Using a secure SHA1 GPRS technology to provide mobile outpatient care in Jamaica.

Project supervisor: Sean Thorpe
Michael Foster, Andre' Harris, Stevon Nembhard, Snovia Russell and Alrick Williams
University Of Technology, Jamaica

0.0 Abstract

The aim of this project is to show how SHA1 and GPRS can be used to provide secure mobile outpatient care in Jamaica. The FISH clinic in Papine was chosen as the institute of focus because of its locale to the University of Technology. This project includes the design, development and implementation of a set of tools for outpatient monitoring at the FISH clinic via the use of cellular phones technology. These tools will provide support for both medical care and clinical research tasks. The work is centred on four main tasks:

I)Creating subsystems for collecting data under different situations, data includes clinical history, hereditary history, patient's identification, et-cetera.

II) Developing a method of presenting the collected data as a virtual clinic and,

III) Developing tools for validating and extracting the knowledge.

IV). Using SHA1 to provide security to the data used.

1.0 Introduction

Mobile phones have become a way of life for many people in Jamaica. They influence every aspect of our lives from the way we work to the way we leisure. In the medical community of Jamaica outpatient care is now a huge area of the operations of most medical facilities. With this increase the need for improvement of this service also increases and warrants research and implementation of new technology to make it better. Understanding mobile information access and related human interaction issues becomes increasingly important as more mobile phone devices are used and more people are away from home phones because of the availability of mobile phones. Therefore designing an interactive software using GPRS, Visual Studio Mobile Emulator technology and Wireless Application Protocol (WAP) to operate between the hospitals and patients mobile phones should be explored and implemented to see if outpatient care can be improved within a secure medium. In outpatient care the stakes are high for accessing up-to-date data such as patient personal information, patient medical records and treatment plans and delivering it over a phone. Patients are increasingly involved in managing their health care and the health care providers are challenged to motivate, educate and help people adhere to healthy behaviours and medication requirements. The interaction between patients and medical institutions can be greatly improved by issuing up to date appointments for follow up and reminders for taking medical prescription to ensure that patient's health is not endangered.

Given that patients are cautious of their privacy rights, it is very important to prevent violations of data security within the clinic data system or during the transmission of data between the clinic and cell phones. Therefore, we have to focus on the security requirement that procures the

outpatient data using GPRS services. Thus we need to construct a secure mechanism for patients' data at both clinic and on mobile phone platform and in the transmission between both by using proven encryption algorithms. Several encryption algorithms are available to secure data on mobile platform.

Secure Hashing Algorithm 1(SHA1) exists for securing data on mobile platform such as the Mobile Emulator in the .Net framework. In securing patients' data and privacy it will be dangerous to store passwords anywhere in plain text along with patients' names and other important data. The SHA1 gives a quick and easy way to encode passwords and other data into a non-human readable form. This means it will be safer to store data in a database, and should the database be viewed by anyone who doesn't have authority; it will be much more difficult for them to work out what a user's password and patients' data are. This paper presents the architecture of a system using visual studio mobile platform along with WAP and GPRS using SHA1 algorithm to secure patients' data and provides a mobile approach to improve outpatient care.

1.1 Scope Of The Study

The research will be based on the applications of the FISH clinic and will focus on how the use of GPRS and WAP mobile technology developed with Visual Studio Emulator will help to improve outpatient care. By limiting the scope of our research to The FISH clinic we can focus more in-depth on the doctors, nurses and patients. Since there is a small amount of people to deal with samples taken for proof of effectiveness of the system will illustrate true results that can be used to represent the entire group. The system is expected to allow for more efficient checking of Prescription, confirming appointments, storing of patients' records including clinical and hereditary history, storing blood pressure (BP) and blood sugar (glucose) results. Security of such delicate data is also a major area of focus for this project.

These main areas are analyzed in-depth in the methodology section of this paper.

1.2 Limitations

1) Time period: This project has to be completed in 2 semesters. This is simply not sufficient time for a project of this magnitude.

2) The FISH clinic is not fully automated therefore we have to make them automated before we can proceed with the ultimate project.

3) The staff at FISH was a bit hesitant about the project because they believe it would deprive them of their jobs, the doctors believe it would reduce patients' visits thus reduce revenue.

1.3 Research Questions

1. What types of data are used in outpatient care?
2. What are the various processes use to collect data?
3. What are the main drawbacks of the present outpatient care?
4. Is the FISH clinic automated?
5. How long will it take for it to be automated?
6. What are WAP and GPRS all about?
7. How can WAP and GPRS be used to send data among mobile phones and a PC?
8. How can the Visual Studio Mobile Emulator be used to aid in this research?
9. What security requirement would be necessary in launching the environment that procures the outpatient data using GPRS services?

1.4 Definition Of Terms

GPRS: General Packet Radio Service.

WAP: Wireless Application Protocol.

Visual Studio Mobile Emulator: An artificial environment that uses ASP.Net (Active Server Pages) mobile controls to permit the production and testing of a wide variety of applications for mobile devices.

Telematic: Technology that uses mathematical calculation to formulate conclusions.

Software: Execution of program instructions.

Telemedicine: The use of technology to improve outpatient care in the health sector.

Outpatient: A patient who attends a hospital without staying there overnight.

Outpatient Care: Treatment including services, supplies and medicines provided and used at a Hospital under the direction of a Physician to a person not admitted as a registered bed patient; or services rendered in a Physician's office, laboratory or X-ray facility, an Ambulatory Surgical Centre, or the patient's home.

2.0 Literature Review

The use of technology to aid in outpatient care in the medical industry is being adapted world wide by many countries.

According to a recent study released by (Medford, 2005) this corporation of technology and the medical industry is called telemedicine and is being implemented in a variety of ways, but its main focus is on improving outpatient care. In Europe Mrs Grenda Van Biervliet managed a project entitled “Smart insole monitoring for diabetics”. It was an IST project, code named Diafoot, in which a system for remote monitoring of patients feet in Europe, not just within the clinic but as they go about their everyday lives, was developed. In Hong Kong a system very similar to the one we are proposing was developed. Kevin Young and Yuan-Ting Zhang state that the implementation of a WAP based telemedicine system for patient monitoring was done at The Chinese University of Hong Kong. The system utilizes WAP devices as mobile access terminals for general inquiry and patient monitoring services. Authorized users can browse the patients’ general data, monitor blood pressure (BP) and electrocardiogram (ECG) on WAP devices in store-and forward mode. The system showed how WAP could be feasible in remote patient-monitoring (outpatient care) and patient data retrieval. Another article titled MEDICI: Inpatient/Outpatient Monitoring for Diagnosis and Medical Research in Ischaemic Cardiopathy, declares that a collaboration of hospitals and universities, mostly Hispanic, are working on a project with the purpose to design, develop and implement tools for inpatient and outpatient monitoring of patients suffering from Ischaemic Cardiopathy. The work is being organized around three development lines:

a) a system for collection data including monitored electric and hemodynamic signals and data related to remotely monitored signals outside the hospital.

b) Techniques for integrating the collected information and presenting the history associated to the patient and

c) tools for extraction and violation of medical knowledge.

The technological improvement of outpatient care is a bit costly to obtain but the results illustrate that it is well worth it. According to (Medford, 2005) US $77 million was pumped into the telemedicine segment of the health care InfoTech market in 1995 alone. The same article states that a $2.8 million contract was awarded to Beth Israel Deaconess Medical Centre from the National Library of Medicine of the National Institutes of Health to develop a home-based, two-way videoconferencing computer link for parents whose very premature or sick newborns require round-the-clock intensive care. The telemedicine computer home stations will help to educate and comfort parents who must leave infants in the neonatal intensive care unit by allowing them to see their babies as they eat, sleep and grow, and to talk to doctors and nurses who monitor their care. It also will allow staff to remotely monitor the progress of their young charges after they leave the hospital for home.

Telemedicine is definitely emerging as an interesting new tool for working with developing countries. According to reports from Howard University College of Medicine it has even reached its fingers into the Caribbean. Two new telemedicine installations linking Caribbean hospitals to leading medical facilities in the United States may become models for reducing costs and providing better health care in the developing world. Massachusetts General Hospital and Howard University College of Medicine are using telemedicine applications to establish links with Caribbean island hospitals, eliminating patient travel costs for routine medical care. The first new installation connects the Centro de Diagnostico y Medicina Avanzada and the adjacent Centro de Conferencia Medicas in Plaza de la Salud, Santo Domingo, Dominican Republic, with the Massachusetts General Hospital, a teaching hospital of Harvard Medical School. Through its ties with Massachusetts General, the new Plaza de la Salud complex will be the primary acute-care facility for the Dominican Republic, offering diagnostic services and support in radiology and pathology. Additional telemedicine links are also under way to extend the reach of services to other parts of the Dominican Republic.

In the second Caribbean installation, a telemedicine network was established between the Roy L. Schneider Hospital in St. Thomas, U.S. Virgin Islands, and Howard University Hospital and its College of Medicine in Washington. The network allows physicians at Howard University to provide telediagnosis (the use of computer to diagnose certain illnesses) and medical consultation services to St. Thomas in such areas as paediatrics, cardiology, infectious diseases, pathology and continuing medical education.

Bulletins posted on the ATALACC web site along with confirmations from ATALACC's Caribbean representative MD. Winston Davidson, the members of ATALACC are indeed interested in improving telemedicine in Latin American countries and the Caribbean. The American Telemedicine Association Latin-American & Caribbean Chapter (ATALACC) is comprised of professionals from Latin-American and Caribbean countries that are committed to the development and application of telemedicine and medical informatics. ATALACC also seeks to provide a forum for the sharing of information and resources in order to educate and promote telemedicine initiatives in this region.

The overall mission of the ATALACC is:

1) The application of telemedicine and medical informatics solutions in different political, economic, and

social systems in Latin America and the Caribbean.
2) The dissemination of these solutions within the respective health care systems.
3) The education and promotion of telemedicine and medical informatics solutions within the region.
4) The building of resource capacity for telemedicine and medical informatics solutions in the respective countries.
Jamaica has in no wise been left out of this movement towards telemedicine. According to Omar Tomlinson the University of the West Indies (UWI) Jamaica is also in the move toward telemedicine. From the year 2004 UWI has been offering Telemedicine Certification. According to Mr. Omar Tomlinson the telemedicine programme is meant to complement the telemedicine network platform known as The Caribbean Model, an integrated technological system, which he designed over the course of several years. The Model employs the use of a variety of technologies including the telephone, an electronic medical record system which patients will be able to access, and multi-media computer capabilities such as media clips and video-conferencing.
It is clearly shown here that the use of technology to improve outpatient care is already a success in many countries, and more countries are moving towards the same trend. UWI has already seen to the fact that Jamaica does not get left behind in this seemingly global move. It is therefore only imperative that we endorse the move towards the future of outpatient care.

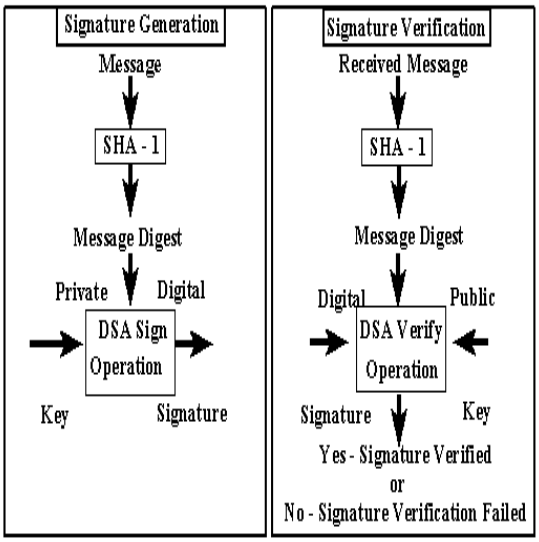
3.0 Methodology

This research is being done in a quantitative research method, with the use of survey questionnaire and qualitatively by developing a prototype of a software system. The research is targeted at approximately 200 patients and a 20 member staff comprised of doctors, nurses and receptionists from the FISH clinic along with UWI Hospital. Inclusion criteria requires that the staff members must have some knowledge of computing or at least be willing to learn about computers, the patients must use phones with GPRS and WAP technology and must know how or be willing to learn how to browse through the internet with their mobile phones. This also means that the patient must possess or be in the care of some one who possesses the ability to speak and understand the English language well enough to navigate themselves through the outpatient care system. Exclusion criteria include severe mental or physical limitations and those who were unable to own a cellular phone with GPRS and WAP capabilities.
Taking a closer look at the FISH clinic it is realized that their system is not automated. That is all the patients' records are not computerized. Therefore the first thing to be done is to computerize the FISH clinic. This requires a database created for the storage of patients' data on the site of the FISH clinic. The database is designed so that each patient is assigned a unique identification number. Doctors, nurses and receptionists will have different access privileges to the system which will give credit to the integrity of the data stored in the database. This database application, which is the interface that the user will interact with, is created using the Visual Studio.Net tool. The database was generated using the SQL 2000. This computer at the site of the FISH clinic will be the content server and the centre of this outpatient care system. If this computer crashes, the system crashes. Therefore it is imperative that security is most

exuberant in this system and an efficient back up system is in place. Users of the system, passwords are encrypted using the SHA1 algorithm so that it is difficult to figure out what the passwords are from unauthorized personnel. The patients identification number along with their names are also encrypted to ensure that data being transmitted to mobiles phones are secure and only can be viewed by the patients themselves and those authorized by the patients to ensure privacy. The Secure Hash Algorithm 1(SHA1) that is used takes a message of less than 2^{64} bits in length and produces a 160-bit message digest which is designed so that it should be computationally expensive to find a text which matches a given hash. The message digest can then be input to the Digital Signature Algorithm (DSA) which generates or verifies the signature for the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature. The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify.

While the patients' data is being entered into the database by the staff at the FISH clinic, the initiation of the ultimate project will commence.

The first desire in approaching this project is to establish a link between the server and the mobile phones. The internet already supplies such a connection via the use of WAP and in most cases GPRS technology. The two major cellular phone providers in Jamaica use GPRS and WAP to connect to and send and receive data to and from the internet. Since WAP will continue to be a common feature in hand-held devices and its possible use in telemedicine has already been investigated and proven true, it is worthwhile to use this technology to improve outpatient care at the FISH clinic.



Using the SHA-1 with the DSA

A WAP-based telemedicine system will be developed. Its aim will be to utilize WAP devices as mobile access terminals for general inquiry and patient monitoring services. With this system authorized users who can be doctors, nurses, patient's relatives or the patients themselves can view the patients' monitored physiological parameters on WAP devices in store and forward mode. The FISH clinic confirms that the heart conditions of elderly patients have to be continually monitored when those patients are diagnosed with chronic diseases and the blood pressure readings help to identify some amount of abnormality with the heart. For these reasons the parameters for this WAP based system will incorporate:

- Blood pressure (BP) readings.
- Blood sugar (glucose) readings.

- Patients' clinical and hereditary records.
- Prescriptions.
- Appointment details.

The development of this WAP base system will require browsing of information on the internet, and it grants the option of entering data into the system via the use of the mobile phones. In the case of patients being bed ridden and having to stay at home, a nurse can perform the BP, ECG and glucose tests and post them on the patient's mobile phone. The doctor then reading the result will decide whether or not it is imperative for a consultation with the patient before the next appointment date. Note: outside of the health centre stay at home nurses or the patients themselves will be able to input data in to the database. However, once the database has stored the data only authorized individuals who can access the server at the site of the health facility will be able to edit or delete the data (SHA1). Others will be only ably to browse. This means that a WAP site must be created for the FISH clinic. For access to this new WAP based telemedicine system, users simply need to subscribe to WAP data service and use WAP phones along with the password of the patient to access patient data during the browse of the clinic's WAP site. Operation cost is low and mobility is enhanced because the only computer needed will act as a server at the site of the health facility. The other access devices will be cellular phones. Doctors and nurses will be able to monitor their patients' well being from anywhere in the country, and the patients will feel a lot more secure knowing that their doctors are in a sense always with them.

This outpatient care system consists of a WAP mobile phone, a WAP gateway, and a server. The WAP device, mobile phone, communicates with the server which stores information and responds to the users' requests. The gateway in between translates and passes information between the mobile phone and the server .In order to decide exactly which medical applications are possible with WAP it is important to analyze the capabilities of a typical WAP mobile phone. Such a device has limited processing power, memory, battery life, display size and resolution and entry capability. Compared to a wired network, the most currently used wireless have low bandwidth, resulting in delays between data request and response to the mobile phone. Due to the nature of such a network the requests and responses are required to be concise for minimal latency. This latency depends on the type of bearer used. According to Simon Buckingham, with a GSM network, possible bearers are short message systems (SMS), circuit switched data (CSD) and general packet radio switching (GPRS). Yes GPRS is one of the bearers of GSM but because of its distinctions in comparison to the other GSM bearers GPRS is practically placed in a category by itself. GPRS is faster than the CSD bearer of GSM for it provides a 171.2 kb/s data transfer rate compared to CSD's 9.6 kb/s. GPRS also provides immediacy whereby data can be sent and received immediately as the need arises, no dial-up modem connection is necessary.

3.1 System Architecture

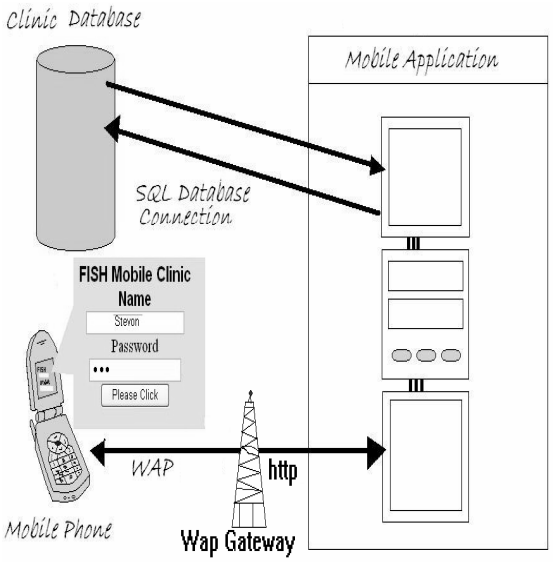


Diagram of the system architectural layout.

The system architecture is built on the Microsoft .Net framework

3.1.1 How The System Will Work

When a patient types in the address for the clinic's WAP site a welcome screen will appear which will give the option of login in. The patient then enters his/her password and gets into the system. The next WAP interface seen will give the option to view one of the following

- Blood pressure (BP) readings.
- Blood sugar (glucose) readings.
- Patients' clinical and hereditary records.
- Prescriptions.
- Appointment details.

When the patient selects an option the request is forwarded to the server which then finds the data of the patient with matching password, makes a copy of the requested results and forwards the request to the WAP gateway, which then converts the data from HTTP and sends it through GPRS to the patient's mobile phone.

After choosing to view the BP and glucose results the patient will see the option of entering data which must be done in the format given. Upon their request to save this data the system will validate the data then save it and the date it and time of it's arrival along with the name and phone number of the person who entered it. This is for security reasons so the records will also contain the name and number of each doctor or nurse that enters the patient's data.

The WAP site will be developed and tested by a Visual Studio Mobile Emulator. The emulator will be used before the actual WAP phones

3.2 Benefits of this Project

I) The patients will feel more connected to their doctors and nurses and will therefore encourage their friends and family members to join the FISH clinic, thus increasing revenue.

II) Patients will be better monitored while away from the clinic because the ability to enter BP and glucose results keeps the doctors constantly aware of the patient's conditions.

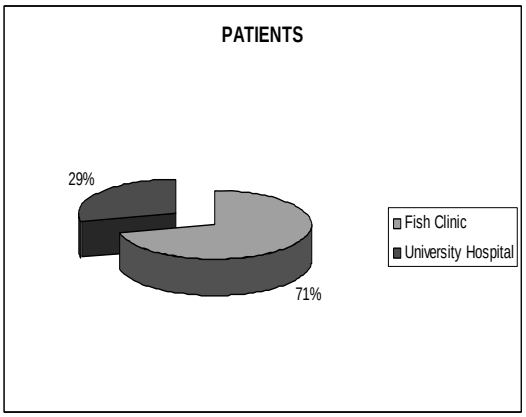
4.0 Results

Of the 200 patients who filled out the questionnaire, 53 were between 15 and 20 years of age 26%, 102 were between the ages of 21 and 30 years and 45 were over 30 33%. 129 of the patients were male and 81were female. Another survey was done of the Doctors and nurses at the Health Facilities. A total of 20 medical personnel participated. Of the twenty medical personnel 14 were doctors and 6 were nurses.

4.1 Statistical Analyses

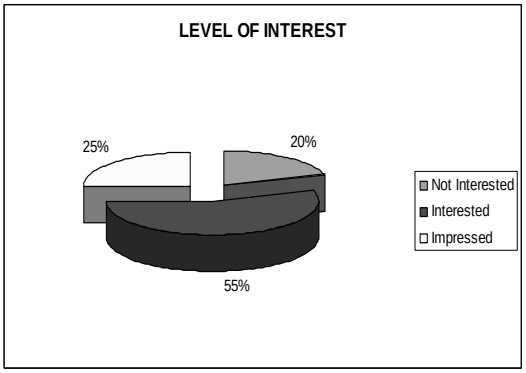
4.1.1 Patients

143 (71.5%) of the patients surveyed were from The Fish Clinic and 57 (28.5%) patients from the University Hospital of the West Indies. Of the two above-mentioned facilities only The University Hospital has a computerized system.

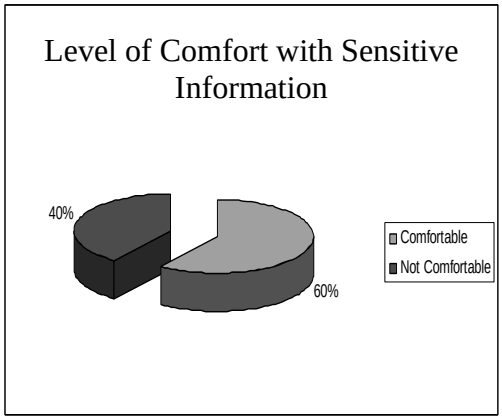


Patients are all reminded by a telephone call or via word of mouth of their appointments.

55% of the despondence stated that the system is interested; 25% state that the system is impressive, and 20% stated that it was not interested.

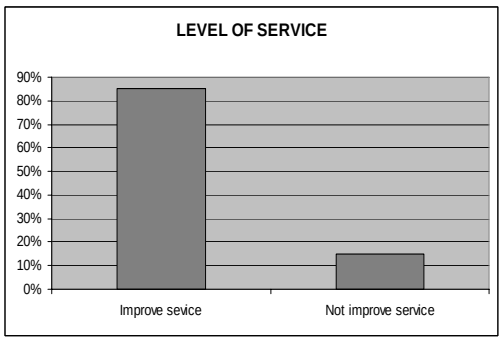


60% of the respondents state that they would be comfortable with the system if it was to show their prescription, blood pressure and blood sugar result, while forty percent would not be comfortable.



4.1.2 Medical Personnel

85% of the despondence stated that the mobile system will improve there outpatient care and services. 15% stated that it may not because patients may not want their personal details known.



In responding to the issue of security 100% responded that security is very important.17 thought that using the internet service on the mobile phone to keep track of your out patients will be feasible to your business. All of the despondence stated that they would purchase such software.

5.0 Summary & Conclusions

The use of technology to aid in outpatient care in the medical industry is being adapted world wide by many countries.

This research set out to explore how GPRS or GSM technology can be used to improve the quality of outpatient care in selected health facilities in Jamaica.

To arrive at a proper conclusion, we sought to first answer the questions:

What types of data are used in outpatient care?

What are the various processes use to collect data?

What are the main drawbacks of the present outpatient care?

How can WAP and GPRS be used to send data among mobile phones and a PC?

What security requirement would be necessary for storage and transmission of the necessary data?

Our findings indicated that in outpatient care, the majority of the data stored pertains to patients' prescriptions, appointment dates, patients' records (including clinical and hereditary history), and test results such as blood pressure and blood sugar results.

The primary problem with outpatient care at present is the inability to keep in contact with particular patients at times. This ultimately prevents medical facilities from following up on their outpatients

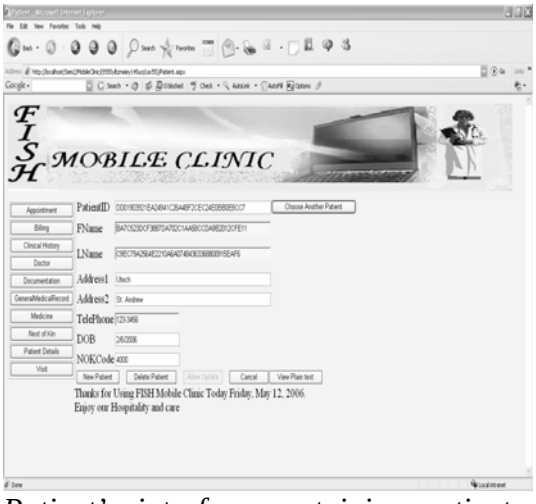
Using WAP enabled GPRS devices such as mobile phones, data can be transmitted across a network. It in fact can facilitate communication between the user of the device and a centrally located server.

The data specific to particular outpatients is sensitive. It is therefore imperative that the storing and transmission of this data over a network incorporates adequate security. The most appropriate method of securing this data is encryption.

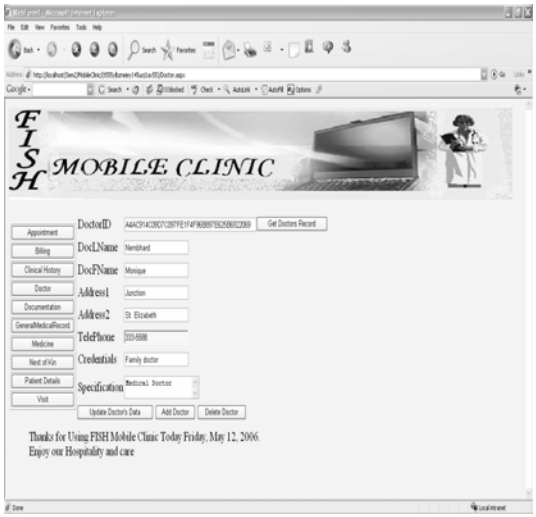
With these findings in mind, the conclusion was made that the quality of outpatient care could best be improved through the development of an interactive information system. This information system would store data pertaining to individual outpatients and which can be accessed by both the patients themselves as well as authorized staff of the health facilities. The system would utilize WAP enabled mobile devices as access terminals for general inquiry and patient monitoring services.

Through survey conducted at The Foundation for International Self Help as well as The University Hospital of the West Indies, the feasibility of this system has been confirmed. Some 55% of the showed direct interest in the system, and 85% thought that it will improve outpatient care.We have since then developed a prototype to demonstrate the operation of this system.

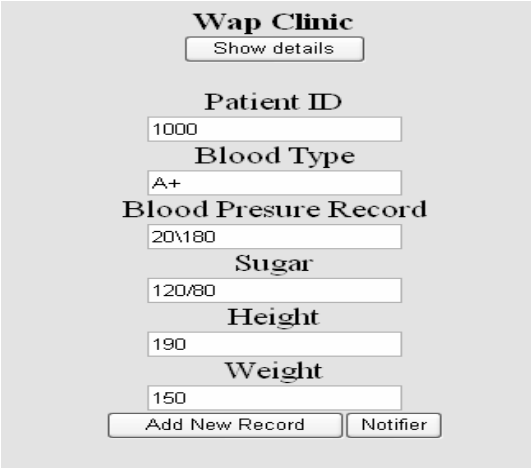
5.1 Screenshots Of The Prototype



Patient's interface containing patient ID, Patient name fields encrypted with SHA1.



Medical personnel's interface containing an ID field encrypted with SHA1.



WAP interface viewed on the mobile phone. A SHA1 encrypted password is required to view it.

5.1 Recommendations

After this phase of the project is completed and implemented the system will be upgraded to keep track of the electrocardiogram (ECG) results of the patients. This is necessary to keep track of the patients' heart beats and to tell whether or not something is wrong with their heart. Other results such as urinary results will also be added to the system.

Reminders will included to inform the patients via text messages of their appointments, to fill prescriptions and to come in for results that cannot be posted over the internet.

The database could also be encrypted to improve the security of the database.

6.0 Bibliography

Overview of WAP, M Toschi, Wrox Press, 2000

Talemed, Evidence Based Telemedicine for Remote and Rural Underserved Regions in LA using e-health Platforms
www.talemed.com

MEDICI: Inpatient/Outpatient Monitoring for Diagnosis and Medical Research in Ischaemic Cardiopathy
http://Platon.escet.urj(iesljspTIW2005/informesPDF)Tic2003-09400-coup.pdf

Medford Ronald ,Telemedicine and Outpatient Care January 2005
http://TelemedicCare.uk.edu