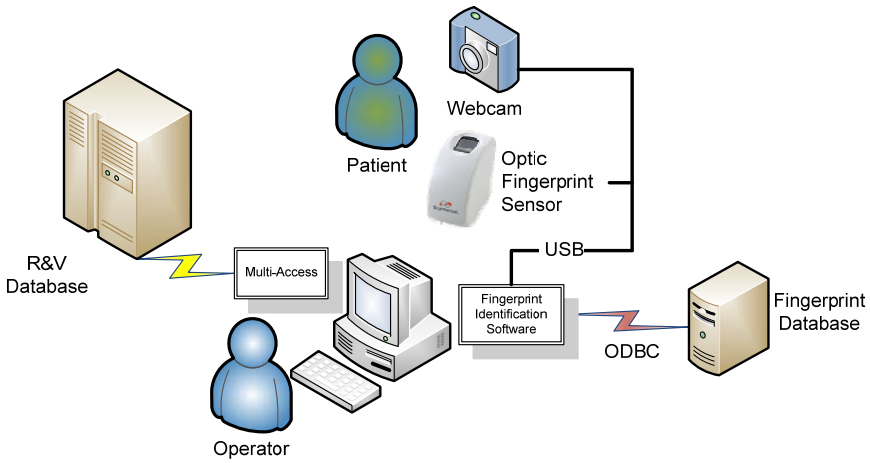


Figure 3. Schematic of the Biometric Automated Patient Identification System (BAPIS)

Hardware

The hardware consists of a personal computer, an optical fingerprint scanner, and a web camera. They are connected via universal serial bus (USB) cables. The optical finger scanner is the model SFR300-S, Biomini (Suprema Inc.) It has a 500 dpi/256 gray scale optical fingerprint sensor in a plastic case.

The scan window is 16 mm x 18 mm. Its physical dimension is 40 mm (width) x 77 mm (length) x 70.5 mm (height). Scanning time takes less than a second. The web camera used in an inexpensive LifeCam by Microsoft.

Software

Our program is written in Microsoft Visual C++. Each patient record in the fingerprint database consists of ID, the maximum 10 fingerprint templates, allergic information, date of birth, a photo image, a phone number, and a hospital record ID. Each scanned fingerprint has key information extracted and stored in a proprietary format (about 368 bytes per scan, stored in 256 bit AES encryption)[13].

The BAPIS is connected to the fingerprint database using Oracle to query patient information. The Oracle database is installed on the Linux server, which is located in the server room of the hospital. While identifying a patient, a scanned fingerprint is sent to the fingerprint matching application that is being run on the Linux server. The fingerprint matching application checks the scanned fingerprint from the Oracle database, and then the matching result is sent to the BAPIS. Figure 4 shows the logic flowchart of the identification process. During actual use, the patient has one fingerprint scanned, the system identifies a patient (about 1 sec / 1000 records to search), and the patient photograph is displayed. To reduce the false-positive error rate, the BAPIS utilize two-phase identification process. The first phase scans the first fingerprint. If it is successfully checked, then the second phase will automatically start. If a single fingerprint of a patient is registered, the BAPIS will bring the patient information with the single fingerprint. Otherwise, the second fingerprint should be checked. In the second phase, the BAPIS tries to check the scanned second fingerprint. If it is successfully checked, the found patient information is shown, and the user has to check whether the patient is correct using the face photo.

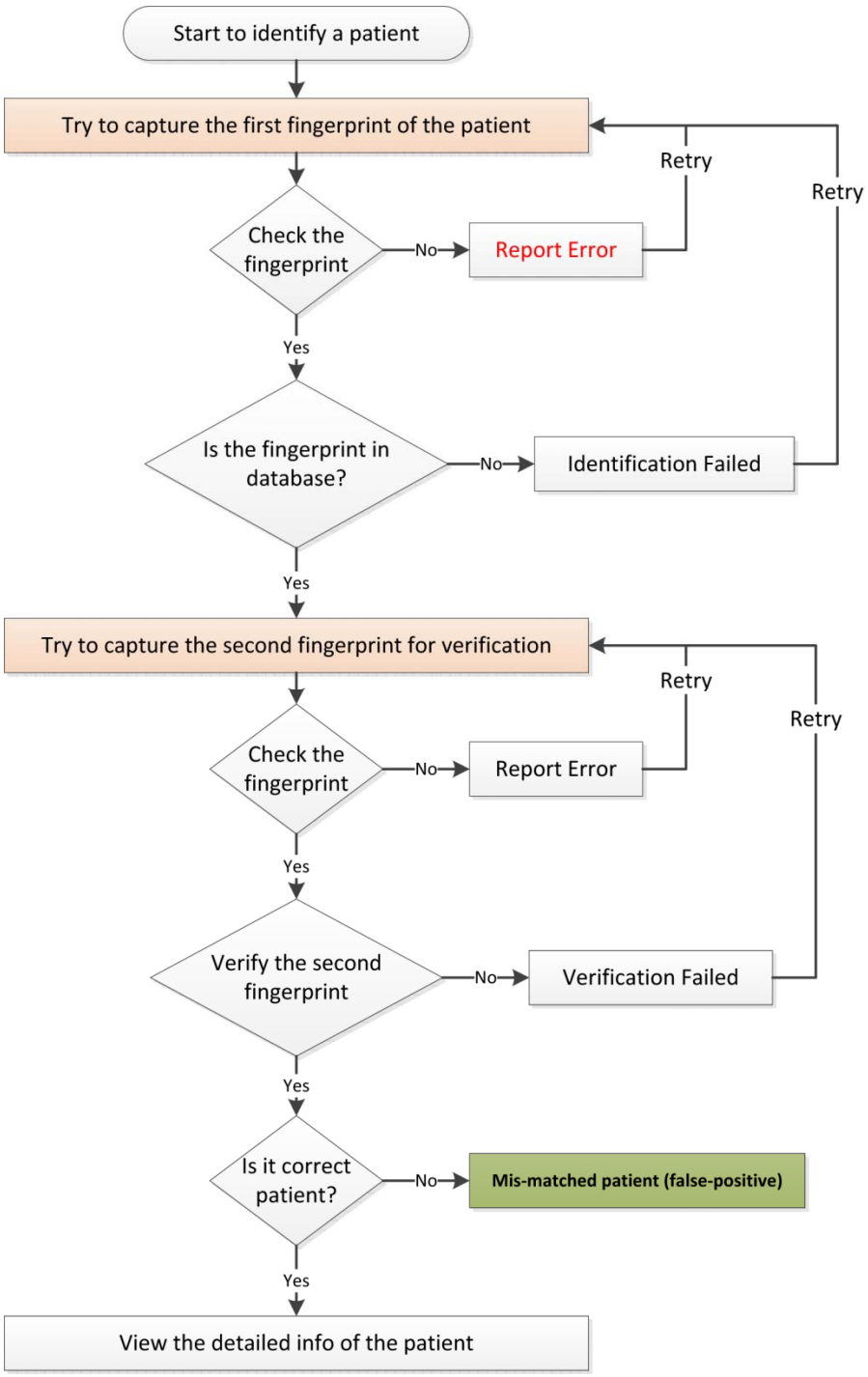


Figure 4. The flowchart of the identification decision process of the BAPIS.

The BAPIS is designed to interact with different databases using a modular approach. The current module interacts with the existing hospital applications (electronic charts (Mosaiq) and PACS). Once the patient is found, by clicking "call Mosaiq" or "call PACS," the patient chart is called up using the connected hospital ID.

Results

We summarized studies that are proposed in the initial proposal to achieve above aims and analyzed the statistic of identifying patients with fingerprints.

Study 1 – Analyzing human factors to design an intuitive user interface for routine clinical user

We performed human factor analyses of the operating system functions, the intuitive user interface, and hardware interaction. For an example, as shown in Figure 5, our system's Graphical User Interface (GUI) is designed similar to a web interface, so that users can intuitively get into desired tasks, such as "Patient Identification Process," "Patient Management," "System User Management," and "Personal Information."

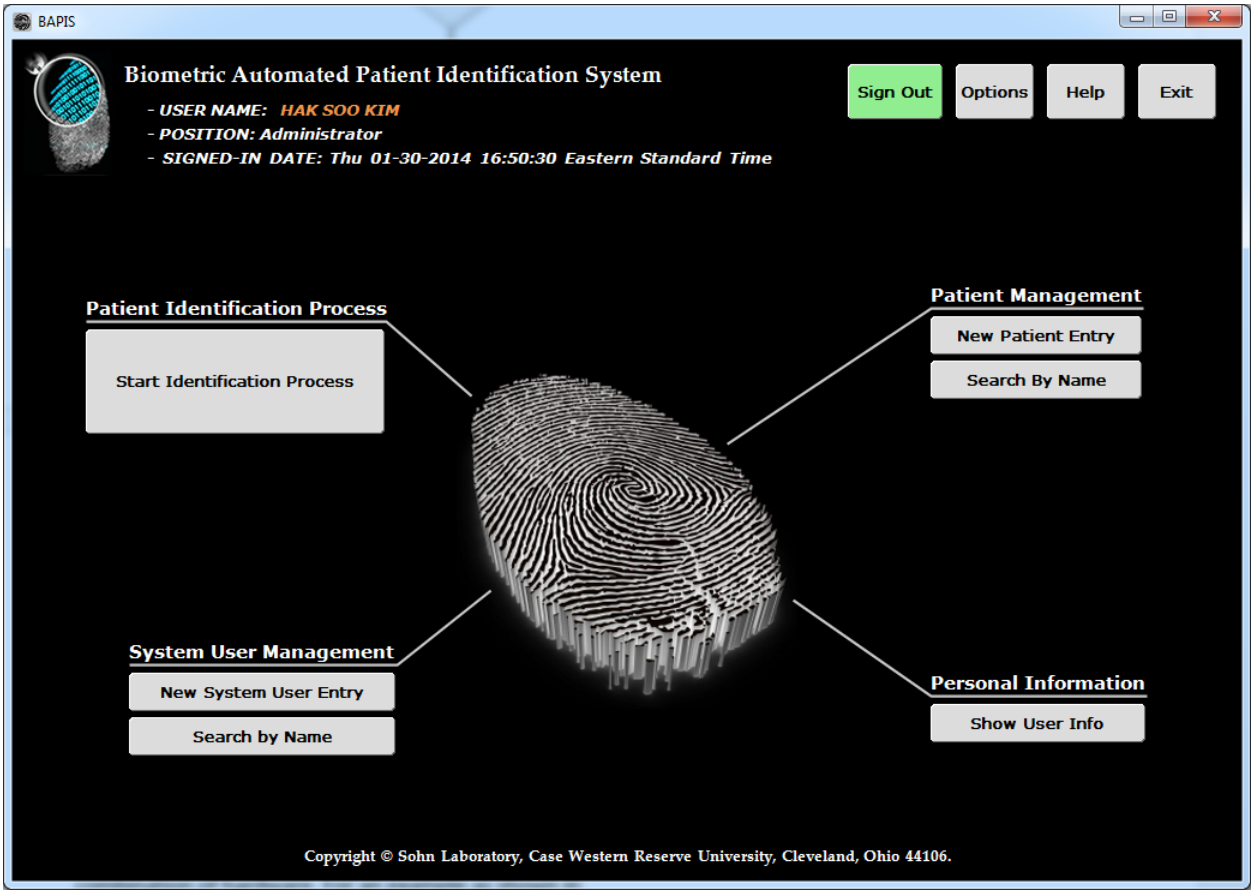


Figure 5. The fingerprint based patient identification system

Study 2 – Modeling authorized user accounts and privileges to protect patient information

To protect the personal information of patients, we designed various authorized users rights to control access to our system. As shown in the yellow box of Figure 6, all the users have a triple security policy (ID, PASSWORD, and FINGERPRINT) that protects the system from being accessed by unauthorized users. The modes of users are created according to their privileges (the red box of Figure 6), accessing patient data and care, such as creating/updating/deleting a patient in our system, identifying an existing patient, and managing system users as a system manager. With various clinical scenarios, we tested

these models in our lab prior to clinical trials. Currently, this model is installed on the hospital computers for clinical trial.

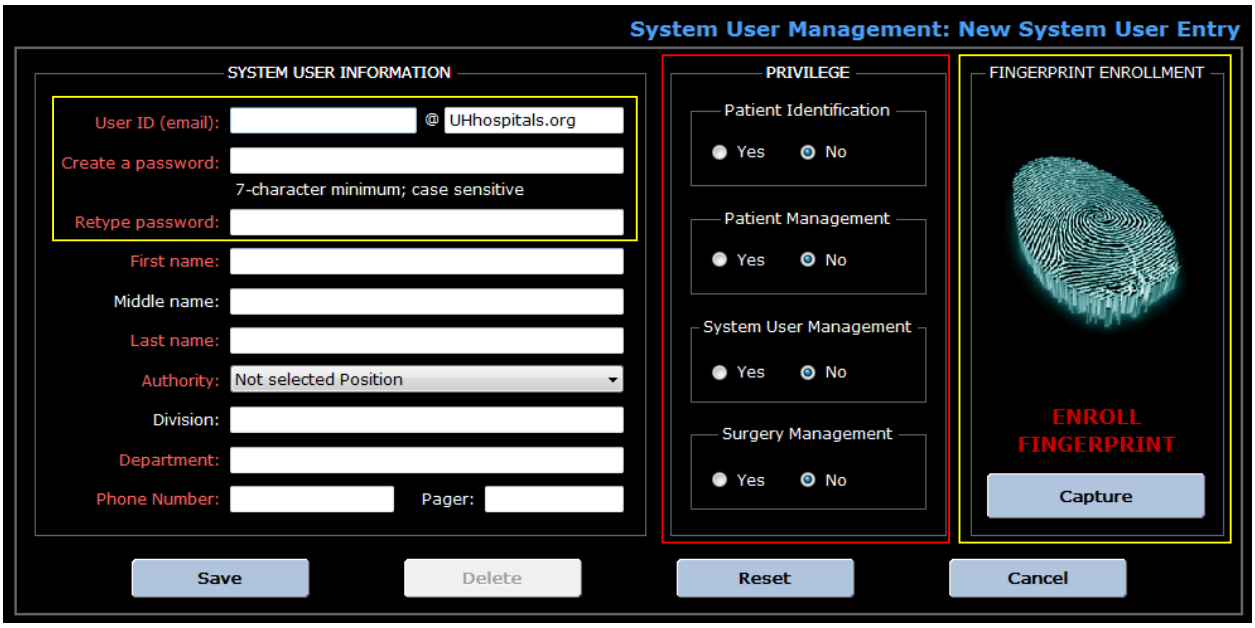


Figure 6. Graphical user interface to register a new system user

Study 3 – Developing a patient identification system for radiation therapy and surgery departments

We developed a patient identification system that identifies and manages the information of patients by scanning their fingerprints, as shown in Figure 7. This system stores patients with the maximum 10 fingerprints in the patient database, as shown in the fingerprint enrollment of Figure 7. Patients do not have to use an ID and Password, unlike authorized users. They interact with our system using only their fingerprints. The identification process that automatically identifies a patient by fingerprints has two steps: 1) identification step that finds a patient with the first scanned fingerprint, and 2) verification step, which verifies the identified patient by scanning another finger. Through these two steps, our system can reduce the errors associated with the fingerprint scanning.

In addition, we developed a surgery procedure verification component within the system, as shown in Figure 8. This allows a surgeon to create a procedure/orientation verification display, consisting of an anatomical sketch, procedure description, and digital image of the patient in treatment position prior to surgery. At the time of surgery, the two fingers of a patient will be scanned and identified, and then our system displays the anatomical sketch, procedure description, and reference photo of the patient. The reference photo is taken in the pre-op room with the patient in correct orientation for the procedure. Images can also be acquired in the operating room and added to the database for documentation.

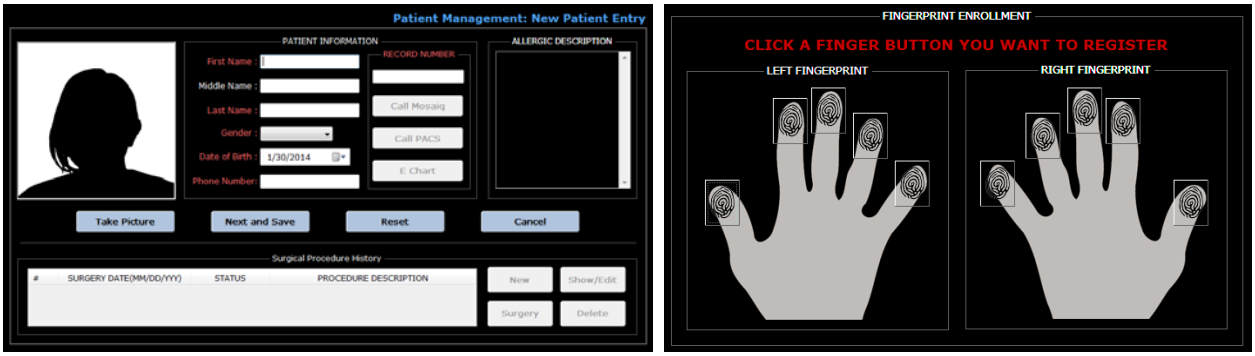


Figure 7. Graphical User Interface to register a new patient

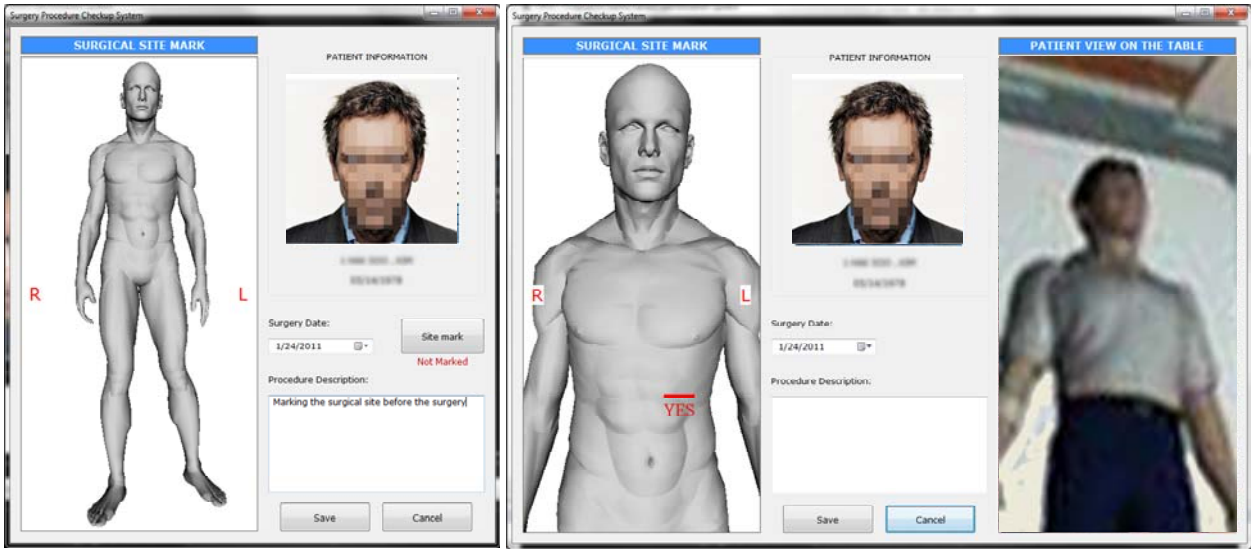


Figure 8. The surgery procedure checkup system: i) the left panel shows the 3D human model before marking for surgery, and ii) the right panel shows the marked 3D model and a reference photo of the surgical patient in correct orientation for the surgery (taken in pre-op).

Study 4 – Developing and integrating modules for connecting to hospital applications

We developed a module interacting with the radiation oncology R&V database Multi-Access (Mosaiq, Elekta Inc.) and PACS, as proposed. After "Call Mosaiq" or "Call PACS" is clicked by a user, as shown in Figure 9, our software sends the medical record (MR) number to the Mosaiq or PACS software using keyboard emulation allowed in Microsoft operating systems. After submitting our alpha version system to our human factors consultant, we modified and released our beta version system to the clinic. We then modified the human interaction to our software based on the feedback from clinicians, staff, and second human factor analysis involving the patient identification interface.

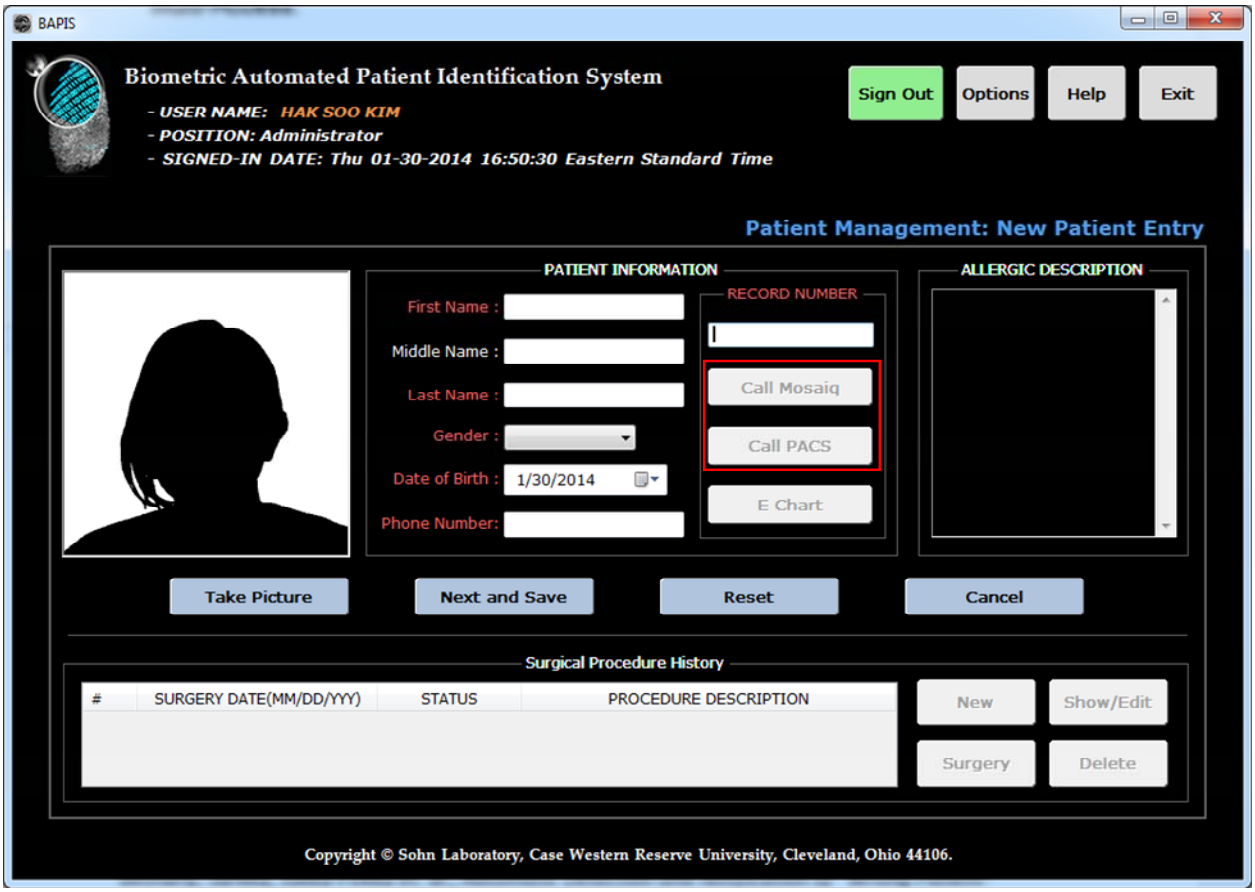


Figure 9. Module interacting with the radiation oncology R&V database Multi-Access

Study 4 – Designing and implementing modules for safety and data monitoring

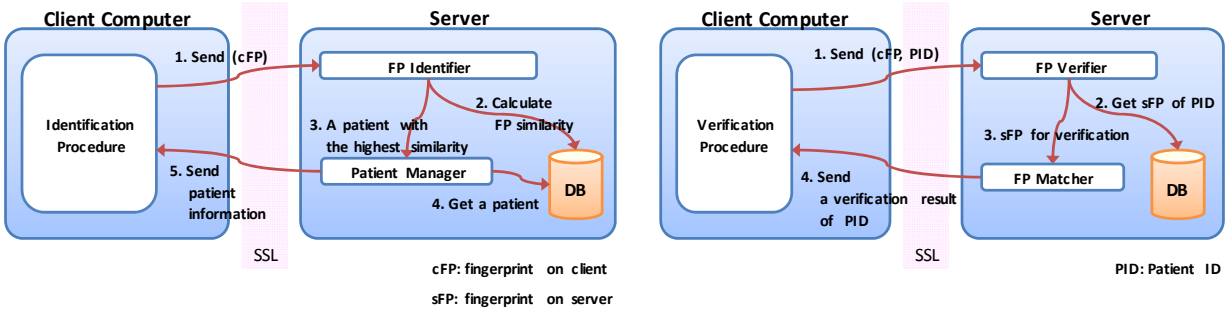
We implemented all aspects of data safety consideration. We collaborated with IT department of University Hospitals (UH) to maintain the information security and PHI protection in accordance with HIPAA regulations. All operations using our system handling patient information are automatically recorded in encrypted database log files. PI is monitoring the log files weekly basis. We developed a software tool to review log files using JAVA framework. The server is protected in a locked server room of UH.

Study 4 – Building secure communication between fingerprint identification servers

We developed an interface messaging framework using the Secure Socket Layer (SSL) protocol for secure communication between fingerprint identification servers. The SSL protocol allows client applications and servers to communicate over a secure network by using public key cryptography, which is based on key pairs (public and private keys). All the messages on the network are encrypted to the recent version of SSL (version 3). Figure 10 indicates our identification and verification procedures to search patient's identification from the patient database in the server. The client can get the detailed information of the found patient identification from the patient database.

"Client" is a computer inquiring patient ID to another computer. Moreover, our developed system adopted a one-time password strategy to block illegal access from unauthorized users. It will prevent reuse of the database connection information in the client application memory.

After the client sends the user information (login ID, password, and fingerprint) to the server, our server managing program generates a one-time use password for the client, allowing a one-time connection to the database in the server. Each inquiry from a client requires a new password from the server managing program. These procedures are automatically performed. The entire system is behind the UH firewall.



(i) Identification procedure (ii) Verification procedure

Figure 10. Identification and verification procedure based on SSL: All messages are encrypted by public key cryptography to protect patients' information.

Study 5 – Layered multi-database architecture and Load balancing strategies to accelerate fingerprint matching

We developed a multi-database system that can be expanded to multi-hospital networks. This architecture consists of root/intermediate nodes as the identification server and leaf nodes as the patient database server, as proposed. When a patient identification is requested to the root server, it is distributed to child identification servers. The child server managing program searches the patient information in its database. The child server passes the encrypted identified patient information to the root identification server, as described in the previous study. This procedure is illustrated in Figure 11. We implemented a load balancing server to accelerate fingerprint matching by distributing the processing overload to virtual fingerprint identification servers, as proposed.

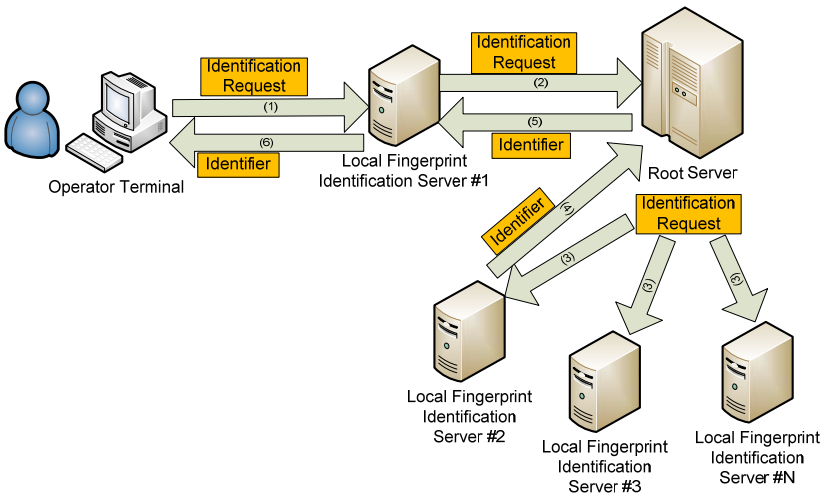


Figure 11. Procedure of transferring fingerprint identification request in multi database systems. Each local server only needs to have trust relationship to the root server.

Statistical Analysis

In the proposal, we planned to recruit a minimum of 600 patients per our radiation oncology clinic and the surgery department. We ran into unexpected problems in recruiting patients to test our system. However, we will continue to collect new patients and data in our clinics.

In total, 73 patients have been tested with our patient identification system. Table I shows the statistic of the identification, verification, and false-positive identification per patient. When capturing fingerprints, the fingerprint image quality is important to extracting the feature points of a fingerprint. This quality setting is directly connected to the success of the fingerprint match rate. The quality setting was changed three times. There are three date ranges. For the first date range, between 6/12/2011 and 10/19/2012, the fingerprint quality of enrollment and identification were set to 70%. In the second date range, between 10/20/2012 and 1/30/2012, the fingerprint quality was set to 30%. Before 1/31/2013, our system could register up to two fingerprints. After 1/31/2013, up to 10 fingerprints could be registered. In the third date range, between 1/31/2013 and the current date, we tested the patient identification using the maximum of 10 fingerprints. Some patients' fingerprints are re-registered due to the change of the system configuration (the maximum 10 fingerprints) after 1/31/2013.

In the first date range, the FP verified count was very low, because the fingerprint quality setting was 70%. When scanning fingerprints, the higher quality resulted in low acceptance rates. The number of the scans for verification increased due to rescans required to pass the quality threshold setting. In the second date range, the FP verified count was higher than the first date range, but the Identified count was 0 in several patients. It was traced to a software bug in generating log files. After this date range, we fixed the software. After lowering the quality threshold setting, the verification performance was improved. In the third date range, the system was very stable, and the verification performance was good compared to previous dates. So far, the false positive (in which the verified patient is not correct) is 0.

Figure 12 shows the bar chart of each date range. We can see that the system becomes optimized.

Table I. The statistics per patient

"1st Finger Identified" column indicates the number of times the patient's first finger scan is successfully identified. "2nd Finger Verified" column indicates the number of times the second finger is successfully identified; therefore, the patient is verified by two scans fingerprints. "False Positive" column indicates the number of mis-identifications of the first and second scanned fingerprints. The gray area indicates that the fingerprint quality of enrollment and identification is set to 70%. The blue area indicates that the fingerprint quality of enrollment and identification is set to 30%. The white area indicates that the maximum number of registered fingerprints is set to 10 and the fingerprint quality of enrollment and identification is set to 30%. In the gray and blue area, the maximum number of registered fingerprints is 2.

Index	Registration Date	Age	Number of Fingerprints in Database	1st Finger Identified	2nd Finger Verified	False Positive
1	6/12/2012	65	2	0	0	0
2	8/27/2012	36	2	36	15	0
3	8/30/2012	82	2	0	2	0
4	9/6/2012	62	2	10	5	0
5	9/10/2012	52	2	9	0	0
6	9/10/2012	59	2	17	15	0
7	9/17/2012	81	2	0	0	0
8	9/19/2012	73	2	30	16	0
9	10/1/2012	61	2	7	4	0
10	10/2/2012	71	2	23	45	0
11	10/8/2012	72	2	1	1	0
12	10/8/2012	74	8	7	11	0
13	10/11/2012	51	2	0	0	0
14	10/17/2012	59	2	2	13	0
15	10/18/2012	78	4	2	7	0
16	10/29/2012	55	10	22	0	0
17	10/31/2012	44	10	20	0	0
18	10/31/2012	35	4	25	0	0
19	11/14/2012	58	6	25	12	0
20	11/15/2012	59	10	41	15	0
21	12/4/2012	51	8	16	19	0
22	12/6/2012	65	6	45	44	0
23	1/9/2013	76	8	0	0	0
24	1/21/2013	62	8	14	14	0
25	4/15/2013	68	1	1	0	0
26	4/19/2013	57	5	0	0	0
27	4/29/2013	72	7	2	2	0
28	5/3/2013	41	7	23	23	0
29	6/10/2013	67	6	25	25	0
30	6/18/2013	59	8	23	21	0
31	7/1/2013	71	7	28	28	0
32	7/2/2013	70	8	22	22	0
33	7/2/2013	74	8	20	20	0
34	7/3/2013	71	7	24	23	0
35	7/3/2013	51	6	3	3	0
36	7/9/2013	68	7	24	23	0
37	7/10/2013	62	8	25	21	0
38	7/11/2013	56	4	9	8	0
39	7/11/2013	53	8	28	26	0
40	7/15/2013	53	6	11	7	0
41	7/23/2013	76	8	20	14	0
42	8/12/2013	53	8	3	3	0
43	8/13/2013	65	8	12	11	0
44	8/13/2013	59	8	1	1	0
45	8/14/2013	52	8	1	1	0
46	9/3/2013	67	2	15	11	0
47	9/3/2013	70	8	2	2	0

48	9/4/2013	56	8	10	10	0
49	9/5/2013	78	3	1	1	0
50	9/5/2013	48	4	15	10	0
51	9/6/2013	49	8	2	2	0
52	9/11/2013	71	8	14	13	0
53	9/12/2013	54	8	3	3	0
54	9/12/2013	72	8	1	1	0
55	9/13/2013	51	8	3	3	0
56	9/13/2013	73	4	3	3	0
57	9/19/2013	60	6	7	7	0
58	9/20/2013	96	5	3	3	0
59	9/26/2013	68	8	43	43	0
60	9/27/2013	51	5	3	3	0
61	10/4/2013	70	5	3	3	0
62	10/9/2013	63	8	16	16	0
63	10/14/2013	34	8	7	7	0
64	10/23/2013	67	7	3	3	0
65	11/1/2013	48	8	3	3	0
66	11/8/2013	51	8	1	1	0
67	11/15/2013	67	8	3	3	0
68	11/18/2013	75	8	2	2	0
69	12/3/2013	58	3	0	0	0
70	12/19/2013	58	3	1	1	0
71	12/27/2013	46	6	3	3	0
72	1/17/2014	70	2	0	0	0
73	1/29/2014	86	4	0	0	0

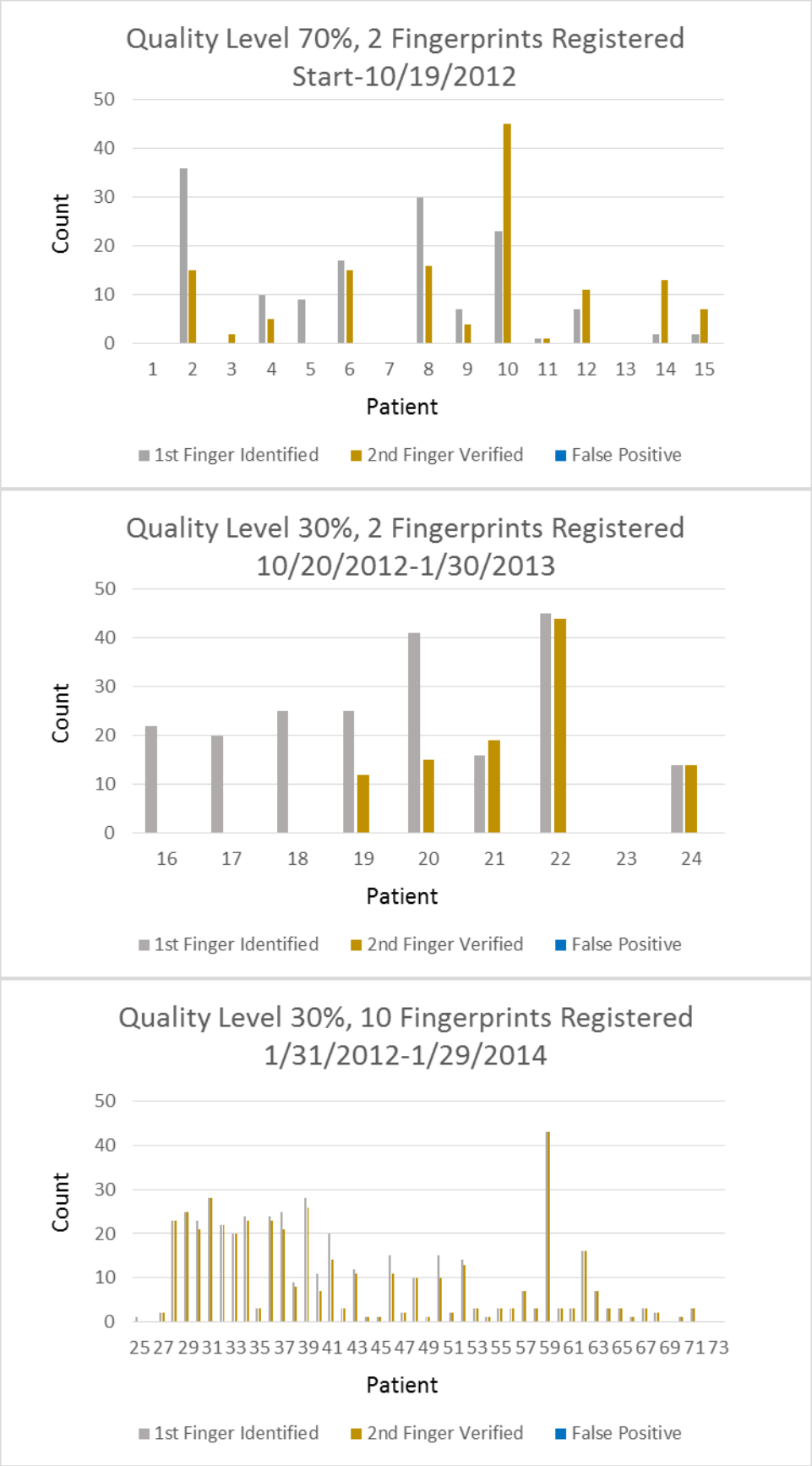


Figure 12. Patient Data Organized By Scan Parameters

Table II. Summary Statistics of Patients Organized By Scan Parameters

	Start Date – 10/19/2012	10/20/2012 – 01/30/2012	01/31/2012 - Current
Fingerprint Quality	Registration Q Level: 70%, Identification Q Level: 70% Using 2 fingerprints	Registration Q Level: 30%, Identification Q Level: 30% Using 2 fingerprints	Registration Q Level: 30%, Identification Q Level: 30% Using 10 fingerprints
Patients	15	9	49
Successfully Identified	144	208	472
Successfully verified	134	104	439
Verification failed	10	104	33
False Positive	0	0	0

Since Jan 31, we have added 10 more patients, and continue to enroll patient this IRB approved study.

Conclusion

We are pleased to report the system is built and works as planned. Both the cancer center and surgical units are using the system successfully. An unexpected difficulty appeared for older cancer patients (~75 and above) , who sometimes did not have fingerprints that can be easily scanned. It should be pointed out that the system did not give false positives but in fact produced no match. This is an important safety feature, because it informs the clinic that the patient at that moment needs to be identified in some other modality (DOB and Name, or wristband). This system is active, an important distinction versus the current methods of identification, which can simply by forgotten. As an example, the patient may not be asked for their name by a busy worker, and this does not stop them from moving forward in the system to a possible mistreatment. But failure to scan in means that no treatment plan is loaded, making treatment impossible. The clinical worker is forced to take action before the patient can move to treatment, making positive identification of the patient an absolute requirement.

The scan success rate for the older patients can be improved with better scanners, as mentioned earlier. As the system is built and operating, replacing and testing scanners is a relatively low cost. We are looking into finding funds to upgrade the scanners and decrease the failed scan rate. There is a fingerprint scanner that is combined with a finger vein scanner, increasing the available data for matching. We think that this device is worth looking at as a way to solve the fading fingerprint issue. There are also palm scanners that take advantage of the larger scanned area.

References

1. Commission, T.J. *2007 National Patient Safety Goals*. [cited 2007 April 17]; Available from: http://www.jointcommission.org/PatientSafety/NationalPatientSafetyGoals/.

2. *A follow-up review of wrong site surgery, Sentinel Event Alert 24*. 2001 [cited 2007 April 17. 2007]; Available from: http://www.jointcommission.org/SentinelEvents/SentinelEventAlert/sea_24.htm.

3. *Sentinel Event Statistics - December 31, 2006*. 2006 December 31, 2006; Available from: http://www.jointcommission.org/SentinelEvents/Statistics/.

4. Jacobson, T.J. and M.J. Murphy, *Optimized knot placement for B-splines in deformable image registration.* Medical Physics, 2011. **38**(8): p. 4579-4582.

5. Hosaka, R., Feasibility study of convenient automatic identification system of medical articles using LF-band RFID in hospital. Systems and Computers in Japan, 2004. **35**(10): p. 74-82.

6. Sandberg, W.S.H., Matti; Egan, Marie; Curran, Paige K.; Fairbrother, Pamela; Choquette, Ken; Daily, Bethany; Sarkka, Jukka-Pekka et. al., *Automatic Detection and Notification of "Wrong Patient-Wrong Location" Errors in the Operating Room.* Surgical Innovation, 2005. **12**(3): p. 253-260.

7. Troyk, P.R., Injectable electronic identification, monitoring, and stimulation systems. Annu Rev Biomed Eng, 1999. **1**: p. 177-209.

8. Rieback, M.R.S., Patrick N.D.; Crispo, Bruno; Tanenbaum, Andrew S., *RFID malware: Design principles and examples.* Pervasive and Mobile Computing, 2006. **2**(4): p. 405-426.

9. Halamka, J.J., Ari; Stubblefield, Adam; Westhues, Jonathan, *The Security Implications of VeriChip Cloning.* Journal of the American Medical Informatics Association, 2006. **13**(6): p. 601-607.

10. Schraag, J. *Patient Identification*. EndoNurse 2006 April 01. 2006; Available from: http://www.endonurse.com/articles/641feat4.html.

11. Neil, Y. and A. Adnan, *Fingerprint classification: a review.* Pattern Anal. Appl., 2004. **7**(1): p. 77-93.

12. Ashbaugh, D.R., *Ridgeology: Modern evaluative friction ridge identification*1989: Royal Canadian Mounted Police (Pub.). 48.

13. *Announcing the Advanced Encryption Standard (AES)*, N.I.o.S.a.T. Department of Commerce, Information Technology Laboratory, Editor 2001.