Case Study
The Teleservices and Remote Medical Care System (TRMSC)

The Teleservices and Remote Medical Care System (TRMCS) Prologue

This preliminary description is deliberately intended to be sketchy and imprecise. Acquisition, formalization and validation processes are needed to complete it and illuminate the many shadowy areas. A number of the requirements of the TRMCS system have a strong impact on the choice of the physical and logical architecture, these include safety critical requirements and economical ones.

Domain Theory: providing assistance to remote users

The current trend in healthcare is to transition patients from hospital care to home care as quickly as feasible. This leads to a need for new medical services to be delivered to the home. This type of patient does not need continuous assistance but might need prioritized assistance when urgencies happen, in which case the patient would call a help center for assistance.

The following two scenarios illustrate these new types of services.

Both assume some prior events where a patient/user has seen a physician and has been approved to receive at-home assistance and that the help center has prior medical information stored about each user registered with it.

1. A patient with a medical emergency sends a help request to a help center. The patient expects to receive the best help suited for his/her case within *a critical time range*. This help may take the form of emergency ambulatory service or online diagnosis and treatment from a health professional at a distance.

2. A patient may have internet-based medical monitors that give continuous readouts, e.g., EKG, EEG. A help center may contract to read these monitors over the net and raise alerts when dangerous values are detected. In essence, the monitoring software, as opposed to the patient, calls for assistance.

In both scenarios, the patient will typically be at his or her home. You can assume that the home has "reasonable" Internet access. Some patients, however, may be mobile, in which case either scenario may in involve mobile computing issues.

To gain approval from government regulatory agencies (e.g., the FDA), a help center must demonstrate that it can deliver the right care at the right time. In particular, monitoring software must be shown to be accurate in terms of detection and alert within specific critical time ranges. It must also be demonstrated that service availability can be provided reliable on a 24×7 basis. A "log" storing the history of inter-communication information (e.g., date, hour, type of request, user requesting the service, state of the request) may be used to certify that the system correctly behaved in controversial situations since it is responsible for delivering a service upon request in the right amount of time.

In the most general case, more than one help center would be in business. Help centers may be run from hospitals, from group practices, or from new medical centers that spring up to meet the need. The centers might form a networked consortium to share patient data, which brings up issues of patient privacy, validation of transmitted data (e.g., is the user eligible for the service? Has the message really been sent by the identified user?), and conformance to formatting standards. In addition, the help centers might compete for business. Hence, a call for assistance might be put up for open bid and help centers compete to answer it. The system must guarantee that at least one center responds.

There are also economic issues. Patients are willing to have this kind of service but may not be willing to, or simply are unable to, pay for it. In other words, they might be willing to pay for the assistance once received but not for the services provided to issue the request. This means the costs in this domain are critical, which might have an impact of the chosen physical architecture in terms of hardware and communication technologies.

System Requirements

The purpose of the TRMCS system is to provide and guarantee assistance services to at home or mobile users.

Any system delivered must meet medical information standards and regulations. This includes privacy standards enacted by government, and industry standards developed by consortia.

The system shall operate on near-future network and computing infrastructure and should scale as new technology becomes practical. For instance, personal medical-monitoring devices will be net-ready in the future, either through wired or wireless connections. A help center must be feasible given near-term compute serves and projected band-width to the home and mobile devices. The system should provide an architecture that allows new medical components to be brought into the mix. Similarly for the computational side, the system should support a range of compute servers, with a mixture of local (at-home) and remote (computational farms) resources.

The players or stakeholders of the system include individual patients, healthcare professionals who enter and maintain patient data, healthcare professionals who make treatment judgments in emergency situations (e.g., call for an ambulance, call for a teleconsulting session with a consulting physician), healthcare professionals who carry out online diagnosis and treatment, patient family members who provide assistance, and quality assurance professionals who provide initial testing of the system (e.g., to pass federal regulations) and runtime monitoring to verify the system continues to meet its goals.

Synthetically, the system should at least provide the following capabilities:

- Allow the user or monitoring software to issue help requests to the assistance center; request are issued asynchronously.

- Guarantee continuous service of the system.

- Guarantee secrecy of user data and secure communications.

- Handle several help request in parallel that compete for service by overlapping in time and space.

- Support conflict resolution according to resolution policies that minimize user damage.

- Be open to new service installation.

- Handle users that are geographically distributed and heterogeneously connected, offering homogeneous service costs.

- Handle dynamic changes to the number and location of users.

- Provide persistent repository of data and history log.

- Conform to medical information standards and regulations