International Journal of Industrial Engineering and Management (IJIEM), Vol.1 No 4, 2010, pp. 131 - 143
Available online at www.ftn.uns.ac.rs/ijiem
ISSN 2217-2661

Seamless Service Delivery Solution for mHealth Application

Dragan Bošković
Senior Director, Motorola Mobility Holding Inc, 600 North US Highway 45, Lybertyville, IL-60048-USA, dragan.boscovic@motorola.com
Milan Kovačević
Deputy General Manager, SAGA d.o.o Beograd, Milentija Popovica 9, Sava Centar, 11070 Beograd, Serbia, milan.kovacevic@saga.rs
Tihomir Ilić
Professor of Neurology and Clinical Neurophysiology, Diagnostic and Policlinical Centre, Military Medical Academy, Crnotravska 17, 11000 Belgrade, Serbia, tihoilic@gmail.com
Dimitri Arges
Founder, NuDyn Technologies, 3277 Skyline View Glen, Escondido, CA 92027, darges@nudyn.com
Mike Wisz
Principal, Mike Wisz and Associates, 21 Broadway, Suite 422, San Diego, CA 92101, USA, mike@mikewisz.com

Received (29.11.2010); Revised (21.12.2010); Accepted (24.12.2010)

Abstract
ICT opens up many new opportunities for higher-value products and services, of which Personal Health System (PHS) is just one of the possibilities. PHS for remote management of diseases, treatment and rehabilitation, outside hospitals and care centers is based on closed-loop approaches and integrates wearable, portable or implantable devices into a subsystem coupled with appropriate platforms and services.
This article discusses such subsystem that we called mHealth Console and puts an accent on gathering and analysis, interpretation and use of the multiparametric data, in conjunction with established or newly created medical knowledge, for shared patient-doctor decision support systems.
After discussing business motivation for remote provisioning of healthcare services in Section1, the paper continues by describing a framework for ICT deployment on Section 2. The proposed service delivery architecture is based on Over the Top (OTT) delivery principles and enables perspective mHealth provider to reach service users (e.g. patients, health insurance, health providers, employers, pharmacies etc) irrespective of their locations and type of physical connectivity in that location. The Section 3 continues by offering a detailed functional architecture for mHealth Console and Portal, description of signalling message flows for different SIP and DLNA based use cases.
The article concludes that mHealth system is a powerful ICT based solution that process comprehensive sensor data, both environmental and behavioral, and is critical component enabling provision of monitoring and rehabilitation services to the patients. The features of the proposed solution such as independent communication session initiation, seamless and automated exchange of stored and real time information and use of devices of affordable price, makes the proposed architecture a viable solution for seamless delivery of mHealth services.

Key words: *Mobile Health Care, ICT for Personal Health Care, Seamless mHealth Service Delivery, Health Home Portal, mHealth Console*

1. BUSINESS CASE FOR mHEALTH

Mobile technologies and related ICT solutions hold great promise for personalizing health care and keeping people healthy, managing diseases, and possibly lowering healthcare costs. Recent market research [1] has found that 40% of respondents would be willing to subscribe to relevant service in order to enable direct interaction with their doctors on medical conditions of special concern to them. Equally physicians from their experience agree that patient compliance is a major obstacle to achieving higher treatment efficiencies, 88% would like to see their patients involved in monitoring their own health. Weight and blood sugar were most frequently cited as the most relevant parameters to monitor remotely by means of sensors and mobile technology pulled together into a mHealth solution, with other vital sign parameters following not far behind.
Mobile internet technologies have demonstrated the ability to penetrate wide consumer base very quickly and mobile devices are the most personal technology that consumers own. By allowing consumers to set

and control personal preferences for sharing and communicating the mobile internet devices provide an ideal platform from which health and wellness can be delivered on basis of mass personalization. And it is this set of personalized health services ubiquitously available and accessible from mobile and portable platforms/devices that we refer to as mHealth.

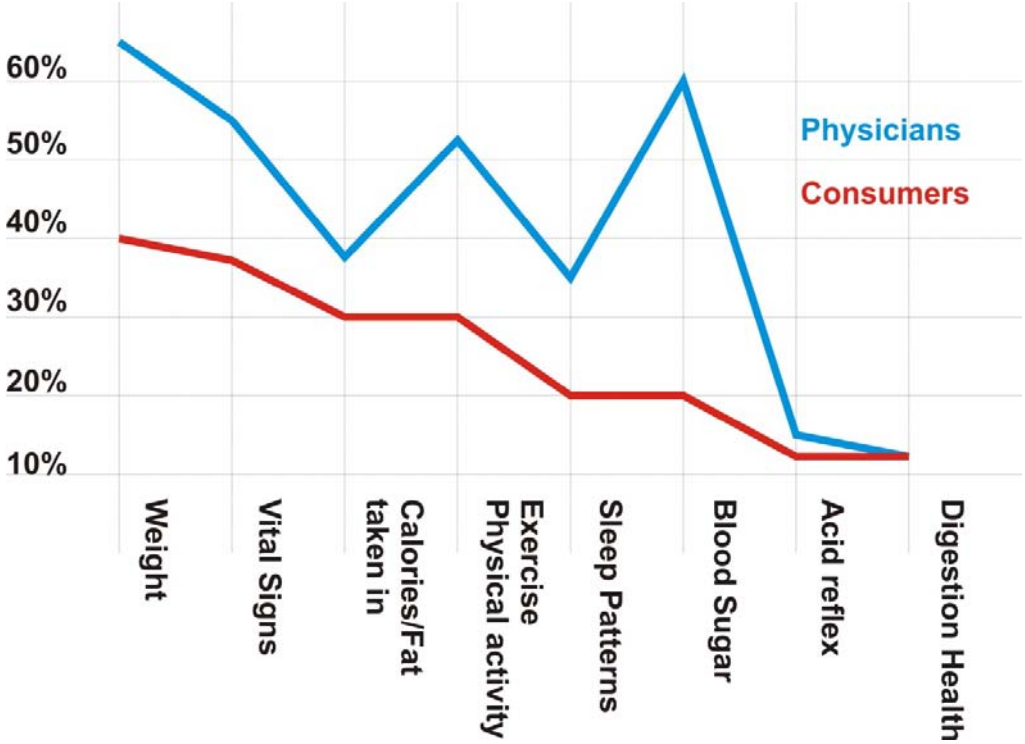

Figure 1. Desirability for remotely tracking health parameters (source [1])

Different players are starting to develop easy to use, affordable mHealth devices, services, solutions that are attractive from consumers' point of view. Market research report [1] estimates the annual market for remote/mobile management of disease treatment and rehabilitation monitoring in USA alone to be somewhere in range of $43 billion. This is giving rise to the new business models, that will continue to evolve, and can be grouped into three main categories:

1. **The operational/clinical model** enables healthcare organizations to run their business operations better and more efficiently. The beneficiary categories may include but are not limited to healthcare provider, payer, employer, medical device vendors/suppliers and drug companies as well as non-traditional healthcare organizations. Key parameters for the operational/clinical model are likely to be as follows:
    a. mHealth solution has to improve the use and the value of physicians' time. s The key here is making better informed decisions and faster as the access to more accurate data in real-time becomes available.
    b. Large portion of office visits can be eliminated by the use of mHealth technologies like remote monitoring, email, or text messaging with patients.
    c. Current method of reimbursement is based on in-person consultations, and reimbursement for phone consultations, email consults, telehealth and text will need to be eligible for billing too in order for the above business model to be accepted.

2. **The device and services model** interprets bio sensory data and enables individuals to relate to their health metrics. Moreover, it creates possibility of sharing that information with those who might need to know of their state of wellbeing (family member, physicians, fitness companions etc) This business models take advantage of the following:
    a. Personal devices such as cell phones and tablet computers are a ubiquitous device to inform and engage consumers.
    b. The simple act of texting and emailing has picked up momentum across all age groups. Especially important is that new form factors and UIs brought about by the tablets are increasing rate of acceptance among seniors.
    c. Different age groups are likely to want different type of services; fitness

monitoring might be more attractive to more active population while the remote health management is likely to appeal to more senior population.

3. **Infrastructure business models** base its value on providing reliable connectivity as well as secure and timely transfer of data and ubiquitous service availability. This business models rests on the three main pillars of the overall system requirements:
   a. *Interoperability*: mHealth solution has to effectively integrate its service logic into the rest of IT infrastructure within a given medical establishment. For instance, it has to incorporate existing EMR solution and other legacy IT systems In order for physicians and patients to derive value.
   b. *Security:* Privacy and Security of bio sensory data are of primary concerns to all players in the mHealth value chain. Thus the effective solutions covering these requirements will create value that can be monetized or used for business differentiation.
   c. *Bandwidth*: Legacy IT infrastructure either in medical establishments, or patients home might not be adequate to guarantee timely information/service delivery. mHealth solutions that will use processing and memory/cash resources to alleviate the pressure on network bandwidth resources will be an important parameter to factorize in the overall business model.

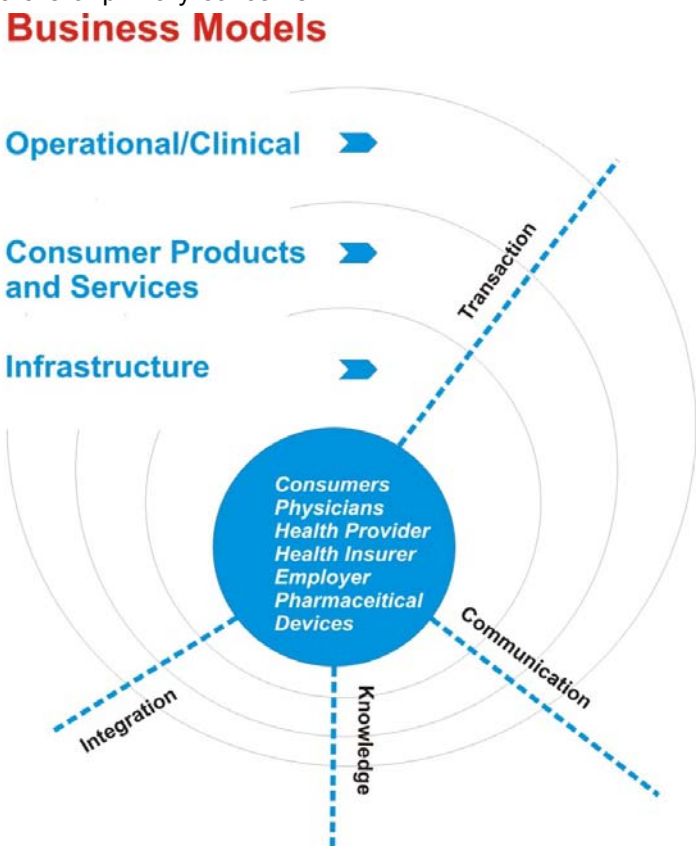

Figure 2. mHealth Business Models can be grouped into the classes, namely: 1) Operational/clinical capabilities, 2)Consumer products and services and 3) Infrastructure to connect, secure and speed up information and services. The business value in each of the three classes can be extracted out of a) transactions, b) communication, c) knowledge or d) system/data integration related activities. (Source [1])

2. mHealth AS A COMPREHENSIVE FRAMEWORK FOR PERSONAL HEALTH SYSTEMS

mHealth unifies business and technology platforms from which to pursue ideas of the Personal Health Systems (PHS) [2], presented on the European Commission ICT 2010 Conferences [3], [4] and other FP7 documents [5],[6],[7].

At its basic PHS is envisaged as a system which, on basis of Information & Communication Technology (ICT) Solutions, provides comprehensive and continuous healthcare for the patients in their native, everyday environment. The schematic presentation of the PHS concept [2] is depicted in the Fig.3.

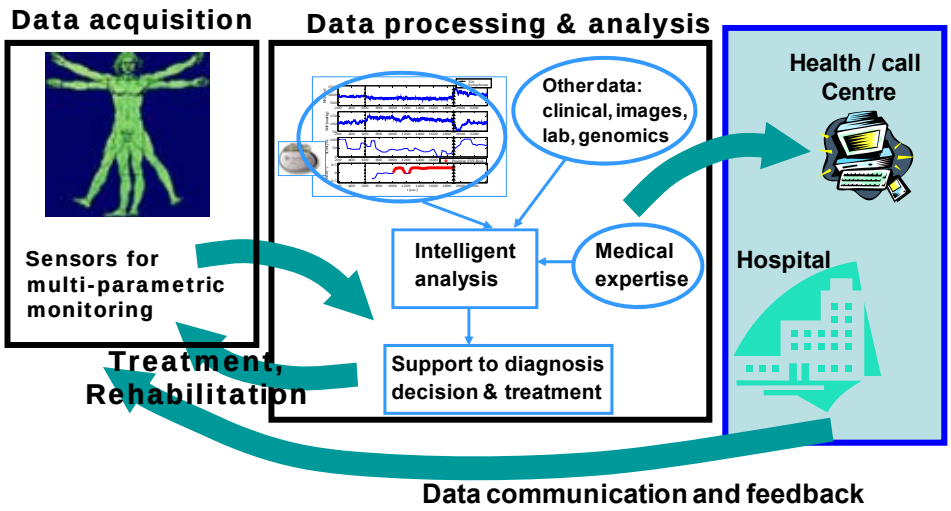

Figure 3. Schematic Presentation of the PHS Concept

The basic idea of PHS concept is to utilize powerful edge computing resources (most likely deployed in the form of GRID computing) to apply complex analytics algorithms on a comprehensive set of multi-parametric data (environmental and behavioral). Once constructed the system would be tested in clinical practice in order to calibrate the algorithms and prove the concept.

A mHealth schematic design brings together all building components and functional entities necessary to provide PHS services are depicted in Fig 4. The basic intention (or better say the main requirements) is to use the IP infrastructure as unifying medium to ensure ubiquity and seamlessness of PHS services.

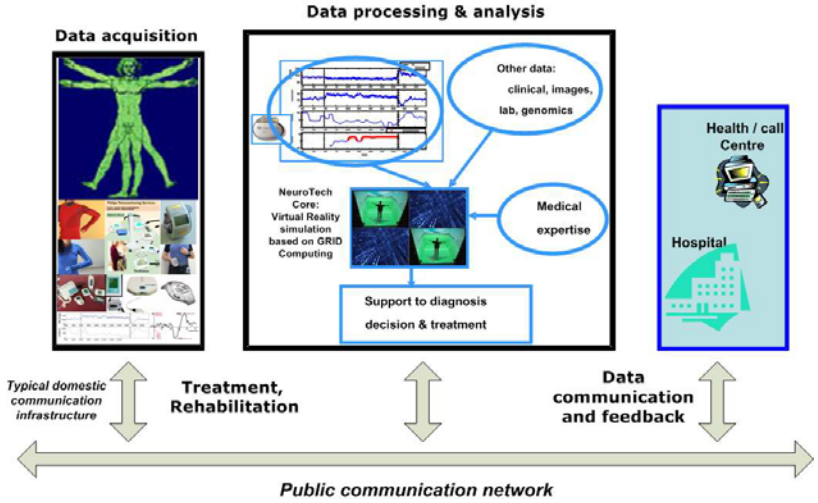

Figure 4. General Communication Setup for PHS services

One of the basic ideas behind the PHS concept is to acquire large amount of data of various kind, many of which are contextual and not known to have any relevance to the disease being monitored. These data are collected over a long period of time and are subjected to data analytics in order to correlate them with the patients' health condition and prove or disprove their significance to the disease/condition being monitored. These data will comprise vast number of sensor signals resulting from the measurements of patients' medical condition as well as the measurements of the relevant environmental conditions together with the video records of the patients in their natural environment. Altogether it is likely to be vast amount of data that needs to be moved between different logical entities of mHealth solution.

In order to more effectively manage this flow of information/data some kind of pre-processing and/or local caching might be needed. The analysis of the sensor measurements signals that can be done locally (pre-processing) would have for its purpose to determine the events/conditions relevant for the specific PHS service. Only pre-processed and relevant data would be stored and/or transmitted to PHS core for further processing. This distributed data caching and data analytics would serve to:

- considerably reduce the information rate and hence the required communication bandwidth
- preserve and protect data integrity and the patients' privacy

3. SEAMLESS SERVICE DELIVERY FOR mHealth APPLICATION

3.1 Seamless Service Defined

A seamless service is defined as user service or application that is required to exhibit one or more of the following characteristics:

- *Ubiquity across disparate access media* – wireless and wireline.
- *Convergence of media* – Voice, video and data.
- *Personal Convenience, Control, and Context of service* -Provides user programmable policy driven personalization
- *Interactive Service* – enables mash up of available service logic into different applications.

The mHealth services are ubiquitous across multiple access and core network infrastructure and truly multi-modal in its nature in which voice, data, and video are integrated into different applications depending on a given context.
Essentially, seamless service should empower mHealth users to have ultimate control over the information/data collected and when, where and with whom they should be shared.
As explained in the section 0 the PHS services will meet the above seamlessness requirements if offered as "over-the-top" services [8] and this paper will proceed to describing such a solution.

3.2 Use Cases

Many use cases could be envisaged as part of the overall mHealth service offering. Nevertheless the uses cases presented in this section emphasize the capability of the proposed communication system to provide seamless, secure, dedicated communication between the MHEALTH core application and the mHealth Console which resides at patient's location and as such is an ultimate mHealth appliance. In addition to servicing MHEALTH service logic, mHealth Console could be an application platform facilitating overall data processing, relaxing communication bandwidth requirements, enhancing service availability and preserving privacy of the patient's data.

- Regular monitoring and/or data collection. Session is initiated from the MHEALTH core application as regular polling of the patient's condition. Once the session is established the stored data (organized in appropriate data structures convenient for later processing) would be downloaded from the patient's mHealth Console to the MHEALTH core and stored there for later processing. At the same time the mHealth Console storage and processing resources would be freed for the future data recording and/or processing.
- Direct doctor/patient interaction. Physicians might need to communicate with the patients, at mutual request. Through the proposed communication solution the doctor could initiate a video or voice call from any communication appliance and have real time interaction with the patient. In case that the doctor might not be available the patient could leave a message pointing out some relevant condition he/she experienced in the near past, which is recorded and stored in the mHealth Console by request of the patient him/herself. At convenient time the doctor would establish connection with the patient's mHealth Console (not necessarily with the patient present!) and review the recorded material without the need to download it to the MHEALTH core system. Depending on the doctors' expert opinion these records could just be ignored (deleted) or downloaded for the future processing.
- Real-time data streaming**.** In another case, if an emergency condition was automatically diagnosed, or if a patient requires critical response/guidance from the MHEALTH core application, a session could be initiated from the mHealth Console side. In this situation, the data records do not have to be downloaded to the MHEALTH core. The proposed technical solution provides functionality which allows mHealth Console to become a data (e.g. video) server streaming recorded data, or data acquired in real time for that moment, directly to the MHEALTH core application and/or doctor for immediate analysis and reaction.
- Automatic patient interview. The MHEALTH core application (or the doctor) might require certain structured input from the patient in a form of the questionnaire or interactively designed video session which also can be stored in the mHealth Console. The patient would take the interview at his/her convenience interacting only with the local application stored on mHealth Console where the results would also be recorded. Later, a communication session between the mHealth Console and MHEALTH core applications could be established on mHealth Console request and these data than could be downloaded to the MHEALTH core system.

3.3 Service Delivery Requirements

At the very high level MHEALTH service delivery communication system can be presented as in Fig. 5

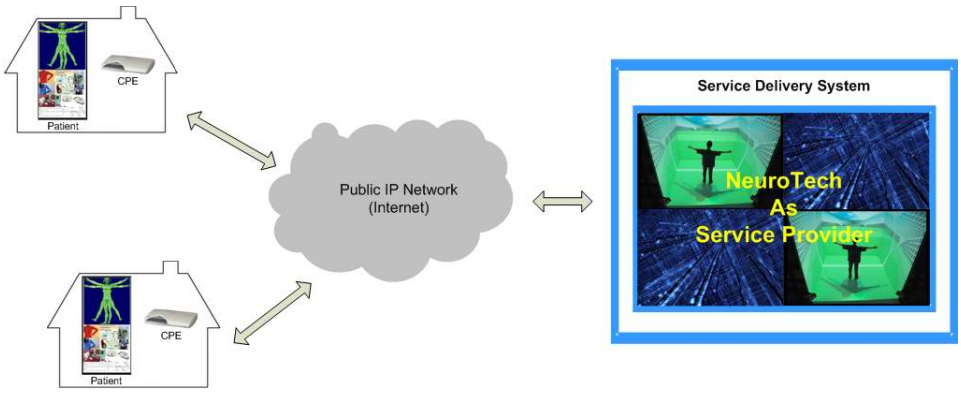

Figure 5. High LevelmHealth Service Delivery Communication System

Patients' residential locations are equipped with the mHealth Console. By the mHealth Console here we do not necessarily imply a single device (or box). It could comprise several, appropriately designed devices but fully integrated into unique equipment which comprises all or combination of the following functionalities:

- Sensory data gathering and remote control functionalities:
    - patient's and environmental sensors measurements acquisition and recording
    - video recording of the patient in his/hers living environment
    - preprocessing of the recorded data and "relevant event recognition"
    - temporary storage of the relevant event recorded data
- Multimedia interactive communication functionalities:
    - video
    - audio
    - data
- Accessibility/Networking functionalities:
    - OTT service functionality
    - general and/or "multi-play" access to public networks

The software application installed in the mHealth Console collects health data from the sensing devices directly attached to the patient or other devices present in the patient's home and connected to the mHealth Console. Example of this devices may include but are not limited to wireless scales, sleep detectors, motion cameras etc … All these bio and contextual data are collected, filtered in accordance with predefined policies and rules, and stored in an appropriate data structure for later retrieval and processing.
Using appropriate communication layers, the mHealth Console provides secure and dedicated connection between the local application and the core MHEALTH application over the public IP network infrastructure. This will be explained in some details in the later subsections of this document.

3.4 mHealth Network Architecture

The proposed service delivery solution, comprising the functionalities listed in the section above, provides a generic and very flexible platform from which to offer the mHealth services. This is quite important aspect as the mHealth services can be only a small subset of the total number of services offered by a given service provider. In this way the "entry barrier" is lowered and indirectly the consumers are to see the benefits of such approach through increased provider/network choices and reduced prices.
The mHealth Console is the central component of the proposed communication system. It provides control over all communication sessions between the client and the core mHealth applications.
At the Central Office end, the mHealth core application should have a piece of software identical to the one installed in the home mHealth Console device. In the rest of text we would refere to this network entity as mHealth Portal. As it will be shown later, the communication software in mHealth Console device has several layers, the most important of which is the middleware overlay which enables the Console to form a secure group and maintain an optimal communication path between members of the group, independent of IP address changes, interface changes, host failures etc. This middleware overlay is application agnostic, i.e., it does not know the communication protocol details or service logic of applications using the middleware. It simply provides an API to enable an application to create or join a group, provide callbacks when new Hosts join or leave and securely communicate with Hosts in the group. Practically the mHealth Portal in the Central Office will use this API to seamlessly establish and use secure connection to the home mHealth Consoles i.e. patients.

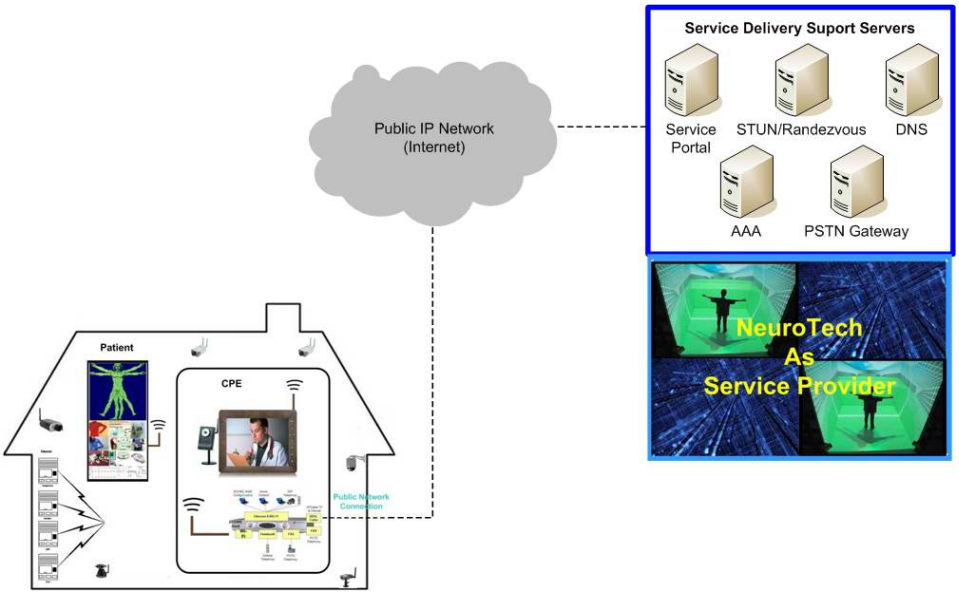

Figure 6. NeuroTech Service Delivery Communication System

The mHealth Console and mHealth Portal interact with each other using standard protocols such as SIP, http etc. The Console also comprises DLNA proxy server to enable access to and control of other DLNA sensory devices. The access to the sensory data on home DLNA devices or control of their configuration can be done via Web based applications running on the local Console or from any other Console via the mHealth Portal.

At the mHealth Central Office side there are several servers supporting the related service delivery... Here is a brief description of the additional servers needed in support of the overall mHealth solution.

- **STUN/Rendezvous server:** This server enables mHealth Consoles to determine if they are behind a NAT, figure out the NAT type and also maintain a connection in order for other Consoles to connect with each other. Clients maintain a persistent TCP connection with this server. They may also obtain reachable UDP ports via this server. Note that if the Console has a public addressor has port forwarding enabled it will be able to communicate directly with another mHealth Console. If not, data will be relayed through this server.

- **mHealth Portal:** The Portal provides many of the same functions in the Console itself. It enables devices that are not attached to Console to obtain services from devices in the mHealth network. For example, it has a DLNA proxy that enables the DLNA sensory device in a home to receive/send data directly from/to the mHealth core. It also enables policies, user preferences and other settings in the Console to be managed remotely via the portal.

- **PSTN gateway:** It provides signaling and media gateway functionalities to inter-work the PSTN circuit switched network with the mHealth network. This covers interoperability with both fixed and mobile legacy networks.

- **AAA server:** it provides Authentication, Authorization and Accounting services for CPEs. It authenticates the CPEs, and stores the billing records* resulting from the service consumtion.

- **DNS:** Standard Dynamic Name Server.

In general, as proposed solution is architecturally a network overlay, the mHealth services can be provided as an Over the Top (OTT) service and across heterogeneous access networks and operator domains. With its SIP and DLNA proxy capabilities the solution will have access to all kind of sensor, communication and electronic devices residing on the patient's premise or to patients portable and mobile devices when he/she is on the move. Each mHealth Console essentially creates or joins one or more overlays, which are simply secure groups consisting of selected Consoles. The overlay is then used by the client applications to securely exchange information among themselves or with the Central Office applications. The overlay middleware enables specific Hosts to form a secure group and maintain an optimal communication path between members of a group independent of IP address changes, interface changes, host failures etc. It also provides controlled access to a Console from any other mHealth client via the Portal. The middleware is application agnostic, i.e., it does not know the protocol details or service logic of applications using the middleware. It simply provides an API to enable an application to create or join a group, provide callbacks when new Console join or leave and securely communicate with mHealth Portal.

In this way proposed solution provides all the flexibility needed to manage and control a complex ecosystem formed around mHealth service offering.
By the mechanism described above the mHealth Portal can access any Console in the network. It can download stored event content records from them or it can issue commands to Clients for the purpose of starting new sessions or simply sensory device reconfiguration.. Patients' Console will act as clients/slaves to core/master mHealth Portal application and therefore they all can operate as the unique system even though they are located far apart and are connected across heterogeneous access networks and operator domains over which they form a secure group and maintain an optimal communication path between the members of the group independent of IP address changes, interface changes, host failures etc.

3.5 mHealth Console Architecture

This section describes the components of the mHealth Console and protocols and message flows they use to provide specific services. Each mHealth Console essentially creates or joins one or more overlays, which are simply secure groups consisting of selected, mHealth client devices. The overlay is then used by applications in the mHealt Consoles to securely communicate between them as well as with Central Office/Cloud. Such overlays can be brokered and managed by the user, the operator, or a 3rd party provider. To create an overlay, a mHealth Console uses a STUN/Rendezvous server to register the overlay identity and becomes reachable from other mHealth Consoles by maintaining a persistent TCP connection with the Rendezvous server. Other hosts can join the overlay using the Rendezvous server and once initial connectivity is established between mHealth Consoles, based on their respective NAT type, they may either continue using the Rendezvous server or may establish direct connection. The Rendezvous server authenticates each and every mHealth Console which maintain persistent TCP connections. The mHealth Consoles also authenticate each other when they establish direct connectivity. Note that while the following discussion uses a rendezvous server that is separate from an mHealth Console, every mHealth Console also has the rendezvous server function. So if a mHealth Console has a reachable address it can serve the functions of rendezvous server to enable creation of the overlay.

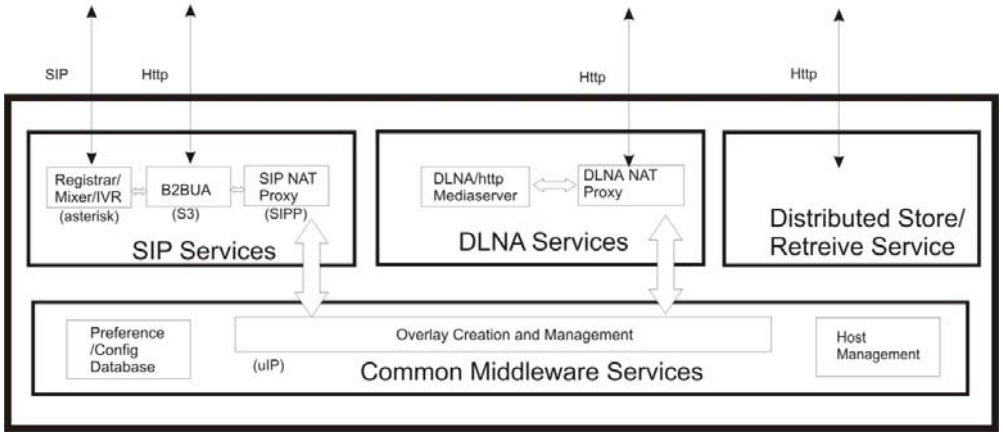

Figure 7. A Functional Architecture of a mHealth Console The mHealth Console consists of two main layers:

- a layer providing common set of middleware services which may be used to a number of other applications residing in the mHealth Console . One of the key functions of this layer is to enable mHealth Console to locate and reach each other, irrespective of whether they are behind NAT, form a secure association and maintain an overlay that can be used by mHealth services to communicate using a fixed identifier, irrespective of IP address changes. Another key function of this layer is to provide the enablers for configuration of control thru the portal and

- a layer consisting of applications that use the middleware to securely communicate and to provide services to a user or another agent. The services in the mHealth Console hosts are SIP call management and inter-working between remote DLNA devices.

These two layers work together to provide NAT traversal and OTT service delivery for mHealth [8]. Specifically there are two components to NAT-traversal [9,11,14]. At the IP level there is a need to take a packet from one NAT-ed subnet to another subnet and at the application level it is necessary to translate NAT-ed IP address embedded inside application level packets. In the proposed mHealth architecture, all applications use the underlying middleware for IP level NAT traversal. The middleware itself uses http/TCP connection for IP level traversal. For application level translations mHealth Console provides protocol specific proxies. For DLNA, xDLNA creates a http/TCP proxy that creates virtual instances of remote DLNA devices in the local mHealth subnet. For SIP, SIPP creates a SIP/UDP proxy [12, 16,17, 18]. Additionally SIPP uses a media proxy for NAT traversal of RTP streams.

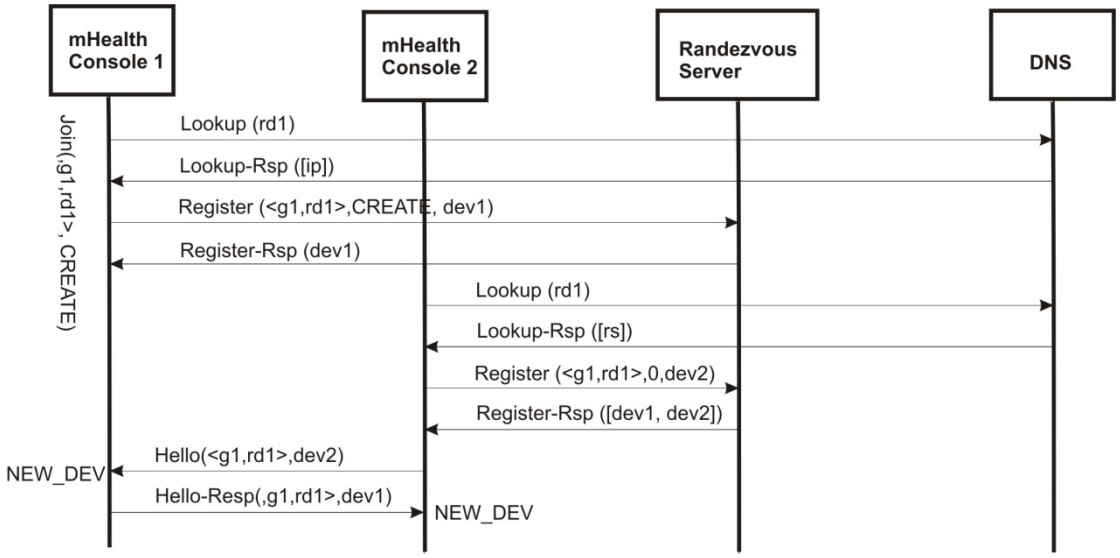

Figure 8. Overlay Creation in the proposed mHealth solution

3.6 mHealth Console Middleware

The overlay middleware enables specific mHealth Consoles to form a secure group and maintain an optimal communication path between members of a group independent of IP address changes, interface changes, host failures etc. Applications simply need to determine which group(s) they want to be part of and be concerned with how to locate and communicate with other hosts in the local subnet or a remote subnet. The middleware also provides controlled access to mHealth Console from any device in the Internet via the mHealth portal. The middleware is application agnostic, i.e., it does not know the protocol details or service logic of applications using the middleware. It simply provides an API to enable an application to create or join a group, provide callbacks when new mHealth Console join or leave and securely communicate with other mHealth Consoles in the group.

Each group is uniquely identified by a **<group_name, rendezvous_domain>** duple. Similarly, the middleware identifies each device in a group, irrespective of its underlying IP address, using a device_ID. A device can be a member of multiple groups and must have the necessary group specific credentials (such as a password or a certificate) to create or join. The middleware registers new groups with the rendezvous server corresponding to the rendezvous domain and uses the domain to determine the membership list of a group.

In the message flow in Fig 8, the middleware in mHealth Console 1 receives a request to create a group, for instance, from an application. The middleware creates a new group **<g1, rd1>** first by locating a rendezvous node corresponding to **rd1** using a directory (e.g. DNS) lookup. Once a rendezvous server is located, the middleware registers with the server. This registration process also establishes a persistent http/TCP connection between the mHealth Console and the server, thereby making the mHealth console reachable via the rendezvous server. The rendezvous server authenticates the mHealth Console and determines if it is authorized to create or join the group. If so a group is created with **dev1** as the only current member. Some additional points to note are:

- while the example message flow uses DNS, other forms of directories such as a distributed Hash Table may also be used, and

- in case that NATs support UPnP gateway device specification, the middleware may also configure the NAT to forward packets destined to the middleware port to the appropriate NAT-ed IP address of the device hosting the middleware.

When another mHealth Console (**dev2**) joins the same group, the rendezvous server authenticates and authorizes **dev2** and sends a response which includes information about **dev1**. This information includes an IP address and port that can be used to contact **dev1**. If **dev1** is behind a NAT, this address is simply points to the Rendezvous server. Otherwise the public address of **dev1** is provided to **dev2** so that they can communicate directly. The middleware in mHealt Console 2 (mhc2) then sends a hello message to mhc1, there by informing mhc1 of its presence. This message authenticates mhc2 to mhc1 and depending on whether mhc2 is behind a NAT, this message includes an address at the rendezvous server or a directly reachable IP of mhc2. The mhc1 authenticates itself to mhc2 via the **Hello-resp** message. The overlay middleware also provides call backs to application when a new peer joins or leaves the group. Some additional points to note are:

- During group creation an mHealth Console may mark a group as private. In that case the rendezvous node will not provide a full member list to new members, but will only provide the creator identity to subsequent members,

- After the initial hello exchanges, based on the NAT types corresponding to mHealth Console, either a direct communication path may be setup between them or they may continue communicating via the rendezvous server. Furthermore, if both the mHealth Consoles are behind the same NAT, for instance if mc1 is a PC and mc2 is a mobile phone in the same home, then the middleware will automatically use the direct path, and

- At any point, a group may be moved to a different rendezvous sever for load balancing or due to failures. This move is transparent to the applications using the middleware.

3.7 mHealth Console SIP Service Delivery

On an mHealth Console, three applications collaborate to provide the various SIP call services. They are (1) Asterisk (2) S3 and (3) SIPP. Asterisk is an open source PBX and provides the functions of SIP registrar, SIP call routing, conferencing and IVR. The S3 is a SIP Call feature engine and a Back-to-Back user agent (b2bua) which provides http/AJAX interface. It provides call features such as staggered ringing, pulling a call from a new device, joining a call from a new device etc. Its http interface is used for 3rd party Call Control (3PCC) services. SIPP is a SIP proxy that enables P2P connectivity between mHealth Consoles and between the mHealth Portal and mHealth Console. It uses the services of the overlay middleware. It also acts as an application-level network address translator (A-NAT) to remap NAT-ed IP address embedded in SIP headers. It also remaps NAT-ed address in the Session Description Protocol (SDP) [15] payload carried by SIP messages by obtaining public IP addresses/ports from the STUN/Rendezvous server for relaying RTP [10, 13].

3.7.1 SIP Voice, Data or Video Calls

In this section, we describe the simple case of how a SIP video/data call from mHealth Console in location 1 is made to another mHealth Console in location 2. Fig 9provides a pictorial representation of the flow of a SIP INVITE message from a SIP User Agent (UA) in location 1 to a SIP UA in location 2 via the various applications that collaborate to provide the SIP services. For simplicity we assume that mHealth Consoles in both location 1 and location 2 are in the same operator domain (mHealth.net).

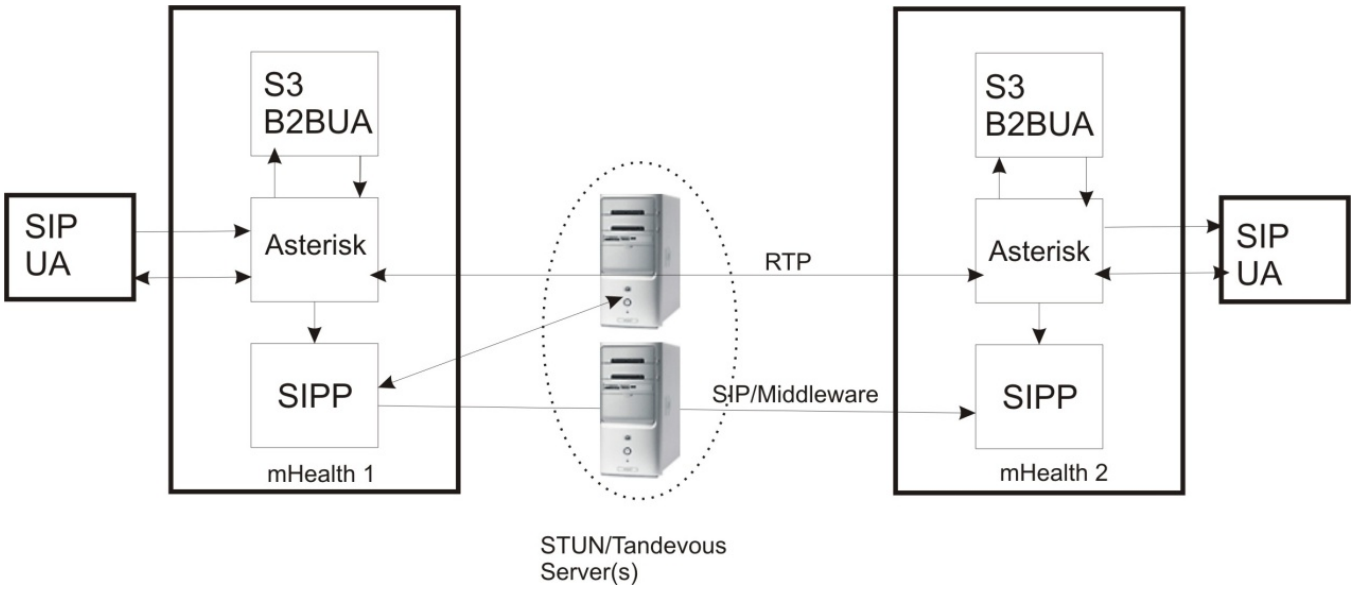

Figure 9. Schematic diagram of SIP Voice/Data or Video Calls between two mHealth Consoles

Upon startup, the SIPP application in mHealth Console uses the middleware to create an overlay group for the URIs corresponding to their respective hosts. In this example, the SIPP application in mhc2 creates a private group <5020, mHealth.net>. As described in the earlier sections, this triggers the middleware in mhc2 to create a persistent TCP connection with the rendezvous server corresponding to mHealth.net and register a private group named 5020.

When a SIP UA attached mhc1 makes a call to 5020, the SIP INVITE goes to S3 via Asterisk. The S3 B2BUA in turn creates another call leg and sends it to Asterisk for further routing. Note that S3 is in the path, so that at a later time if the call needs to be pulled from the calling SIP UA to a different device, S3 will be able to generate the necessary SIP messages to make the move. Additionally note that while Asterisk by itself can provide some call services such as simultaneous ringing, push a call to a different device etc., S3 is used to provide additional services such as pull or join a call from an authorized device. S3 also provides a web interface to view call state and control calls.

3.8 mHealth Console DLNA Service Delivery Architecture

The xDLNA application in the mHealth Console provides the DLNA proxy and address translation functions. It can interact with remote xDLNA

applications (in other Nat-ed domains) and create, in its local network, virtual instances of remote DLNA devices in the remote domains. The function of the xDLNA application is transparent to the DLNA devices. Optionally, a DLNA media server, such as mediatomb, may be present in a mHealth Console to share content hosted locally.

3.8.1 DLNA Remote Access

In this section, we describe the simple case of how content at a Media Server connected to an mHealth Console in home 1 can be rendered on a Media Renderer connected to an mHealth Console in home 2 (can also be in doctor's office). While in the general case the media controller can be in a 3rd location, for simplicity we assume that the controller is also in home2. We assume that the both home 1 and home 2 have an mHealth Console and xDLNA application in mhc 2 has been configured to join the group <5020, mHealth.net>. Note that for convenience we use the same group that was also used by SIPP application in mhc2. Also assume that the xDLNA application in mhc1 has also joined the same group. This action could be trigged automatically, for instance, by the SIPP application in mhc1, when the SIPP join 5020@mHealth.net. Alternately a user may manually use a GUI to trigger this action. In any case, both the mHealth Consoles are now part of the overlay group 5020@mHealth.net.

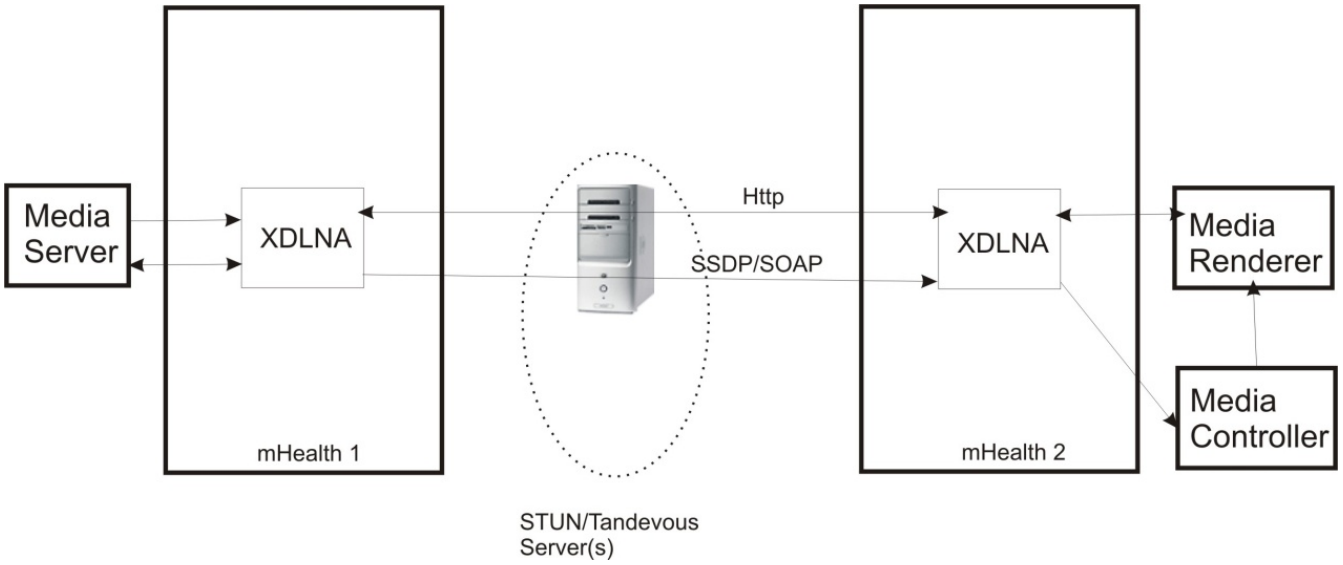

Figure 10. Exchanging media between two mHealth Consoles using DLNA service logic

Fig. 10 provides a pictorial representation of the logical connectivity between different functional entities. The xDLNA application discovers local devices and services (based on their multicast advertisements) and sends the information to its peer xDLNA applications using the overlay middleware. In this example, xDLNA1 (i.e. xDLNA in mhc1) sends information about the media server to xDLNA2 using the overlay middleware. On receiving this information, the xDLNA2 first maps the address/port in the SSDP message to a local address and re-advertise this information in their local domain. The media controller in home 2 receives this information and may then obtain additional information from the media server. This occurs transparently via the xDLNA applications. Finally the media controller sends a request to the media renderer in the local network to play a file. The media render receives the content from the media server, transparently via the xDLNA applications. Note that the media flows from the server to the render multiple split TCP connections. When there is congestion, for example in the typical case the bandwidth between mHealth Console is less than the bandwidth between the media server and the xDLNA application in home 1, the xDLNA application reduces the flow control window so that the different levels of congestion does not require large buffering in mhc1.

3.8.2 Mobile brokered DLNA Remote Access

The previous use case assumed that both homes have an mHealth Console. However in this use case we assume that only home 1 has an mHealth Console. In home 2 (or doctor's office) there is only a DLNA media renderer. Instead the mHealth portal hosts the necessary xDLNA functions and creates a virtual instance of media server in home 1. A mobile device, belonging to say a user in home 1, acts as a broker and provides a pointer to this virtual instance by joining the LAN of location 2.

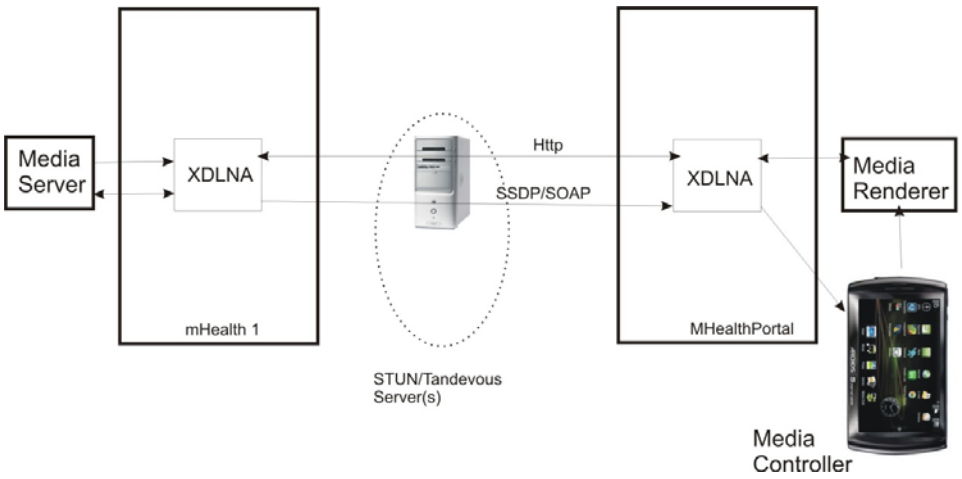

Figure 11. Exchanging media between a mHealth Console and Portal using DLNA service logic

Figure 11 provides a pictorial representation of the flow of messages. As in the previous case, the xDLNA application in home 1 discovers local devices and services (based on their multicast advertisements) and sends the information to its peer xDLNA applications using the overlay middleware. In this example, xDLNA1 (i.e. xDLNA in mhc1) sends information about the media server to xDLNA in the mHealth portal using the overlay middleware. On receiving this information, the xDLNA in the portal first maps the address/port in the SSDP message to a public address and re-sends this information to the mobile device that is registered with the portal. The mobile device in home 2 receives this information and advertises this locally. A media controller in the local network (say in the mobile itself) can browse the content by directly contacting the xDLNA in the mHealth portal. The media render also contacts the portal directly to receive the media.

3.9 Practical Implementation and Deployment

In this section we would describe in more detail how the features of the proposed solution are technically implemented and embodied in various consumer electronic devices.

Schematically the home environment of the patient who is subscribed to mHealth services could be presented as in Fig.12.

At the central position we have the mHealth Console which in fact represent a set of companion devices and sensor actuators used for data acquisition, pre-processing and storage, video and audio presentation, graphical presentation and interaction A number of portable sensors can be attached to the patient body taking measurements of relevant physical and bio-chemical parameters. The signals from these sensors would be A/D converted and sent to the mHealth Console over the wireless communication.

The patients' home environment is also comprehensively equipped with various environmental sensors providing a complete physical status of the environment in which the patient is living. They are also connected to the mHealth Console. This will provide many additional contextual data might have some relation/influence on the actual health conditions.

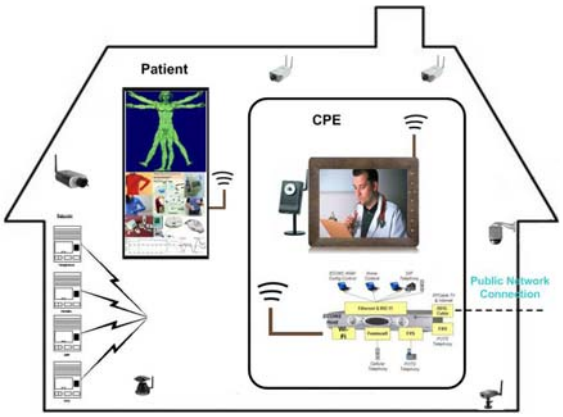

Figure 12. Patient's NeuroTech-Communication Home Environment

Additionally we can have number of motion sensing and/or video cameras, appropriately distributed around the patient's home feeds the video signals to the mHealth Console.

An application in the mHealth Console collects all these signals in a temporary buffer and processes them in order to detect the relevant event for the mHealth system. Care must be taken that all signals, coming from various sensors, over different connections, have to be time synchronized in order to construct a consistent set of data.

When the relevant event is detected, buffered signals, together with the signals recorded after the moment of detection would be combined into a single data structure and labeled as the "event content record". The event content record should in fact be carefully designed multimedia data structure characterized by its content and attributes. The content would comprise all recorded sensor and video/audio signals relevant to the detected event, appropriately stored in the data structure. The attributes would be in fact meta-data describing particular event content record (time it is recorded, size, format, medical condition, etc.)

Over the time the mHealth Console collects these event records and stores them in the local storage. Depending on the particular service, or user/system request, these records can be downloaded to the mHealth Cloud or used as a streaming transmission source.

The same collection process would be needed both during monitoring and rehabilitation phase of a given clinical condition.

4. SUMMARY AND CONCLUSION

This paper presents a comprehensive seamless service delivery solution that is well suited for mHealth applications.

The proposed service delivery concept is based on the OTT delivery enabling perspective mHealth provider to reach service users (e.g. patients, health insurance, health providers, employers, pharmacies etc) irrespective of ther locations, nature of their physical connectivity and offer services across heterogeneous networks, devices and operator domains, seamlessly. Detailed functional architecture for mHealth Console and Portal is given, signalling message flows for different SIP and DLNA based use cases are described as well as explanation of other supporting functions such as NAT, Randezvous servers etc.

The concept of mHealth Console and its powerful middleware architecture is well suited as the local sensory gateway, SIP and DLNA proxy as well as DM (device management) proxy.As such it might prove indispensable when it comes to local data pre-processing and local cashing in order to ensure the overall system/solution scalability and protection of data privacy.

The mHealth system is envisaged as a powerful ICT based solution that process comprehensive sensor data, both environmental and behavioral, from the AD and PD patients and their living environment and, based on virtual reality simulation provides monitoring and rehabilitation services to the patients.

The features of the proposed solution such as independent communication session initiation, seamless and automated exchange of stored and real time information and use of devices of affordable price, makes the proposed architecture a viable solution for seamless delivery of mHealth services.

5. REFERENCES

[1] Price Water House Coopers Health Research Institute.(2010), "Healthcare Unwired", available at: http://www.pwc.com/us/en/health-industries/publications/healthcare-unwired.jhtml [08.12.2010]

[2] Gatzoulis L. (2011-12), "Personal Health Systems", ICT WP 2011-12, Challenge 5 - Objective 5.1, available at: http://ec.europa.eu/information_society/events/cf/ict2010/document.cfm?doc_id=14587 [08.12.2010]

[3] ICT 2010 Conference, organized by the European Commission and hosted by the Belgian Presidency of the European Union, Brussels Expo, 27-29 September 2010, available at: http://ec.europa.eu/information_society/events/ict/2010/index_en.htm [08.12.2010]

[4] Conference session: WP 2011-12: Personal Health Systems (PHS), ICT 2010 Conference, available at: http://ec.europa.eu/information_society/events/cf/ict2010/item-display.cfm?id=3650 [08.12.2010]

[5] ICT - INFORMATION AND COMMUNICATION TECHNOLOGIES, Work Programme 2011-12, A Theme for research and development under the specific programme "Cooperation" implementing the Seventh Framework Programme (2007-2013) of the European Community for research, technological development and demonstration activities, available at: ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2011-12_en.pdf [08.12.2010]

[6] PHS research roadmap, developed by the project PHS2020, available at: http://ec.europa.eu/information_society/activities/health/docs/projects/phs2020/phs2020-roadmaps.pdf [08.12.2010]

[7] Consultation Workshop on Personal Health Systems, PHS 2010 consultation, 14 January 2010, ICT for Health Unit, DG Information Society and Media, European Commission, available at: http://ec.europa.eu/information_society/events/cf/ict2010/document.cfm?doc_id=13775 [08.12.2010]

[8] Wedge Greene, Barbara Lancaster (Dec 2007), "Over the Top Services", Pipeline Magazine, available at: http://tools.ietf.org/html/rfc2663 [08.12.2010]

[9] Srisuresh P., Holdrege M., RFC 2663 "IP Network Address Translator (NAT) Terminology and Considerations", available at: http://tools.ietf.org/html/rfc2663 [08.12.2010]

[10] Rosenberg J., Weinberger J., Huitema C., Mahy R., "STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", available at: http://tools.ietf.org/html/rfc3489 [08.12.2010]

[11] Rosenberg J., Weinberger J., Huitema C., Mahy R., "Session Traversal Utilities for NATs (STUN)", available at: http://tools.ietf.org/html/draft-ietf-behave-rfc3489bis-06 [08.12.2010]

[12] http://list.sipfoundry.org/archive/ietf-behave/pdf00000.pdf [08.12.2010]

[13] Rosenberg J., Mahy R., Huitema C., "Obtaining Relay Addresses from Simple Traversal Underneath NAT (STUN)", available at: http://tools.ietf.org/html/draft-ietf-behave-turn-02 [08.12.2010]

[14] Rosenberg J., "Internactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offser/Answer Protocols", available at: http://tools.ietf.org/html/draft-ietf-mmusic-ice-15 [08.12.2010]

[15] Rosenberg J., Schulzrinne H., "An Offer/Answer Model with the Session Description Protocol (SDP)", available at: http://tools.ietf.org/html/rfc3264 [08.12.2010]

[16] Bryan D., Lowekamp B., Jennings C., "dSIP: A P2P Approach to SIP Registration and Resource Location", available at: http://www.p2psip.org/drafts/draft-bryan-p2psip-dsip-00.txt [08.12.2010]

[17] Cooper E., Matthews P., Bryan D., Lowekamp B., "NAT Traversal for dSIP", available at: http://www.p2psip.org/drafts/draft-matthews-p2psip-dsip-nat-traversal-00.txt [08.12.2010]

[18] "Session Initiation Protocol", Wikipedia, available at http://en.wikipedia.org/wiki/Session_Initiation_Protocol [08.12.2010]