INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Technical Paper

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(24 November 2006)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Audiovisual services

FSTP-RTM
Roadmap for Telemedicine

Summary

In the last years, the evolution of advanced digital telecommunications techniques, the fall of the costs for many of the information and communication technologies and the wide spread of Internet have enabled the development of the so called Information Society. In this environment, the use of Information and Communication Technologies (ICT) means to support medical needs which have specially had a great influence on the field of e-health. The use of multimedia systems to support e-health applications and new, highly sophisticated medical equipments are just two examples of the advances in this area.

In the actual social and medical context, marked by the rapid advance of telecommunication technologies which exposes the telemedicine applications to obsolescence, a policy of global standardization of all fields related to telemedicine could bring benefits like cost reductions and long-term investments without fear of depreciation. Other important advantages that make standardization completely necessary to guarantee the success of e-health applications are:

– Interoperability and compatibility, making easier the exchange of data among heterogeneous sources and facing the problem that most of the solutions up to now have been developed unfortunately on a proprietary basis so that it remains difficult and frustrating to put systems together.

– Public knowledge, fair competition and proper quality of performance, as the finally recognized standards should be freely available and continuously updated and upgraded by in charge working groups.

Ideally, suitable specifications – ITU and otherwise – would be internationally recognized as appropriate for e-Health applications. However, a basic consensus between standards development and later standards implementation is obviously needed. Looking for solutions along these lines, Q28/16 agreed in January 04 to develop an ITU-T Standardization Roadmap for Telemedicine. This Roadmap aims at defining the areas in which open global international standards for e-health applications are currently needed.

Before identifying these gaps, the Roadmap reviews the present situation and points out the main trends and future challenges. A key factor in each of the sections of the Roadmap is to review the proposed or already existing approaches before suggesting new solutions. The final version of this Roadmap shall provide the following:

– How technical, clinical and administrative processes are actually implemented, analyzing related best practices and former disappointing solutions and results.

– Describes how the processes are intended to work in the future, taking into consideration issues as quality, accessibility, cost effectiveness and patient and clinical acceptability.

– Clarifies the purpose and benefits of available standards, establishes the criteria to choose the best solution from the possible options, and provides guidelines for implementing the selected one.

Change Log

This document contains the first version of the ITU-T Technical Paper on "*Roadmap for Telemedicine*" approved at the ITU-T Study Group 16 meeting held in Geneva, 14-24 November 2006. Feedback are welcome and should be sent to:

Editor:	Vicente Traver BET –ITACA Universidad Politécnica de Valencia – Spain	Tel: +34 96 387 76 06 Fax: +34 96 387 72 79 Email: vtraver@itaca.upv.es
ITU-T SG 16 Secretariat:	International Telecommunication Union TSB / Place des Nations CH1211 Geneva 20 – Switzerland	Tel: +41-22-730-6805 Fax: +41-22-730-5853 E-mail: tsbsg16@itu.int

Contents

ITU-T Technical Paper
Roadmap for Telemedicine

1 Introduction

In the last years, the evolution of advanced digital telecommunications techniques, the fall of the costs for many of the information and communication technologies and the wide spread of Internet have enabled the development of the so called Information Society. In this environment, the use of Information and Communication Technology (ICT) means to support medical needs which have specially had a great influence on the field of e-health. The use of Multimedia Systems to support e-health applications and new-high sophisticated medical equipments are just two examples of the advances in this area.

In the actual social and medical context, marked by the rapid advance of telecommunication technologies which exposes the telemedicine applications to obsolescence, a policy of global standardisation of all fields related to telemedicine could bring benefits like cost reductions and long-term investments without fear to deprecation. Other important advantages that make standardisation completely necessary to guarantee the success of e-health applications are:

- Interoperability and compatibility, making easier the exchange of data among heterogeneous sources and facing the problem that most of the solutions up to now have been developed unfortunately on a proprietary basis so that it remains difficult and frustrating to put systems together.
- Public knowledge, fair competition and proper quality of performance, as the finally recognized standards should be freely available and continuously updated and upgraded by in charge working groups.

Looking for solutions on this line, in January 04 the development of the following roadmap for Telemedicine standards was approved in Geneva.

2 Objectives

In order to promote stronger coordination amongst the key players in the e-health standardisation area and avoiding duplication of efforts, this Roadmap draft aims to define the areas in which a set of open global international standards for e-health applications is currently needed.

Therefore, before starting to analyze the Roadmap for Telemedicine standards, it is important to review the present situation and point out the main trends for future challenges.

Nowadays there are many standardisation organizations already working on most of the fields listed below, but there is still a need to harmonize and coordinate these efforts and future evaluation strategies across projects in order to fulfil the real needs of standardisation. So, in each of the points of the roadmap structure it is a key factor to review the proposed or already existing approaches before suggesting new solutions.

The ultimate goal should be the arrival to a situation in which a group of de facto world used and ITU standards will be recognized internationally as suitable for their appliance in the new e-Health services assuring that new applications conform to them. This final endpoint should be achieved taking care of securing the participation of developing countries' interests, a maximum business orientation and preserving participation from all concerned parties, openness and transparency of the whole process.

A basic consensus between standards development and later standards implementation is obviously also needed. The framework of each point should highlight these key variables:

- How technical, clinical and administrative processes are actually implemented, analyzing related best practices and former disappointing solutions and results.
- Delineating how the processes are intended to work in the future assuring most relevant questions like quality, accessibility, cost effectiveness and patient and clinical acceptability.
- Making clear the functions and benefits of each possible standard, establishing the criteria to choose the best solution in between the possible options and finding out the way to implement the selected one.

All these ideas have to be regarded on the development of the following roadmap.

3 Roadmap structure

This roadmap covers the main points related to telemedicine issues, since telemedicine can be seen as the part of e-health where telecommunication systems allow interconnecting remote locations and accessing distant resources. The first part of the roadmap is oriented towards informatics and telecommunication matters, where the need of new standards development or adaptation of existing ones might be higher than in other fields typical of the classical medicine (like clinical data representation or data sets). These are also enumerated at the end of this document.

However, when looking for a common multimedia framework, the topics should be approached by trying to define the functionality and benefits of applicable (existing or future) standards, by finding out relevant information from related best practices and finally by establishing the criteria to choose the best solution amongst the possible options. By following this approach, particular aspects and needs of common examples of telemedicine applications like teleconsulting, teleradiology and telesurgery are identified.

4 Telemedicine Hardware

There are many possibilities in what refers to telemedicine hardware but none of them are included as goals of this document. The telemedicine hardware has its own market and should have as standards the already developed standards as USB, or Firewire for the internal communication bus or IrDA, USB Bluetooth for devices buses. This document will try to use existing standard communication protocols to define standardisation in e-health instead of standardizing or creating new ones.

5 Clinical Devices

Clinical devices are instruments used to asses the human condition and to deliver medical treatment.

Medical technology has benefited greatly by incorporating rapid advances in the science of information technology into many measurement and devices. But often this has been done in an unstructured manner with many devices being developed in an isolated way that makes impossible both communication between them and with hospital data management systems.

As the advantages of such communication became more and more obvious, a pressing need for technical standardisation and new protocols resulted in the creation of some standardisation activities. Great efforts were mainly held by the IEEE 1073, VITAL and the POCCIC (Point of Care Connectivity Industry Consortium) to enable communication to exist in an easy and open way, with subsequent clinical, administrative and research benefits.

As the question of interoperability raises many technical, safety, and legal issues which are worthy of consideration, each SDO addressed distinct fields: IEEE 1073 family of standards was recommended for heavyweight devices while POCCIC was recommended for use in lightweight devices where the overhead of 1073 would be prohibitive. VITAL deals with the vital signs representation, which is a pre-requisite for the development of true interoperability itself.

Like in other areas, telecommunication significant advances have transformed the way to understand this field in the last years. Using a complete data-transfer protocol such as RS-232, RS-422, or RS-485, or using wireless protocols such as Bluetooth, new functionality can be built into medical devices. That enables them in many cases to upload some of the manual tasks to the server. Traditional patient charts are replaced by the data delivered to a central processing station. These data are then analyzed and time-stamped by a knowledge-based engine and delivered to a nursing station in real time, along with an at-a-glance summary. Such a system eliminates delays between the gathering and the delivery of the information to the clinician. The systems are also designed to prevent manipulation of the database, ensuring the validity of the data.

Another great advance has occurred regarding home care medical devices. These allow the patient to receive appropriate assistance at home, checking the status of the individual on a daily basis by monitoring his specific vital signals.

A brief description of the main characteristics of the most common used medical devices is given below.

5.1 Spirometer

Spirometry is a methodology to measure how well the lungs take in air, the volume of air the lungs hold and how well the lungs exhale air.

The Spirometer is a precision differential pressure transducer for measurements of respiration flow rates. The information gathered during the test is useful in assessing certain types of lung disorders. The most common ones are Chronic Obstructive Pulmonary Disease (COPD) and Asthma. Spirometry can be used for assessing the severity of both of these respiratory diseases.

Spirometry with COPD patients requires two parameters to be measured:

Forced Vital Capacity - FVC (ml) which is the total volume of air that can be forcefully expired and Forced Expiratory Volume 1 - FEV1 (ml) which is the volume of air that can be forcefully expired in the first second.

Spirometry with Asthma patients requires just one parameter to be measured:

Peak Flow - PEF (ml/s) which represents how hard air can be expired from the lungs.

Connecting the spirometer to handheld or laptop devices typically via an RS-232 interface or through PC-Card technology makes it possible to upgrade online the internal software and to store patient results in a local data base. Besides, a usual network card and an HL7 interface allow spirometry results to be uploaded to a hospital or a lab electronic clinical record making them readily available for physicians review.

5.2 Capnographs

A capnograph is a medical instrument used in both hospitals and doctors offices providing feedback on the patient's airway condition and ventilatory status helping to identify situations that can lead to hypoxia if uncorrected. Attached to tubing near the end of the breathing or tracheotomy tube, they essentially measure the amount of CO2 in expired air from the lungs of a patient providing information about CO2 production, pulmonary perfusion, alveolar ventilation, respiratory patterns, and elimination of CO2 from the anaesthesia circuit. They are usually applied in different fields like

exercise testing, athletic training, critical care, operating rooms, sleeplabs, procedural sedation, when undergoing surgery or in an intensive therapy unit.

A classical RS-232 connector is commonly used as communication interface to transmit data to a computer.

5.3 Weight and Fat Scales

Related to nutritional matters, obesity is proven to cause or aggravate a wide range of health problems from high blood pressure, to arthritis, to certain forms of cancer. In fact, it is starting to be considered as one of the mayor health problems in many developed countries.

But it is fat and not weights, what represents in most cases a problem. Many experts believe that the percentage of body fat is a better measure of physical fitness than weight alone. A person who is "overweight" according to height-weight charts does not necessarily have too much fat. The extra weight may be due to an above-average amount of muscle. On the other hand, a person can be "overeat" even if they are not overweight, if they have too much fat in proportion to the muscle in their body. Until recently, measuring and monitoring body fat has been a complicated process. The most common methods required a trained technician, expensive equipment or uncomfortable procedures. Body impedance is measured when a small, safe electrical signal is passed through the body, carried by water and fluids. Impedance is greatest in fat tissue, which contains only 10-20% water, while fat-free mass, which contains 70-75% water, allows the signal to pass much more easily. By using the impedance measurements along with a person's height and weight, and body type: gender, age, fitness level, it is possible to calculate the percentage of body fat, fat-free mass, hydration level, and other body composition values. Conventional BIA normally uses underwater weighing as its method of reference. Using BIA to estimate person's body fat assumes that the body is within normal hydration ranges. When a person is dehydrated, the amount of fat tissue can be overestimated. Factors that can affect hydration include not drinking enough fluids, drinking too much caffeine or alcohol, exercising or eating just before measuring, certain prescription drugs or diuretics, illness, or a woman's menstrual cycle. Measuring under consistent conditions like proper hydration and same time of the day will yield best results with this method.

In the traditional BIA method, a person lies on a cot and spot electrodes are placed on the hands bare feet. Electrolyte gel is applied first, and then a current between 1 kHz and 150 kHz is introduced. BIA has emerged as a promising technique because of its simplicity, low cost, high reproducibility and non-invasiveness. BIA prediction equations can be either generalized or population-specific, allowing this method to be potentially very accurate. Selecting the appropriate equation is important for determining the quality of the results. To minimize variables caused by a person's hydration level, measurements should always be taken under constant and controlled conditions. For clinical purposes, scientists are developing a multi-frequency BIA method that may further improve the method's ability to predict a person's hydration level. New segmental BIA equipment that uses more electrodes may lead to more precise measurements of specific parts of the body. In these cases up to 8 electrodes should be placed on hands and feet.

Advanced BIA systems can be connected via USB or serial port to a laptop PCs or even to a handheld computer. So, the results can be shown graphically on the screen and downloaded to a local hard disk. The compilation of consecutive results offers the possibility of an historical follow up of the patient in order to adequate best individual diets to nutritional lacks.

5.4 Pulse Oximeter

Pulse oximetry is a simple non-invasive method of monitoring the percentage of haemoglobin (SpO2) which is saturated with oxygen. The pulse oximeter consists of a probe attached to the patient's finger or ear lobe which is linked to a computerised unit. The unit displays the percentage

of haemoglobin saturated with oxygen together with an audible signal for each pulse beat, a calculated heart rate and in some models, a graphical display of the blood flow past the probe.

A source of light originates from the probe at two wavelengths (650nm and 805nm) in the red-infrared spectrum. The light is partly absorbed by haemoglobin, by amounts which differ depending on whether it is saturated or desaturated with oxygen. By calculating the absorption at the two wavelengths the processor can compute the proportion of haemoglobin which is oxygenated. The oximeter is dependant on a pulsatile flow and produces a graph of the quality of flow. In cases of vasoconstriction where flow is sluggish the pulse oximeter may be unable to function. By taking advantage of new technological breakthroughs in signal processing, oximeters greatly improve analysis of the pulse signal and are capable of distinguishing pulsatile flow from other more static signals, such as tissue or venous signals, to display only the arterial flow.

Bluetooth connection between the patient and another host system is already available in some of the models but always taking care that medical devices usually act as slave Bluetooth terminals and are not able to initiate a communication.

5.5 Glucometer

Regular blood sugar testing is important to control diabetes and reduce long term complications. Different researches show that good control of blood sugar can lower the risk of eye disease, kidney disease and nerve damage that can develop due to diabetes.

A glucometer tests the level of sugar found in a drop of blood. Even though no other method capable of measuring this parameter in a non-invasive way has been developed up to now, there have been some advances in the blood test methodology. Actually just a tiny quantity of blood is needed for test because the sensor automatically draws the right amount. There is always more choice and flexibility about the part of the body where to test: finger, forearm, palm, abdomen or thigh.

Wireless technologies are being currently applied as state of the art solutions trying to minimize the impact on the patients' daily activities. Using Bluetooth technology in combination with mobile phones and body sensors opens up for remote wireless health monitoring applications as well, and will become increasingly important in future health care systems and services. Future plans involve sending the glucose data to health care specialists and diabetologists for statistical and follow up purposes.

Other researchers, like the latest breakthrough of the University of Pittsburgh, go even further and point to non invasive techniques. The state of the art technology is based on a thin plastic sensor that changes colour depending on the concentrations of glucose. They plan to embed the sensor material into contact lenses worn in the eyes. People wearing the sensors could check their glucose levels by looking into a specially designed mirror. The mirror, similar to a woman's makeup compact mirror, would have a colour chart. While looking in the mirror, the wearer could measure his or her glucose levels by comparing the colour of the sensor in their eyes to the colour chart on the mirror. The sensor turns red when it detects dangerously low glucose concentrations and turns violet to indicate dangerously high glucose concentrations. Green is the colour for normal glucose levels. However, it will be at least a year before the sensor is tested on humans.

5.6 Heart Rate Monitors

Medical literature is replete with evidence of the benefits of physical activity on health and longevity.

Basically all the heart rate devices in the market are designed to work in two pieces. Worn on the chest, the transmitter reads the electrical impulses of the heart and then wirelessly transmits the

ECG-accurate readings to a monitor, usually worn on the wrist. Some models offer also the possibility to direct the information to wired headphones.

Apart from the basic features of a heart monitor like to display the time of the day and the inherent ability to measure the heart rate, there are a lot of other different features depending on the model and the manufacturer. Visual or audible absolute heart rate alarms; complex data calculations and analysis like averages and disparities; more sophisticated data collection like the caloric consumption, altitude and VO2 estimation, representing the body's oxygen consumption; coding signal in order not to interfere with other devices; speed, pace and distance display, countdown timer, etc..

Some models collect precise information from the Heart Rate Sensor in larger memory banks. And through a USB connection, this data can be later uploaded to a PC, and used with proprietary software to chart the progress and achieved goals, and to maximize the workouts.

5.7 ECG and Holter

An electrocardiogram (ECG) is a test that records the electrical activity of the heart.

An ECG is a non-invasive, quick, safe, painless and inexpensive test that is routinely done if a heart condition is suspected. The ECG records the heart's electrical activity, traditionally as a graph or series of wave lines on a moving strip of paper. This information gives a physician important information about the heart.

Latest Information and Communication Technologies are being applied in the new generation of ECG systems. PDA devices, compatible with the latest Bluetooth, GPRS and wireless LAN technology, offer great expectations in mobile health diagnosis allowing a user definable 3 or 6 lead views on a crystal clear colour TFT screen. Multiple ECGs can be stored and be downloaded directly into a patient management system. And some models even have the option of an infra red print.

A Holter Monitor is intending to be a portable version of an ECG. It provides continuous recording of a limited ECG for 24 or 48 hours. You will be connected to a small portable recorder by a few electrodes on the chest. The device is being carried for the allotted time and records on a diary the activities as well as the occurrence of any symptoms. Electrodes in form of small conducting patches are placed on the chest and attached to a small recording monitor that can be carried in a pocket or in a small pouch worn around the neck. The monitor is battery operated.

5.8 Echocardiograph

Also known simply as an "echo", echocardiography uses high-frequency sound waves to get a picture of a particular part of the body. For instance an echocardiogram of the heart's chambers and valves, which is one of the most common ones, is called a transthoracic (across the chest) echocardiogram. In that case, the sound waves bounce back from the heart chambers and the four heart valves, producing images and sounds that can be used by the physician to detect damage and disease. It is painless and because it does not involve any of the radiation that an x-ray does, it is a very safe test. In fact, it uses the same technology that is used to evaluate a baby's health before birth.

To perform an echocardiogram, a special gel is placed on the chest over the area being examined. A small device called transducer is then moved over the gelled area and images can be seen immediately on a video monitor

There are many different types of echocardiograms, which include:

- One-dimensional, two-dimensional, or three-dimensional echocardiograms.

- Doppler ultrasound. Measures the speed with which blood is travelling through the heart.
- Stress echocardiogram. Measures the wall motion of the heart's pumping chamber before and immediately after exercise, generally the test is made on a treadmill or stationary bicycle.
- Chemical stress echocardiogram. Measures the wall motion of the heart's pumping chamber using a drug that causes the heart to react as if the person were exercising.
- Transesophageal echocardiogram (TEE). Produces clear images of the heart structures and valves, without the interference of the chest wall and lungs. A transducer is placed down the patient's throat, into the oesophagus.
- Intravascular echocardiogram. Produces clear images of plaque and calcium deposits on the inside of a blood vessel. A transducer is placed inside the blood vessel.

5.9 Thermometer

Digital thermometers are easier to read than traditional thermometers and don't contain mercury, which is a known health risk if the thermometer breaks. In between the different possible techniques, ear temperature measurements are recognized to be the most significant and accurate. Ear temperatures measures the infrared heat generated by the eardrum and surrounding tissue. They accurately reflect core body temperature, since the eardrum shares blood supply with the temperature control centre of the brain, the hypothalamus. Therefore, changes in body temperature are reflected sooner and more accurately in the ear than at other sites.

Through this technique, instant readings are possible in one second assuring also high accuracy by taking 8 measurements or more in this second and displaying just the highest temperature. There is no need to put a thermometer in anyone's mouth and the risk of cross contamination is virtually eliminated by the use of the disposable lens filters. An audible beeper indicates start and finish of the measurement and Fahrenheit and Celsius measurement scales are available in a great part of the models.

5.10 Defibrillator

A defibrillator is a device that is designed to pass electrical current through a patient's heart. The passing of electrical current through the heart is called defibrillation. A defibrillation is done through pads placed on the patient's chest. This technique is used to restore a patient's heart rhythm to normal. Abnormal heart rhythms may be treated with medications while other rhythms need to be treated with defibrillation. Life threatening heart rhythms need defibrillation immediately while other heart rhythms may be defibrillated in a scheduled fashion. Defibrillation may be done using the manual defibrillator or the automatic external defibrillator (AED). Patients needing emergent defibrillation are usually unconscious and do not feel the defibrillation. Patients with abnormal but stable heart rhythms needing defibrillation will receive sedation and pain medication before the defibrillation is done. However, patients usually have no memory of the defibrillation. Defibrillators pads may cause a skin irritation and leave a temporary redden area where they contacted the chest. Unfortunately defibrillation does not always return the patient's heart rhythm back to normal.

As a CPR previous to the defibrillation is proved to increase the chances of survival, most of the defibrillation devices provide coaching for adult/child CPR. With voice instructions and timing cues for each breath, the appropriate number and rate of chest compressions, and the duration that CPR should be performed.

5.11 Foetal and Maternal Monitoring

For monitoring of pregnant women and helping to manage the total pregnancy - from antepartum monitoring through labour, delivery and recovery -, a portable foetal and maternal vital-signs monitor presents comprehensive data for both mother and baby on a single display. These devices also provide modem transmission of medical data to a physician or medical facility for analysis and consultation.

After the entry of maternal parameters such as non-invasive blood pressure, weight, temperature, blood glucose and urine albumin, the device gives typical measures like foetal heart rate and uterine contractions. Foetal movement marking trough a touch screen and then transferred directly to a PC via an infra-red link are also part of the current possibilities of these devices.

5.12 Multiparameter devices

Multiparameter devices provide a cost-effective and relatively non-heavy solution (around 3-4 Kg) for complex patient monitoring. These systems pack and offer a comprehensive number of functions associated to ECG, NIBP (Non Invasive Blood Pressure), respiration measures, SpO2 and temperature. These types of devices are commonly used in scenarios like ambulances or aircraft assistance in which space conditions are not great.

Specially designed for telemedicine and home care applications, some models transmit the data wirelessly to a gateway, which then forwards this information via internet to a telemedicine call centre or a secure data repository.

Additional features like pacemaker detection, apnoea alarm function, capnography measurements and arrhythmia analysis can be available depending on the model.

A typical multifunctional monitoring equipment could be formed by following modules. A blood pressure monitoring apparatus: for measuring the blood pressure and pulse of the patient; a cardiovascular monitoring apparatus: which, if necessary, can be connected to an external pacemaker; a pulse oximeter for measuring the amount of oxygen in the blood; a capnograph, which indicates how much carbon dioxide is exhaled from the lungs helping the doctor to determine the quality of the ventilation and increase or reduce the amount of oxygen accordingly.

As seen in the previous analyzed devices, here new wireless communications capabilities have been also added to transfer the data to a central processing station.

5.13 Future trends and standardisation field efforts

The standardisation activities in the field of medical devices have to be coherent with the rapid advance of the new technologies in this field.

6 Specifications for real-time group work and video conferencing

Standard specifications for real-time group work and video conferencing should cover the many different communication aspects involved in this area, from real time protocols to dedicated hardware like videoconferencing cameras.

6.1 H.323

ITU-T Recommendation H.323 provides a cornerstone foundation for audio, video, and data communications over packet-based networks. It specifies the components, protocols, and procedures needed. Its utility includes the Internet, private global networks, corporate LANs, MANs and WANs. While it may operate over a variety of transports, H.323 is almost exclusively used only on IP networks. This has not limited the use of H.323. In fact, H.323 is successfully used for

communication between users over wired and wireless links, including satellite and microwave links. H.323 can be applied in a variety of areas: audio, audio and video (videotelephony); audio and data; and audio, video and data. H.323 can also be applied to multipoint-multimedia communications. Many products from many vendors interoperate to form complex systems for health, education and industry being applied in consumer, business, and entertainment areas. H.323 interoperates particularly well with H.320 and other VoIP applications, so that a single infrastructure can support voice and video both on the IP network and PSTN, the traditional wired phone lines. In this sense, the benefits obtained from the cost balance of VoIP appliance for voice communications over Internet could signify a great chance for implementing telemedicine applications into developing countries. H.323 operates over IP networks, regardless of the access technology. This means that H.323 can be used over cable, DSL, WiFi, WiMAX, microwave links, etc. In developing countries, various wireless access technologies may be more cost effective than traditional PSTN wiring, this better enabling IP and H.323 communication. H.323 actually supports the same addressing mechanisms as SIP; both standards have the same kind of call transfer, hold, services, etc

H.323 was first defined by the ITU in 1996 and has been regularly updated by means of annexes, related Standards, and amendments to the base text on matters like: robustness, transfer of modem signals, far-end camera control, etc. The most recent version is H.323 version 6 (2006). The ongoing work is focused on: interworking with SS7 and other networks, communication over error prone connections like wireless, quality of service, NAT and firewall traversal and integration with other IP-based communication systems including presence, instant messaging, etc. There is a continued focus on improving and maturing the protocol, adding functional capability where vendors and service providers identify a need for specific enhancements.

The H.323 is an “umbrella” specification that includes the standards H.225.0, H.245, the H.235-series, the H.450-series documents, and the H.460-series and also allows the use of T.120 for data collaboration and file transfer. However, not every document is mandatory as part of a standard H.323 system. For example, H.460.2, which describes number portability, is generally not used in enterprise videoconferencing systems.

H.323 was designed with multipoint voice and video conferencing capabilities, though most users do not take advantage of the multipoint capabilities specified in the protocol. Initially designed for communication over Local Area Networks (LANs), the scope of H.323 has long since expanded to include any kind of packet-based network. Even so, LANs are popular and overwhelming networks that include packet-switched TCP/IP and IPX over Ethernet, Fast Ethernet and Token Ring network technologies. Therefore, the H.323 standards are an important basis for a broad new range of LAN-based applications for multimedia communications. It includes RTP/RTCP for audio and video transmission and audio codecs (G.711, G.723.1, G.728, etc.) and video codecs (H.261, H.263) that compress and decompress media streams.

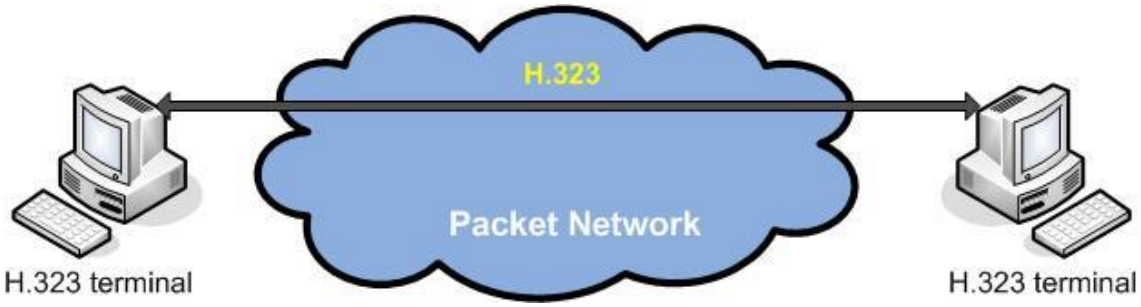

Figure 1: H.323 communication

The H.323 standard specifies four kinds of components which provide the communication services: terminals, gateways, gatekeepers and multipoint control units. An H.323 terminal can be a PC or a stand-alone device with the capability to interwork with other multimedia terminal like: H.324 terminals on wireless networks, H.310 and H.321 terminals in B-ISDN, H.320 terminals on ISDN and H.322 terminals on guaranteed QoS LANs. A Gateway connects dissimilar networks (i.e., an H.323 network and a non-H.323 network). This is achieved by translating protocols for call setup and release and converting media formats. However, a gateway is not required for communication between terminals in a H.323 network. Gatekeepers provide services like address resolution, bandwidth management, accounting, billing, charging, authorization and authentication in an H.323 network. Finally, Multipoint Control Units (MCU) support conferences between terminals and Gateways by managing conference resources and negotiating media capabilities between terminals.

A typical H.323 terminal is logically implemented as shown below[1]:

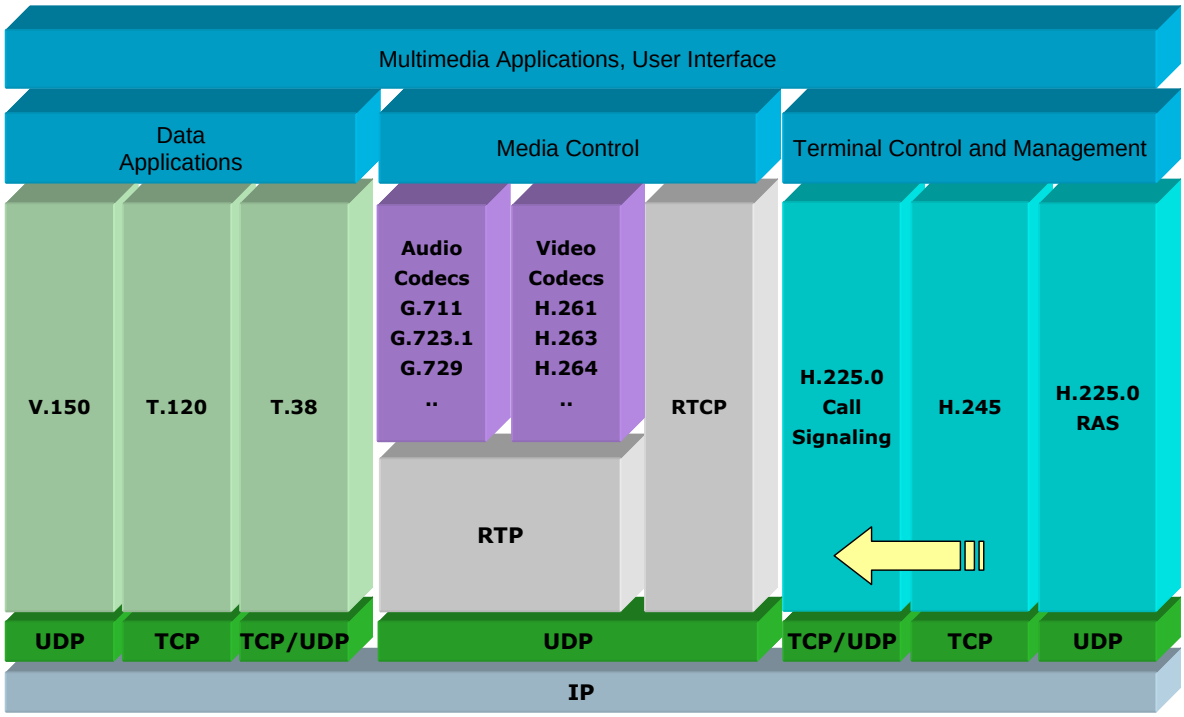

Figure 2: H.323 stack protocol

6.1.1 Audio codec

An audio CODEC encodes the audio signal from the microphone for transmission on the transmitting H.323 terminal and decodes the received audio before it is sent to the speaker on the receiving H.323 terminal. Because audio is the minimum service provided by the H.323 standard, all H.323 terminals must have at least one audio CODEC support, as specified in the ITU-T G.711 recommendation (audio coding at 64 kbps). Additional audio CODEC recommendations such as G.722 (64, 56, and 48 kbps), G.723.1 (5.3 and 6.3 kbps), G.728 (16 kbps), and G.729 (8 kbps) may also be supported. H.323 is designed to enable use of any codec, with capability advertisement and logical channel signalling procedures defined such that any standards body or company may define a means of signalling and using a codec within H.323 systems.

[1] Extracted from http://www.packetizer.com/voip/h323/papers/h323_protocol_overview.ppt (Paul Jones)

6.1.2 Video codec

A video CODEC encodes video from the camera for transmission on the transmitting H.323 terminal and decodes the received video before it is sent to the video display on the receiving H.323 terminal. Because H.323 specifies support of video as optional, the support of video CODECs is optional as well. However, any H.323 terminal providing video communications must support video encoding and decoding as specified in the ITU–T H.261 recommendation. Use of other video codec's can optionally be negotiated by the endpoints (e.g. H.263, H.264 etc.).

6.1.3 H.225.0 Registration, Admission and Status

RAS is the protocol used between endpoints and gatekeepers to perform registration, admission control, bandwidth changes, status and disengage procedures. This channel is established prior to any other communication.

6.1.4 H.225.0 Call Signalling

This is used to establish communication between endpoints by exchange of messages trough a dedicate channel.

6.1.5 H.245 Control Signalling

This protocol is used to exchange end-to-end control messages with information related to: capabilities exchange; opening and closing of logical channels used to carry media streams; flow-control messages and general commands and indications.

6.1.6 Real-Time Transport Protocol

RTP (IETF RFC 3550) provides services of real-time audio and video delivery. This protocol is commonly applied to transport data over the user datagram protocol (UDP). RTP provides payload type identification, sequence numbering, time-stamping and delivery monitoring.

6.1.7 Real-Time Transport Control Protocol

The primary function of RTCP is to provide feedback on the quality of the data distribution as a control service. This protocol is also used by receivers to synchronize audio and video.

Other protocols for supporting videoconferencing

6.2 SIP

The Session Initiation Protocol is a signalling protocol for Internet. By means of SIP mechanisms, end systems and proxy servers can provide services such as call forwarding, called and calling number delivery, terminal capability negotiation; caller and called authentication; blind and supervised call transfer invitations to multicast conferences and personal mobility, i.e. the ability to reach a called party under a single, location-independent address even when the user changes terminals, terminal-type negotiation and selection. Extensions of SIP to allow third-party signalling are available. It is worth to state that H.323 can also do all of these things.

SIP addresses users by an email-like address and re-uses some of the infrastructure of electronic mail delivery such as DNS. SIP addresses can also be embedded in web pages. SIP is addressing-neutral, with addresses expressed as URLs of various types such as SIP, H.323 or telephone. SIP can also be used for signalling Internet real-time fax delivery. This requires no major changes. Fax might be carried via RTP, TCP or other mechanisms.

SIP is independent of the packet layer and only requires an unreliable datagram service, as it provides its own reliability mechanism. While SIP typically is used over UDP or TCP, it could, without technical changes, be run over IPX, frame relay, ATM AAL5 or X.25.

6.3 H.320

This protocol has a long and successful history with its foundation in 1985. H.320 supports videoconferencing over ISDN and switched networks. H.320 includes the standards H.242 and H.243 and paved the way for the H.323 specification. Private industry still relies heavily on this protocol, and it provides an important bridge to the PSTN.

6.4 H.321

H.321 provides support for videoconferencing over ATM. The H.321 protocol is designed to support H.320 compressed video using ATM switched virtual circuit transport. The use of switched virtual circuits conserves network bandwidth by only using it when a conference is actually in progress. It also conserves network resources because point-to-point conferences do not need the services of a multipoint control unit.

6.5 H.324

H.324 was originally designed for low bandwidth videoconferencing over PSTN utilizing V.34 modems. H.324 terminals may carry real-time voice, data, and video, or any combination.

H.324 terminals make use of the logical channel signalling procedures of ITU-T Rec. H.245, in which the content of each logical channel is, described when the channel is opened. H.324 terminals may be used in multipoint configurations through MCUs, and may interwork with H.320 terminals on the ISDN, as well as with terminals on wireless networks.

In 1998, after the approval of Annex C and Annex D, H.324 was extended to be used in mobile (error-prone transmission environments referred to as H.324/M) and ISDN. In 2006, the ITU-T, 3rd Generation Partnership Project (3GPP) and International Multimedia Teleconferencing Consortium were integral in shaping the resulting solution, the newly created Annex K. This Annex K, also known as Media Oriented Negotiation Acceleration (MONA), is the result of more than 18 months of industry discussions and collaboration to achieve a standardized call session acceleration technique. Long session setup times are recognized as one of the limiting factors for consumer acceptance of video telephony services. Annex K of H.324 contains a range of techniques to substantially improve session setup times, reducing call setup negotiation time to the equivalent of a voice call.

6.6 H.350

H.350 provides directory services for a variety of conferencing protocols including H.323, SIP, H.320 and non-standard protocols. It makes it easy to find and dial users, support identity management to allow for high scalability in deployments, and store call handling preferences.

6.7 T.120

T.120 is a data collaboration conferencing standard often used in conjunction with videoconferencing protocols to provide application sharing, electronic whiteboarding, file transfer, text chat, and other data services.

6.8 Cameras

Videoconferencing cameras adhere to one of the following standards:

6.8.1 EIA RS-170

In the United States, RS-170, produced by the Electronic Industries Association, embodies the technical specifications that were originally defined in the late 1930s in order to standardize the black and white TV industry. RS-170 defines an aspect ratio of 4:3, a 2:1 interlaced scan technique,

and horizontal and vertical sync pulses. An entire RS-170 frame consisting of one even and one odd field is made up of 525 lines; each frame is sequenced out every 33.33 milliseconds. The vertical sync interval and settling period chew up 20 line times per field, however, leaving 242.5 lines per field or 485 lines per frame for image. RS-170 also specifies electrical voltages.

6.8.2 NTSC

In the 1950s, the National Television Systems Committee adapted the RS-170A colour standard, widely known as NTSC. NTSC describes a composite colour signal created by combining colour and brightness information on a single signal. Hue and saturation are combined using phase and amplitude modulation techniques into a single chrominance signal. This is added to the RS-170 brightness signal, together with a reference called colour burst at the start of each line. The NTSC system allows the coexistence of monochrome and colour television, a very important constraint at the time it was introduced.

6.8.3 CCIR

The CCIR video standard is the European equivalent of RS-170. CCIR specifies a 625-line image with a frame rate of 40 ms, a 2:1 interlaced scan, and a 4:3 aspect ratio. The CCIR standard was also adopted for colour; this is known as PAL (Phase Alternate Line). However, France, Russia and a few other countries use a third standard called SECAM (Séquentiel Couleur Avec Mémoire).

6.8.4 Y/C-Video

While component systems carry the R-G-B colour information on separate signals, and composite signals carry all the information on one signal, an intermediate standard has evolved. The Y/C component colour standard conveys the colour video signal as a luminance (Y) signal identical to the standard RS-170 monochrome video signal and a chrominance (C) signal identical to the chrominance subcarrier defined in the NTSC standard. However, by using separate signals, a higher quality level is achieved. Y/C video is also known as S-Video, super-video, and S-VHS. Many videoconferencing systems handle NTSC and S-video signals.

RS-170 was optimized for the human perceptual system and the technology available to the broadcast TV industry decades ago. Interlaced video reduces flicker for the human eye and 30 frames per second eliminates many noise problems associated with 60 Hz power supplies. The 4:3 aspect ratio makes for a pleasing TV image. But these technologies are not well suited for the computer industry. For example, with interlaced lines coming off a camera, the computer, which uses progressive scan, has to reorder the data to make a sensible image while in the human eye this is done automatically. And for applications like videoconferencing, where other constraints may limit a system to 20 frames per second or slower, being locked in to the 30 frames or 60 fields per second specified in RS-170 has no logical basis and is a distinct disadvantage.

Therefore here are the steps that need to take place on a desktop videoconferencing system:

The camera’s sensor produces an analog signal of an image. The camera then converts the analog signal coming off the sensor to a digital signal that is compatible with the camera's internal processor. The camera’s processor then processes the digital signal to produce the required data stream. This data stream is then encoded back to an industry-compliant analog signal i.e. NTSC or PAL and fed into the computer. The signal must be converted back to digital using a chip in the PC. Typically this is done on a frame grabber board, also known as a camera interface. The videoconferencing application can now process the image.

The process of converting an analog signal to a digital signal to an analog signal then back to a digital signal seems wasteful, and expensive. This is the basis for the interest in digital cameras for the PC industry, and videoconferencing in particular. There really is not any reason to stay with the NTSC constraint, other than most cameras are NTSC devices. Digital cameras do away with all the

convolutions described above and send a digital signal back, sometimes already compressed, to the videoconferencing host through one of several interfaces. Current performances include:

- The delivery of full image resolution at a full 30 frames per second to the PC bus;
- To be powered directly from the PC, eliminating the need for an external power pack;
- PC interface and image processing are performed at the PC end of the camera cable, either on an add-in card or on the motherboard itself;
- Only 8 bit pixel samples need to be transported to the PC instead of 16 bit YUV processed pixels;
- With a convenient camera head control capability in place, host software can interrogate the camera's EEPROM chip to learn specific and useful data about the connected camera, such as resolution, bias setting, colour calibration, and even serial number;
- Software controls include variable frame rate and continuously variable exposure times;

For digital devices, there are several ports on a PC that customers can use, including the keyboard port, mouse port, joystick port, serial port, parallel port, audio in port, video in and video out ports, and proprietary ports used by specific manufacturers for specific devices. This is usually confusing to the end user. The key aspect behind new technologies is the standardisation of a single connector for a wide variety of devices. New digital cameras use one of four approaches to connecting to the PC: proprietary interfaces, parallel ports, FireWire, or USB. The last three do not require the user to open the PC, a major advantage.

A common approach today is to use the parallel port. The major advantage is that the parallel port is available on all PCs. The disadvantage is that the parallel port imposes a limit to videoconferencing performance.

FireWire/IEEE 1394 is a complex, IEEE standard serial bus. FireWire promises several advantages, including speeds up to 400 Mbps, isochronous support, linking of up to 63 devices, and ease-of-use through automatic configuration. FireWire interface boards are now coming to market, and motherboard implementations are likely to follow.

Universal Serial Bus (USB) is peripheral bus designed to provide a plug and play environment without rebooting outside the box, eliminating the need install cards into dedicated computer slots and to reconfigure the system. USB allows up to 127 devices to be connected simultaneously to a computer. The bus automatically determines what host resource, including driver software and bus bandwidth, each peripheral needs and makes those resources available without user intervention. USB peripherals, including keyboards, monitors, mice, joysticks and videoconferencing cameras have already hit the market. The USB provides high-speed data transfer rates of 12 megabits-per-second, as compared to standard PC serial port rates of 115 kbit/s. USB also provides isochronous and asynchronous data transfer as well as a star-hub architecture that makes it possible for a single PC port controller to link up to 63 digital peripherals.

USB and FireWire/IEEE 1394 are likely to coexist for quite some time and together will dominate the future of the PC peripherals market. USB is low cost and better suited for slower speed PC connections like keyboard, mouse, etc. USB's data rate is adequate for many multimedia applications if the bus is not shared by lots of peripherals. FireWire, which uses more expensive chips and cables, will be used for higher-speed multimedia connections.

7 Messaging Standards

7.1 Background information

7.1.1 Definitions of EHR (Electronic Health Record)2

It is first necessary to agree on the meaning and scope of the EHR itself[3]. There is as yet no single ISO definition of the EHR. These definitions range from very succinct to quite lengthy and encompass a range of somewhat different scopes. This is not surprising since several of these definitions originally referred to the more or less variant names for the EHR including the EHCR (Electronic Health Care Record), EPR (Electronic Patient Record), CPR (Computerized Patient Record), and EMR (Electronic Medical Record). Whilst it is recognised that these terms are sometimes given different shades of meaning in different countries and different health sectors (e.g. the English NHS makes a distinction between the EHR and the EPR), it is intended that the requirements for standards related to Technical Specification will generally apply to all of these variants.

7.1.2 National Initiatives and nomenclature

PMRI – Patient Medical Record Information (US)

ICRS – Integrated Care Record Services (UK)

CMR – Computerized Medical Record (US)

CPR – Computer-based Patient Record (US, Int)

PCR – Patient-carried (Card-based) Patient Record (G)

PHR – Personal Health Record (Int)

EMR – Electronic Medical Record (US)

DMR – Digital Medical Record (Asia)

EPR – Electronic Patient Record

EHR – Electronic Health Record

LHII – Local Health Information Infrastructure for EHRs (US)

CCR – Continuity of Care Record (US)

7.1.3 Electronic record essential attributes

The electronic record must include eight essential attributes[4]:

- Provide secure, reliable and real-time access to patient health information where and when it is needed to support care.
- Capture and manage episodic and longitudinal electronic health record information.
- Function as clinicians' primary information resource during the provision of patient care.

---

[2] Academic Reference: "Good Characteristics of a EHCR" (Eurorec 1997, Paris). Werner Ceusters, Belgium

[3] ISO/TS 18308 ISO TC 215/SC /WG 1 (2003-04-23)

[4] [(July 09, 2003)US, The Healthcare Information and Management Systems Society, http://www.himss.org]

- Assist with planning and delivering evidence-based care to individuals and groups of patients.
- Support continuous quality improvement, utilization review, risk management and performance management.
- Capture information necessary for reimbursement.
- Provide longitudinal, appropriately masked information to support clinical research, public health reporting and population health initiatives.
- Support clinical trials.

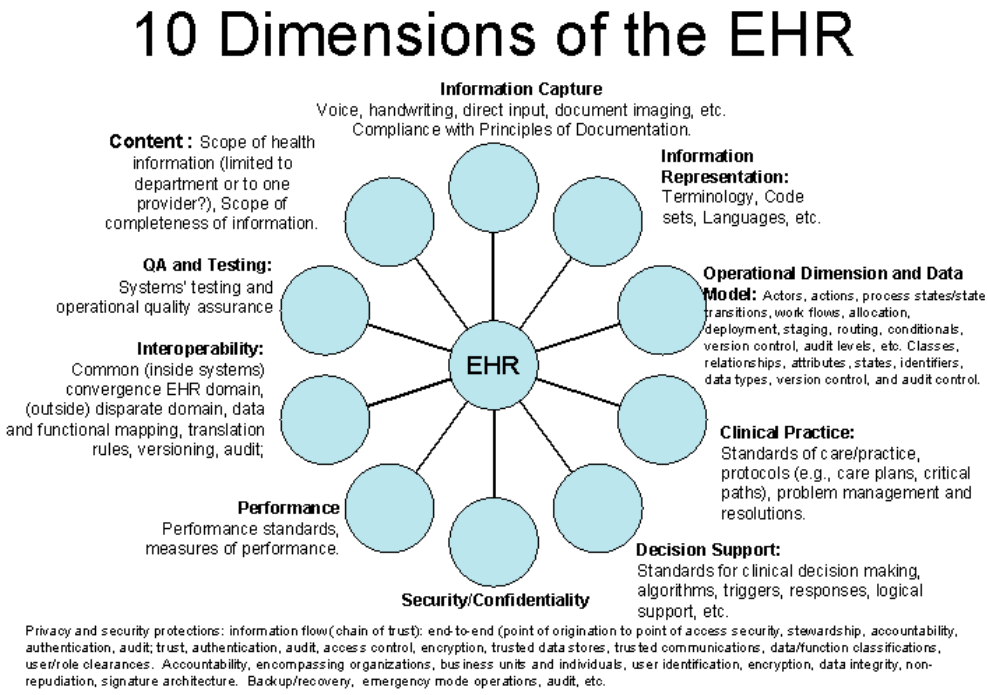

Figure 3: 10 Dimensions of the EHR

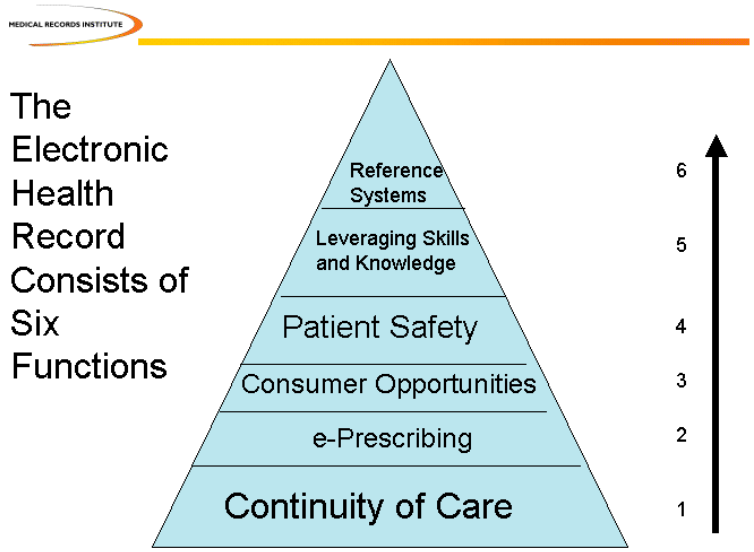

Figure 4: Functions of EHR

7.1.4 EHR architecture5

The principal definition of an electronic health record architecture (EHRA) used in this Technical Specification is:

- "the generic structural components from which all EHRs are built, defined in terms of an information model".

A more descriptive definition is:

- "a model of the generic features necessary in any electronic healthcare record in order that the record may be communicable, complete, a useful and effective ethic-legal record of care, and may retain integrity across systems, countries, and time. The Architecture does not prescribe or dictate what anyone stores in their healthcare records. Nor does it prescribe or dictate how any electronic healthcare record system is implemented. ... [It] places no restrictions on the types of data which can appear in the record, including those which have no counterpart in paper records. ... Details like "field sizes", coming from the world of physical databases, are not relevant to the electronic healthcare record Architecture." (EU-CEN, 1997)

Note that the exclusions specified in this definition highlight the ability of an EHR architecture to encompass a variety of different EHR implementations to suit different purposes.

The EHR architecture should be broadly applicable to all healthcare sectors, professional healthcare disciplines, and methods of healthcare delivery. A "consumer" or "personal" EHR should be able to conform to the same EHR architecture as a more traditional EHR used by providers such as medical specialists, nurses, general practitioners and providers of allied health services.

An open standardised EHR architecture is the key to interoperability at the information level. A standardised EHR architecture enables the whole or parts of the EHR to be shared and exchanged between authorized members of a multi-disciplinary care team, including the patient/consumer, independently of any particular EHR system. EHR information conforming to a standardised EHR architecture should be capable of being accepted, processed and presented by an EHR system that uses the EHR architecture irrespective of the source application or the operating system, database, and hardware on which the EHR system depends.

7.1.5 Why do we need EHR?[6]

- Manage increasingly complex clinical care
- Reduce errors and inequalities
- Reduce duplication and delay
- Connect multiple locations of care delivery
- Deliver evidence-based health care
- Underpin population health and research
- Empower and involve citizens in their health agenda

---

[5] ISO/TS 18308:2004 – Health informatics - Requirements for an electronic health record architecture

[6] Dipak Kalra, OpenEHR presentation at EUROREC 2004

- (Maybe reduce healthcare costs)

The good EHR (academic definition). Ten quality criteria:

- Comprehensive
- Faithful
- Life-long (and beyond)
- Medico-legally rigorous
- Educating
- Supporting diverse cultures and professions
- Capable of evolution
- Empowering and respecting
- Appropriately ubiquitous
- Capable of interoperability

7.1.6 History of EHR in Europe:

Twelve years of European R&D, especially FP4:

- Past EHR Projects (http://www.ehto.org):
    - GALEN, SYNAPSES, SYNEX, I4C, HANSA, GEHR, PROREC, EHCR-SUPA, TOMELO, TELENURSE
- Regional Health Info Projects
    - COCO, CHIN, STAR, REMEDES, ITHACA, PRESTIGE, OPENLABS, EUCLIDES

Lessons learned:

- Ensure well thought-out strategy
- Break the pattern of large scale all at once implementations
- Ensure commitment of the "leaders"
- Keep it up... do not just set it up
- Ensure (legal and ethical) compliance
- Do not underestimate user acceptance
- None of the parties can do it alone!

The Need to address the challenges and to disseminate lessons lead to support of Prorec ('96) and EHTEL ('98) → searching for more stable platforms

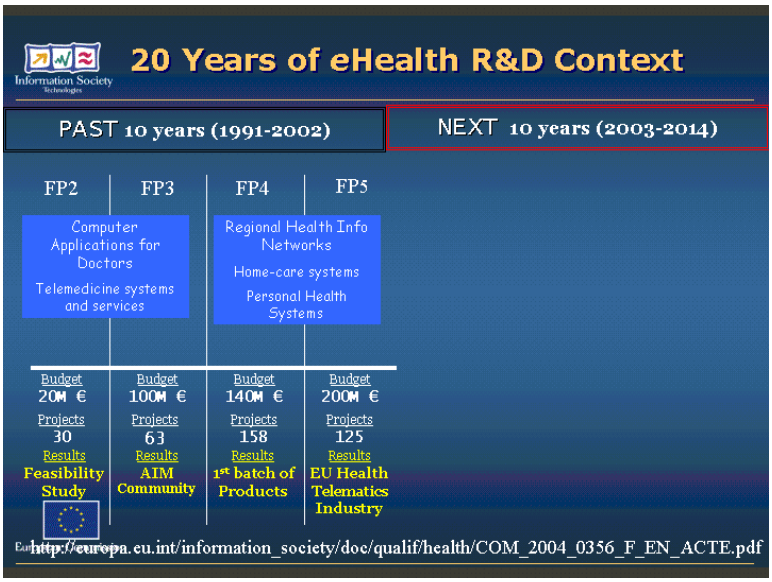

Figure 5: 20 years of e-Health R&D Context

- Two generations of CEN standard
- Well-published requirements
- Public domain EHR specifications

Figure 6: Research on EHR interoperability in Europe

[7] EHRcom: the key to full interoperability of Electronic Health Records, Dr. François MENNERAT, MD PhD, Chairman of ProRec-France, Secretary General of the EuroRec Institute

Figure 7: European research projects on EHR interoperability

Up to now:

- large implementation failed to stimulate wide-scale EHR adoption and interoperability

But now:

- Technical:
  - A new generation of health informatics standards are emerging
  - Global adoption of standards in commercial products
- National Policies:
  - Distributed access to EHRs is now part of many national strategies. It is an item in the Agenda of the Health Ministries
  - England (NpfIT), France, Canada (Infoway), Australia (Health Connect), USA (National Health Information Infrastructure- -NHII)…
- EU Policy:
  - EC Communication -Health - making healthcare better for European citizens: An action plan for a European e-Health Area. COM (2004) 356 final, 30.4.2004, p17, stress on interoperability of Electronic Health Records:
  - " By end 2006, Member States, in collaboration with the European Commission, should identify and outline interoperability standards for health data messages and electronic health records, taking into account best practices and relevant standardisation efforts."

- "Achieving a seamless exchange of health information across Europe requires common structures and ontologies of the information transferred between health information systems"

- Social:
  - Citizens demanding. (References to sentences of the Luxembourg Court of Justice decisions relevant to international health care delivery inside EU)
- Organisational:
  - Adaptation to International reimbursement procedure for Insurance and Social security systems
- Organisational:
  - The main industrial actors are fostering the creation and adoption of standards.

7.2 Standards and Standards supporting initiatives related EHR:

7.2.1 GEHR: Good European Health Record[8]

The GEHR project was and EU 3rd Framework project (Advanced Informatics in Medicine project 2014), and ran from 1992 - 1995. There were 21 participating organisations from 8 countries. The main achievements of the GEHR project were:

- requirements for Clinical Comprehensiveness of the EHR, which have since fed into many other projects, including ISO 18308;
- a Architecture Model: a structured object-oriented model of the EHR, which contained basic data types, versioning semantics, and the multi-level structuring now accepted in CEN and HL7

There are initiatives outside Europe in cooperation with GEHR (Australia).

7.2.2 OpenEHR Foundation[9]

OpenEHR is a non-profit organisation jointly formed in 2000 by UCL (UK) and Ocean Informatics (AUS) uniting an international community working towards the realisation of electronic health records which are:

- clinically comprehensive and ethic-legally sound
- interoperable and standards-based
- implemented as open-source components
- to support seamless and high quality patient care.

OpenEHR promotes open-source (Reference models, Archetype models, Design Principles)

Activities: Architecture of EHR (EHR core services level, Knowledge services level, clinical application services level), reference implementations, academic demonstrators. They are actively involved in CEN and HL7 groups.

---

[8] http://www.chime.ucl.ac.uk/work-areas/ehrs/GEHR

[9] http://www.openhr.org

7.2.3 EUROREC[10]

The European Institute for Health Records is a non-for-profit organisation founded in 2002 by the (then) established ProRec centres
(Belgium, Spain, France, and Bulgaria)

The effective co-operation between all interested parties including users, professionals, authorities, industry, standardisation bodies and others at a European level and through a process of managed convergence towards European EHRs would benefit from the set-up of an appropriate structure based on existing organisations that could promote that mission

PROREC (4 FP): Promotion Strategy for European Health Records

National PROREC centres:

A registered non-for-profit organisation established at the national level gathering in a balanced way. They are solution providers developing contacts with all other stakeholders (public authorities, etc.)

WIDENET (5 FP): Join initiative of various PROREC centres.

Foundation of the European Institute for Health Records: The EuroRec Institute

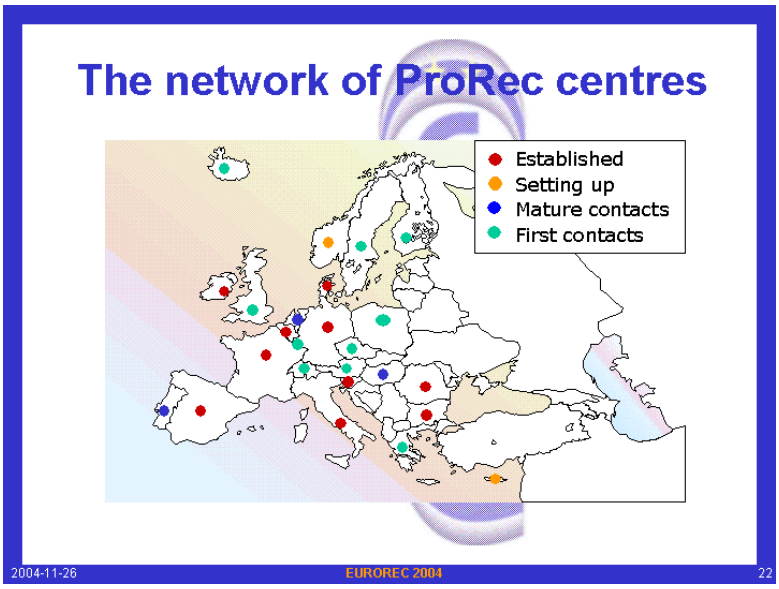

Figure 8: The Network of ProRec centres

Two useful and promising activities in preparation:

- Registration of coding systems used in health care
- Quality Labelling of EHR systems

EUROREC organises one International conference per year.

7.2.4 CEN

Since 1990 CEN has regarded the Electronic Healthcare Record as one of the most important areas for the establishment of European standards, especially in WG1 (Healthcare Information Modelling and Medical Records). It has so far published two generations of EHR standard, in 1995 and 1999.

---

[10] http://www.eurorec.org

7.2.4.1 EHCRA (ENV 12265)

ENV 12265 Electronic Healthcare Record Architecture (1995) was a foundation standard defining the basic principles upon which electronic healthcare records should be based[11].

The scope of ENV 12265 states was to define the basic architectural principles for representing the content and structure of electronic healthcare records.

This European pre-standard provides the foundation for a standard reference architecture for the interchange of electronic healthcare records (in whole or part) between electronic healthcare record systems.

This European pre-standard, in conjunction with succeeding standards:

- enables the content and context of healthcare information of any sort to be recognisable and understandable when displaced from its origin;
- provides the means for referring to healthcare domain information models or syntaxes and for describing how instances of information represented in this way are organised in a healthcare record; and
- provides data structure principles for use by developers in implementing the ethical and legal measures required by national or international regulatory bodies.

This European Prestandard does not apply to the representation of record information within an electronic healthcare system; nevertheless suppliers who wish to exchange records which conform to its provisions may find it convenient to use it as a reference architecture for the storage, processing, and display of electronic healthcare records in the electronic healthcare record system

7.2.4.2 ENV13606

A four-part successor standard for Electronic Healthcare Record Communication, ENV 13606, was published in 1999.

Part 1, the Extended Architecture, built on ENV 12265 and defined additional components for describing the structures and semantics in EHCRs conforming to a range of requirements to allow the content of a healthcare record to be constructed, used, shared and maintained.

Part 2, the Domain Termlist, defined a set of terminological measures to support various degrees of interoperability of the EHCRs created on different systems or by different teams on the same system.

Part 3, the Distribution Rules, specified a set of data objects that represent the rules for defining access privileges to part or whole EHCRs, and the means by which security policies and attributes can be defined and implemented.

Part 4 defined a set of messages to enable the communication of part or whole EHCRs in response to a request message or a need to update a mirror repository of a patient's EHCR.

Since 1999 several demonstrator projects and a few suppliers have elected to use ENV 13606 in an adapted form as their means of EHR interoperability between systems and enterprises. Regrettably the adaptations made to ENV 13606 have been rather ad hoc.

[11] http://www.chime.ucl.ac.uk/work-areas/ehrs/EHCR-SupA/Architecture/index.htm

7.2.4.3 HISA (ENV 12967)

The 1999 CEN 'Standard Architecture for Healthcare Information Systems' (ENV 12967, commonly known as "HISA") seeks to enable the development of modular open systems to support healthcare.

The HISA standard builds on the extensive work of RICHE, NUCLEUS, EDITH and HANSA in this field. The architecture of any generic healthcare information system is described as a federation of heterogeneous applications, interacting and co-operating through a middleware layer of common services. It specifies the structure of the data maintained and retrieved by each service, without prescribing its internal structure. Both applications and the middleware rely on a set of technological facilities (a bitways layer) to enable the physical connection and interaction of various modules.

Two main classes of common services are identified:

- Healthcare-related Common Services (HCS) meeting the particular requirements and activities of users in the healthcare business domain. These relate to the subject of care, activities, resources, authorisation and health characteristics concepts.
- Generic Common Services (GCS) which may be common to any information system in any business domain.

This standard is presently being revised by CEN, and is expected to be published as a full standard (EN 12967) in 2005.

7.2.4.4 The EHRcom TaskForce (prEN 13606)

In December 2001 CEN TC/251 confirmed a new Task Force, known as "EHRcom"[12], to review and revise the 1999 four-part pre-standard ENV 13606 relating to Electronic Healthcare Record Communications. The intention of this work is to propose a revision that could be adopted by CEN as a formal standard (EN) during 2004. The Enquiry Process in CEN has started in October 2004 (prEN13606).

The Task Force was out to base the revision of ENV 13606 on the practical experience that has been gained through commercial systems and demonstrator pilots in the communication of whole or part of patients' EHRs, mainly in Europe and Australia.

The overall mission statement of the EHR communications standard proposed by the Task Force was to produce a rigorous and durable information architecture for representing the EHR, in order to support the interoperability of systems and components that need to interact with EHR services:

- as discrete systems or as middleware components;
- to access, transfer, add or modify health record entries;
- via electronic messages or distributed objects;
- preserving the original clinical meaning intended by the author;
- reflecting the confidentiality of that data as intended by the author and patient.

Parts of preEN13606[13]:

Part 1: Reference Model

---

[12] http://www.openehr.org/standards/t_cen.htm

[13] EUROREC2004: Satellite Workshop on Electronic Health Records, 27 November 2004 (Dipak Kalra, University College London).

- comprehensive, generic EHR model drawing on 12 years of R&D and 2 previous CEN standards
- mapped to HL7 RIM and CDA

Part 2: Archetype Interchange Specification

- adopting the openEHR archetype approach
- compatible with HL7 Template specification

Part 3: Reference Archetypes and Term Lists

- initial archetypes for Europe, and repository specification
- micro-vocabularies for the Part 1 model

Part 4: Security Features

- measures to support access control, consent and auditability of EHR communications

Part 5: Exchange Models

- messages and service interfaces to enable EHR and archetype communication

Reference Implementations:

- Karolinska Institute, Sweden
- University College London
- Universidad Politecnica de Valencia

7.2.4.5 CEN ISSS eHealth Report

The recent report from the CEN ISSS Focus Group on eHealth (V 8.2 available for discussion) stresses the importance of Electronic Health Records and the related standardisation initiative.

One of the identified key strategic aims is "improving access to clinical record" and therefore critical applications for achieving this aims have been highlighted:

- Electronic Health/patient records including health record architecture
- Electronic Transfer of prescriptions
- Electronic Health data messages […]

This report condenses a literature overview of eHeatlh related standards and standardisation initiatives.[14]

7.2.5 ISO

The International Standardisation Organisation within the technical Committee 215 has developed some standards related to EHR. Two WGs are leading the task: TC 215/WG 1 Health records and modelling coordination and WG 2 Messaging and communication

7.2.5.1 ISO TS 18308 (EHR Requirements)

The purpose of ISO/TS 18308:2004[15] was to assemble and collate a set of clinical and technical requirements for an electronic health record architecture (EHRA) that supports using, sharing, and

[14] Refer to pages 54-56 Part1, and executive summary of V8.2

[15] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33397

exchanging electronic health records across different health sectors, different countries, and different models of healthcare delivery. It gives requirements for the architecture but not the specifications of the architecture itself.

The EHR architecture requirements framework in ISO/TS 18308 is divided in:

- STR1: Structure
- PRO2: Process
- COM3: Communication
- PRS4: Privacy and Security
- MEL5: Medico-Legal
- ETH6: Ethical
- EVO8: Evolution

Reference Implementation:

- The first known compliance test against the 18308 requirements has been done for the openEHR Reference Model.

7.2.5.2 ISO/DTR 20514 – EHR Definition, Scope and Context

This project began in August 2001 and its target deliverable is an ISO Technical Report which[16]:

- describes a pragmatic classification of electronic health records;
- provides simple definitions for the main categories of EHR; and
- provides supporting descriptions of the characteristics of electronic health records and EHR systems.

Previous attempts to develop a definition for the Electronic Health Record (EHR) have foundered due to the difficulty of encapsulating all of the many and varied facets of the EHR in a single comprehensive definition[17].

The approach taken in this Technical Report is to make a clear distinction between the content of the EHR and its form or structure. This is achieved by first defining the EHR in terms of its structure (i.e. as a container). This definition (to be called the "basic-generic EHR") is intentionally concise and generic to ensure the broadest applicability to the widest range of existing and future users of EHRs and EHR systems. Such a definition must also be able to support legislative and access control requirements that apply to all 'forms' of EHR.

The basic-generic EHR definition is supplemented by a more detailed and specialised definition to cover two of the most essential characteristics of the EHR not covered by the basic-generic definition. These are the ability to share patient health information between authorised users of the EHR and the primary role of the EHR in supporting continuing, efficient and quality integrated health care. There are of course many other important characteristics of the EHR dependent on the scope and context of care, which will not be explicitly expressed in a single supplementary definition. It would be possible to develop a whole series of formal definitions to capture all of the nuances of different care contexts. However, the approach taken in this Technical Report is to keep

---

[16] Partnership for Health Information Standards Newsletter/Update, Issue 20 – Summer 2004

[17] http://www.openehr.org/standards/t_iso.htm

the number of formal definitions of EHR types to an essential minimum and to demonstrate the inclusiveness of these definitions through explanatory text and examples.

The principle definition of the EHR, which is a specialisation of the basic-generic EHR definition, is called the Integrated Care EHR (ICEHR). The ICEHR is based on a standardised or commonly agreed logical information model which supports semantic interoperability. The openEHR Reference Model and the CEN 13606 Reference Model are examples of models which fit this definition.

7.2.6 HL7

Health Level 7 develops specifications mainly for application-level messaging between health information systems, but also in other areas such as clinical documents and decision support. Its "version 2.x" messaging standards are in wide use in US and around the world, typically between information systems inside the same hospital, and between hospitals and external laboratories.

Since 1997, Health Level 7 (HL7) has been developing a new set of standards, collectively known as "version 3", or "v3". These are still aimed primarily at defining application messages, but are based on formal models, including the "reference information model", or "RIM". Message content schemas are derived by a restriction process which starts from the Reference Information Model (RIM), and continues through domain information models (DIMs), restricted message information models (RMIMs), common message element types (CMETs), finally ending with hierarchical message definitions (HMDs) and generated message schemas in XML.

7.2.6.1 HL7 RIM

The Reference Information Model is a high-level model to govern the definition of future HL7 v3 messages - evolving since 1999. It contains both generic classes and (legacy) specific classes derived from HL7v2 messages. It spans the requirements of purchaser/provider messages, hospital sub-system communications, clinical observations, act/workflow management and knowledge representation. It is increasingly adopted internationally as an industry standard.

The RIM itself is too general to be just a model for the EHR - but it can be “applied” to the EHR. The classes represented in v3 are: entities, roles, relationships, participations, acts, and acts-relationships.

7.2.6.2 HL7 Clinical Document Architecture

HL7 CDA provides standards for the exchange, management and integration of data that supports clinical patient care and the management, delivery, evaluation of healthcare service and management of electronic health records.

CDA is a generic model for the communication of clinical documents, very similar to the "Composition" class in the CEN 13606 specification and the "Transaction" class in openEHR. It was originally intended as a standardised way of communicating clinical notes, but the CDA user community tends to use it more as a persistence specification. It is regarded by some as the HL7 equivalent of a record architecture. CDA release 2.0 defines the structural organisation of fine-grained information inside a document.

It is divided in:

- Level 1 CDA focuses on the content of narrative documents: high-level context (parties, roles, dates and time, places) and structural organisation of headings
- Level 2 CDA (draft standard) models the fine-grained observations and instructions within each heading through a set of RIM Act classes

- A template-based methodology is proposed for Level 3, to define specific kinds of documents, observations or instructions

There is a active cooperation between CEN TC251, ISO TC215, OpenEHR and HL7 initiatives towards harmonisation.

7.2.7 IHE (Integrating the Healthcare Enterprise)

International association of vendors (coming from radiology, imaging systems) whose aims are to[18]:

- Improve the quality and cost of healthcare by removing the interoperability barriers (Integration cost = 20% of IT budget)
- Provide an open interoperability framework, based on existing standards
- Enable cross-vendor environment (best-of-breed)
- Leverage the interoperability solutions in multiple domains (radiology, cardiology, clinical lab, enterprise)
- The approach (very practical with an agreed 20 month cycle for a profile)[19]:
- Solve real-world integration problems
- Close co-operation between users and vendors
- Users prioritise the problems; vendors define the technical solutions
- Common technical framework, based on established standards (e.g. DICOM, HL7,..)
- Regular validation sessions (connectathon)
- 2004 Edition: 50 vendors, 100+ systems
- Demonstrate the implementations at yearly public demo's (USA, Europe, Japan)
- Document implementation in Integration Statements
- IHE gathers the major vendors in medical industry (Philips, GE, Agfa…).

7.2.7.1 IHE XDS

IHE has developed a new Integration Profile for Longitudinal EHR called XDS (based on ebXML, EHRCom, HL7 CDA, DICOM SR, HL7 2.3.1., SQL and internet standards). This new profile will be tested in the next connectathon.

7.2.8 ASTM

ASTM (American Society for Testing and Materials) is a voluntary standards development organization in the world-a trusted source for technical standards for materials, products, systems, and services.

7.2.8.1 CCR: Continuity of Care Record

The Continuity of Care Record, CCR[20], is a standard specification that has been developed jointly by ASTM International, the Massachusetts Medical Society, the Health Information Management

---

[18] http://www.hl7.org/

[19] G. Claeys Agfa Healthcare R&D, Technology Manager Co-chair IHE Europe/ Hans Peter Bursig, secretary general COCIR

and Systems Society, the American Academy of Family Physicians, the American Academy of Pediatrics, and the American Medical Association. The CCR has been developed in response to the need to organize and make transportable a set of basic patient information consisting of the most relevant and timely facts about a patient's condition. It is intended to foster and improve continuity of patient care, reduce medical errors, improve patients' roles in managing their health, and assure at least a minimum standard of secure health information transportability.

7.2.9 Other standards:

7.2.9.1 DICOM Structured Reporting

It is an evolving standard for the communication of the results of investigations to the originating clinical teams. It includes a high-level information model comprising a document header, nested context sections (headings) with a (small) set of defined containment relationships, observations are basic name-value pairs and several data types for values, each with a simple data structure.

Implementation experience is limited. There is currently an active integration work is in progress with HL7 (especially CDA).

7.3 Electronic Health Records Standards

The following is a condensed table of Standards dealing with Electronic Health Records[21].

ENV 13606-1 1999	Health informatics - Electronic healthcare record communication - Part 1: Extended architecture
prEN 13606-1:2004	Health informatics - Electronic healthcare record communication - Part 1: Extended architecture
ENV 13606-2 2000	Health informatics - Electronic healthcare record communication - Part 2: Domain termlist
prEN 13606-2:2004	Health informatics - Electronic healthcare record communication - Part 2: Domain termlist
ENV 13606-3 2000	Health informatics - Electronic healthcare record communication - Part 3: Distribution rules
prEN 13606-3:2004	Health informatics - Electronic healthcare record communication - Part 3: Distribution rules
ENV 13606-4 1999	Health informatics - Electronic healthcare record communication - Part 4: Messages for the exchange of information
prEN 13606-4:2004	Health informatics - Electronic healthcare record communication - Part 4: Messages for the exchange of information
prEN 13606-5:2004	Health informatics - Electronic healthcare record communication - Part 5: Messages for the exchange of information
prEN 13606-6:2004	Health informatics - Electronic healthcare record communication - Part 6:

[20] http://www.astm.org/cgi-bin/SoftCart.exe/STORE/filtrexx40.cgi?U+mystore+ulkl6342+-L+CCR+/usr6/htdocs/astm.org/DATABASE.CART/WORKITEMS/WK4363.htm

[21] Report from the CEN/ISSS eHealth Standardisation Focus Group: CEN/ISSS Report Part 2 V 8.5 page 67.

	Messages for the exchange of information
CR	CEN Report: Electronic healthcare record communication - Domain Model
ISO/TS 18308:2004	Health informatics -- Requirements for an electronic health record architecture
ISO/TR 20514:2005	Health informatics - Electronic health record - Definition, scope and context
ANSI/HL7 CDA-R2 2005	The Clinical Document Architecture - Release 2
ASTM E1238	Standard Specification for Transferring Clinical Observations Between Independent Computer Systems (see ANSI/CLSI LIS05-A below)
ASTM E1394	Standard Specification for Transferring Information Between Clinical Instruments and Computer Systems (see ANSI/CLSI LIS06-A below)
ASTM E1467	Specification for Transferring Digital Neurophysical Data Between Independent Computer Systems
ASTM E1384-02a	Standard Guide for Content and Structure of the Electronic Health Record (EHR)
ANSI/CLSI LIS01-A	Standard Specification for Low-Level Protocol to Transfer Messages Between Clinical Laboratory Instruments and Computer Systems (formerly ANSI/ASTM E1381-02)
ANSI/CLSI LIS03-A	Standard Guide for Selection of a Clinical Laboratory Information Management System (formerly ANSI/ASTM E792-02)
ANSI/CLSI LIS04-A	Standard Guide for Documentation of Clinical Laboratory Computer Systems (formerly ANSI/ASTM E1029)
ANSI/CLSI LIS05-A	Standard Specification for Transferring Clinical Observations Between Independent Computer Systems (formerly ANSI/ASTM E1238-97)
ANSI/CLSI LIS09-A	Standard Guide for Coordination of Clinical Laboratory Services within the Electronic Health Record Environment and Networked Architectures (formerly ANSI/ASTM E2118-00)

8 Security in healthcare

8.1 Introduction

Through this section of the roadmap we are going to establish the main necessities and possible solutions of a health system as well as the legislation which rules the European healthcare system. We are also going to describe some technologies and technical solutions for the informatics part. We need to keep always in mind all the security measures involving the informatics telecommunications that can be as important as the medical security measures themselves. Background information is available in the ITU-T Security Manual on *Security in Telecommunications and Information Technology – An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications*.

To make these things possible, we are going to divide the security involving the health systems into two main sections: Informatics and telecommunication security, and Privacy and confidentiality of

the health information. Inside each section (see figure) we will provide all information needed to show the nowadays health systems situation.

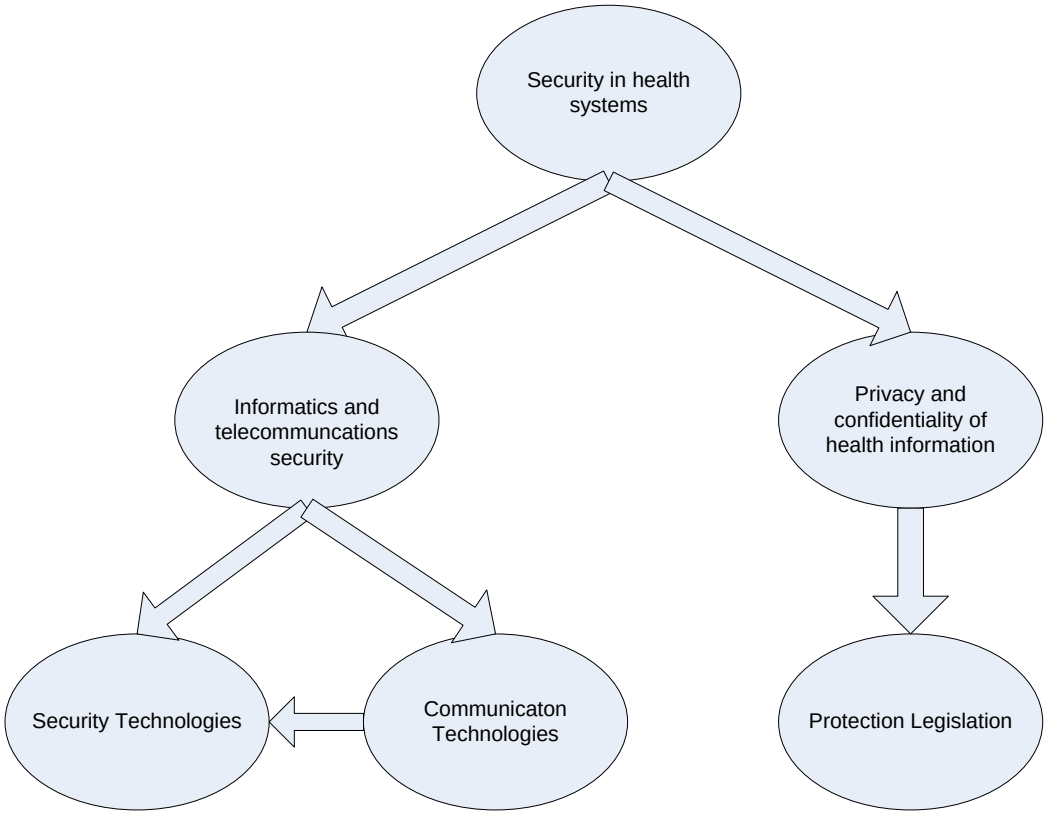

Figure 9: Security Roadmap Structure

8.2 Informatics and telecommunications security

8.2.1 Introduction

Some years ago, security was only oriented to some niche businesses as banking, aerospace, military and some research and development departments. Unfortunately, the exponential grow of the Internet has also brought an important number of security problems to every system as viruses, bugs worms, sniffing, etc.

The standard development must dedicate good time to all the security problems may occur because the Network is accessible to everyone with a little bit of knowledge.

Standards have to be even more careful with new wireless technologies because the intruders do not even need physical connection to obtain the data that is flowing through the network.

We must make clear the division we find in our framework. On one side we have the system's security and on the other side we have the medical information's security.

8.2.1.1 System's security

We need to have a clear understanding of the assets that need to be protected, the threats against those assets must be protected the vulnerabilities associated with the assets and the overall risk to the assets from those threats and vulnerabilities.

Generally, the assets to protect are the communication and computing services, information and data, including software and data relating to security services; and equipment and facilities.

Some examples of threads are:

- Unauthorized disclosure of information
- Unauthorized destruction or modification of data, equipment or other resources
- Theft, removal or loss of information or other resources
- Interruption or denial of services
- Impersonation or masquerading as an authorized entity

So, the standards must take care of most vulnerabilities possible to protect the assets and to avoid the threads.

First of all, a little memory of security terms will help to better follow the roadmap. Authentication refers to the process of verifying the identity of a user. Authorization refers to the process of establishing and enforcing a user's rights and privileges to access specified resources. Encryption refers to the process of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by an authorized recipient holding the matching key.

On the Privacy and confidentiality of health information section, it is shown a brief introduction to medicals information security.

8.2.2 Communication Technologies (Secure Transport)

The information transport has many security problems as described below. The wireless or wired connection has a lot to do with it because the accessibility is not the same to these different networks. The wireless is the most problematic of them and it is the one we are going to start with.

8.2.2.1 Wireless

The phrase "wireless security" is considered by some to be an oxymoron. How can a system with no physical security hope to facilitate secure data transport? Well, with careful planning and configuration, a wireless network can protect itself from many types of attacks and become almost as secure as its wired counterpart. 802.11 can be deployed with various security mechanisms to provide robust, mobile, and hardened network infrastructure. In order to understand how and when to use the security tools at hand, you must first understand the underlying structure of the 802.11 protocol as well as the risks associated with deploying and using a wireless network.

Data in conventional networks travels across wired mediums. Coaxial cable, twisted pairs of copper wire, and strands of fibre optics have been the foundation for networks for many years. In order to view, interrupt, or manipulate the data being transmitted, the wires or switching equipment have to be physically accessed or compromised.

An attacker does not need to physically tap into wired communication in order to eavesdrop on it. Wired communication that uses electrons to transmit data (such as phone calls and 10BaseT Ethernet) radiates small amounts of electromagnetic energy. With highly sophisticated equipment, an attacker can reconstruct the original data stream from the radiated energy. The skill required to pull off this attack as well as the relative proximity the attack requires, however, makes it highly unlikely.

Restrictions on physical access to network cables have been a cornerstone of information security. While physical protection of cables obviously does not solve all the network security problems, it helps mitigate the risk of certain man-in-the-middle (MITM) attacks. Wires are relatively easy to keep physically secure. Placing wires inside of a controlled space such as a data centre keeps the physical layer secure from the majority of attackers. When using radio frequency (RF) communication channels such as a WLAN, users lose the fundamental physical security given to them by wires.

Wireless LANs use high frequency radio waves to transmit their data. These RF waves travel through the air and are difficult to physically constrain. RF waves can pass through walls, under cracks in doors, across streets, and into other buildings. Even if a wireless access point is located inside a physically controlled data center, the wireless data may leave the bounds of the data center into uncontrolled spaces. Data on 802.11 networks can be intercepted from large distances if the attacker has line of sight.

As illustrated in Figure 10, a wired attacker needs to have a physical connection to access the network while the wireless attacker can listen to almost any conversation without physical connection

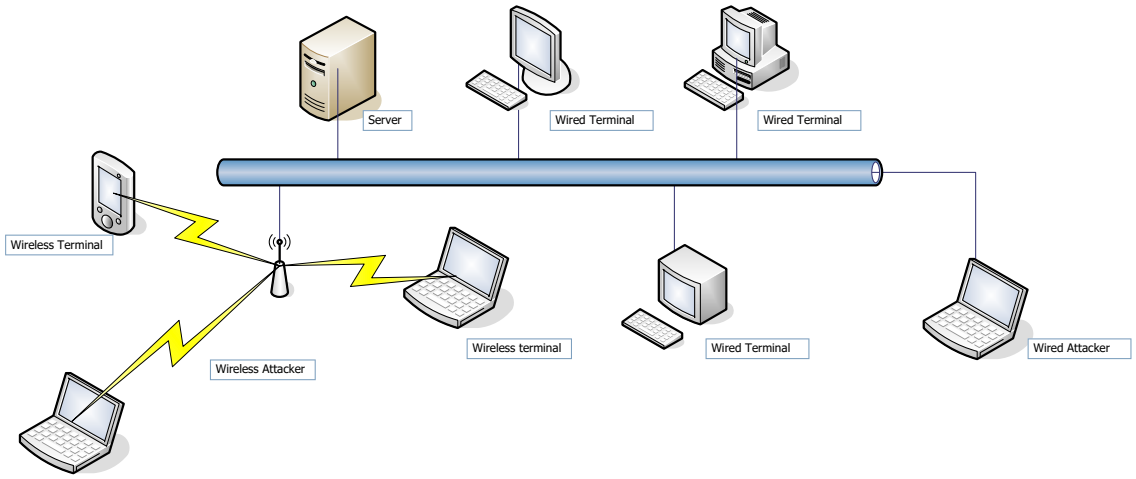

Figure 10: Eavesdropping in a wireless connection

8.2.2.2 Wired

As described above, the wired communications are more secure than the wireless, but there are still constraints that will make insecure the data transmission.

The main subject to avoid data privacy problems is the encryption or ciphering. The public and private key algorithms are some of the most used algorithm because of its simplicity to implement and difficulty to hack.

8.2.3 Security technologies

8.2.3.1 User and Entity Authentication

Authentication answers the question, "Are you who you say you are?" It is a means of establishing the validity of a claimed identity to the system, which becomes the basis for individual accountability. There are three means of authenticating a user's identity, which can be used alone or in combination: validating something the individual knows (e.g., a password, a Personal Identification Number (PIN), or a cryptographic key); validating something the individual possesses, referred to as a "token" (e.g., an ATM card or a smart card); validating something the individual "is", referred to as a "biometric" (e.g., fingerprints or voice patterns).

And within the Authentication section, the Authorization is also important because it is going to have the role to discriminate one user from another and will help with all the medical rights to access the information.

Once authenticated, logical access controls are utilized to authorize and enforce a user's access to and actions towards specified resources. This authorization may be based on identity, roles (e.g., data entry clerk, administrator, supervisor) location, time, types of transactions, service constraints

(e.g., number of concurrent users), access mode (e.g., read, write, delete), or a combination of these criteria. Both internal authorization safeguards (such as Access Control Lists) and external controls (such as secure gateways/firewalls) can be deployed. Another mechanism that can be used for strong access control is encryption, whereby encrypted information can only be decrypted by those possessing the appropriate cryptographic key.

8.2.3.2 Digital Signature and Encryption

The data encryption is essential in every system and even more if the system deals with a wireless network such as WiFi or Bluetooth. Recommendation X.509[22] provides a Public Key Infrastructure standard for strong authentication, base on public key certificates and certification authorities.

Digital signatures are used in cryptography as a method of authenticating digital information often treated, sometimes too closely, as analogous to a physical signature on paper. Whilst there are analogies, there are also differences which can be important. The term electronic signature, although sometimes used for the same thing, has a distinct meaning: it refers any of several, not necessarily cryptographic, mechanisms for identifying the originator of an electronic message.

8.2.3.2.1 Introduction

A digital signature is itself simply a sequence of bits conforming to one of a number of standards. It is the generation of those bits, and their interpretation at some later time/place, and the cryptographic protocols and algorithms which used to govern both which give a digital signature bit sequence meaning in contrast to just any bit sequence.

The mechanism of public key is one of the most used in digital signatures, and it will be useful to understand these principles to see how digital signatures work.

8.2.3.2.2 Public key cryptography

The method depends on the fact that anyone can transform a message into coded text using a public key, but that the 'matching' private key is needed to reverse that transformation. The following is a very brief outline.

It is a simple outline of the method, and does not deal with the details of how the key pairs are generated, how they are applied to encrypt and decrypt the message, and what prevents an attacker with access to the scrambled message and the public key from retrieving the unscrambled message or the secret key.

An important feature of public/private key pairs is that their functions are interchangeable. A message encrypted with the public key can only be decrypted with the private key, but also a message encrypted with the private key can only be decrypted using the public key. It is this feature that digital signatures are based upon.

8.2.3.2.3 Digital signatures

Now consider a somewhat different circumstance, in which Bob wants to send a message to Alice and wants to be able to prove it came from him (but doesn't care whether anybody else reads it). In this case, Bob sends a clear text copy of the message to Alice, along with a copy of the message encrypted with his private key (not the public one). Alice (or any other recipient) can then check whether the message really came from Bob by decrypting the coded text version of the message with Bob's public key and comparing it with the clear text version. If they match, the message was

---

22 ITU-T Rec. X.509 | ISO/IEC 9594 - 8: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

really from Bob, because the private key was needed to create the signature and no one but Bob has it. The coded text version is Bob's digital signature for the message because anyone can use Bob's public key to verify that Bob created it.

8.2.3.2.3.1 The current, legal and practical, state of use

Digital signature schemes all have several prior requirements without which no such signature can mean anything, whatever the cryptographic theory or legal provisions in place.

- First, algorithms must have good quality. Some public key algorithms are known to be insecure, practicable attacks against them having been identified.
- Second, implementations must be properly done. An implementation of a good algorithm (or protocol) with mistake(s) will not work. Software developers typically expect about 1 defect per 1 000 lines, unless intense efforts have been taken to raise its quality, in which case 1 defect per 1 000 000 lines is typically expected.
- Third, the private key must remain actually secret because, if it becomes known to some other party, that party can produce perfect digital signatures of anything whatsoever.
- Fourth, distribution of public keys must be done in such a way that the public key claimed to belong to Bob actually belongs to Bob, and vice versa. This is commonly done using a public key infrastructure and the association of the public key to a user is attested by the operator of the PKI (called a certificate authority).
- Fifth, users (and their software) must properly carry out the signature protocol.

Only if each and every one of these conditions is met will a digital signature can actually be evidence of who sent the message.

8.2.3.2.3.2 Some digital signature algorithms

8.2.3.2.3.2.1 RSA

RSA is a cipher algorithm. It is an asymmetric algorithm and plays a key role in public key cryptography. It is widely used in electronic commerce protocols. The algorithm was described in 1977 by Ron Rivest, Adi Shamir and Len Adleman, who were all at MIT at the time. The letters RSA are the initials of their surnames.

The RSA algorithm basically follows the blocks described in Figure 11.

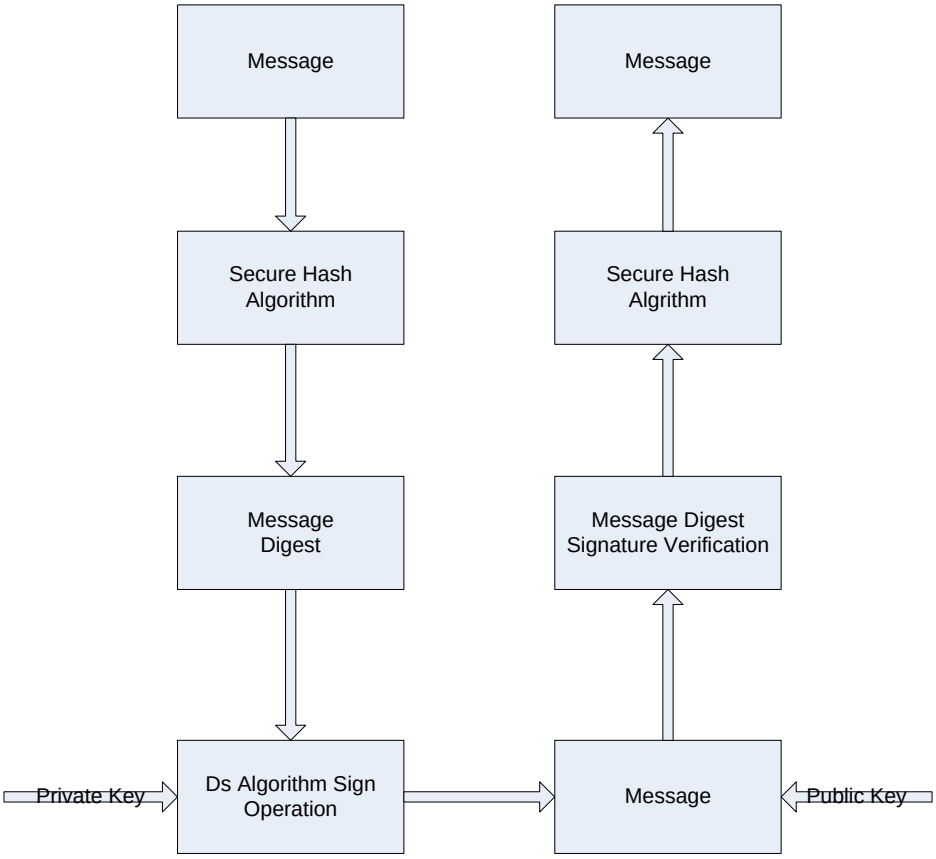

Figure 11: The RSA algorithm

8.2.3.2.3.2.2 DSA

The Digital Signature Algorithm (DSA) is a United States Federal Government standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS), specified in FIPS 186.

8.2.3.2.3.2.3 ElGammal

The ElGamal algorithm is an asymmetric key encryption algorithm for public key cryptography which is based on discrete logarithms and was created by Taher ElGamal. The ElGamal algorithm is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm, even though it is a signature scheme and performs no encryption, is similar to ElGamal in many respects.

8.3 Privacy and Confidentiality of Health Information

8.3.1 Medical information security

This Section talks about the problems that can be found in order to implement a medical system. The study of the rights that the hospital's employees have with the clinical records can be an easy way to explain this topic.

In what refers to a Clinical Record, we can find some problems about the information that is shown and the information that is able to be modified, in function of the hospital personals job.

Some examples:

- A team of doctors must be able to see all the records of their patients, but the commentaries are private to each doctor.

- A nurse must read the treatment or diagnose, but she must not be able to modify it. She must modify the evolution of the patient.
- The hospital administrator must read the treatment to be able to price it.
- Etc.

After these brief descriptions about some of the cases that can be found in medical and system's security (see Informatics and telecommunications security section), this roadmap is going to get into some of the main topics to ensure the security of standards:

8.4 Secure Profile (Medical Records Security)

8.4.1 Introduction

This section identifies and examines the issues pertaining to privacy and security within the healthcare industry. The role of information and technology in healthcare, and the needs and challenges of privacy and security, are considered in opening sections. The chapter ends with a brief discussion of difficulties in implementing security countermeasures in the medical context.

The identified priorities for the application of ICT to health such as:

- Health/patient records;
- Electronic prescriptions;
- Messages between care providers;
- Access to records by professionals and patients;
- E-Health Insurance Cards;

Lead to security requirements relating to:

- Ensuring secure data exchange:
    - Common interpretation;
    - Data integrity;
    - Safe and secure systems;
    - Secure communication;
- Patient and professional identity management (e.g. processor based ID data cards);
- Access control including:
    - Policy bridging between organisations;
    - Role definition;
    - Audit trails.

The need to manage patient identification and protect personal information is thus a common requirement of very many applications and is crucially important given the sensitivity of personal health data. SDOs such as CEN/TC251, ISO/TC215 and HL7 are very active in this field. CEN/TC251 has developed a number of standards and several are approaching their final stages. ISO/TC215 and ITU (X.509) have produced standards on Public Key Infrastructure and ISO/TC215 is producing international guidance on the application of ISO 17799 to the healthcare sector (ISO 17799 on security management is being widely adopted in all sectors and in health by a number of countries). In this area CEN/TC251 and ISO/TC215 are working in the closest collaboration with no overlaps or conflicts.

The highest priorities emerging within Member States as and the EU as a whole are:

- Ensuring secure patient identification;
- Access control to personal health data;
- Policy bridging between organisations.

The security of health data may involve a Public Key Infrastructure and processor-based identity data cards for patients and professionals.

The challenge is to bring standards together so as to create an infrastructure which will meet all business priority requirements. A review of requirements, the standards needs and their availability and a test environment for interoperability is required.

Thus for realising a trustworthy environment for communication and co-operation using personal health information, Member States, through the EU Commission, need to establish a framework of policies and standard-based solutions for guaranteeing appropriate identity and privilege management for authorisation and access control of all those involved in patient care; controlled by patients and, depending on their level of access, by professionals who are given such authority by patients or by their function/role.

8.4.1.1 Standards related to security issues

The following is a list of standards related to security issues in e-health applications:

- AENOR UNE-CR 13694: Safety and Security Related Software Quality Standards for Healthcare (SSQS): Proposes several quality norms related to security and protection in e-health software.
- ASTM E1762-95 (2003): Standard Guide for Electronic Authentication of Health Care Information: The standard defines a document structure for use by electronic signature mechanisms and the characteristics of the electronic signature itself.
- ASTM E2212-02a: Standard Practice for Healthcare Certificate Policy: Addresses the policy for digital certificates that support the authentication, authorization, confidentiality, integrity, and non repudiation requirements of persons and organizations that electronically create or transact health information.
- CEN ENV 12251: Management and security of authentication by passwords: It addresses the management and security of authentication by passwords.
- CEN ENV 12388: Algorithm for Digital Signature Services in Health Care: Defines the algorithm used for digital signatures in medicine information exchange.
- CEN ENV 13608: Security for healthcare communication: Defines concepts for secure systems. Besides that, secure data objects and secure data channels are addressed.

8.4.1.2 Information Is Key to Healthcare.

Information often is described as the lifeblood of a healthcare resource: patient data, research data, human resources and other administrative data, financial data - in fact, all of the details that keep the machine ticking and that are the basis of further development. Infrastructure, hardware, and software matter, but they are the framework and tools that allow the service to process the information that justifies its existence.

A healthcare resource needs information to meet its obligations to its customers. Information supports the timely, cost-effective supply of all the deliverables that are normally thought of as coming under the healthcare umbrella. Information, in the form of medical records, is used to match each patient profile to a given course of treatment and is also a deliverable in its own right.

Information is required to map present and future needs to resources throughout the organization and to map individual profiles to global (e.g., epidemiological) concerns, to take a somewhat very narrow view of medical research.

Patients benefit when healthcare providers and facilities have rapid access to accurate information. Researchers, and ultimately patients, benefit from analyses of treatment efficacies as well as from identification of long-term public health trends and population statistics. Healthcare delivery is improved when healthcare oversight bodies have access to diagnoses and treatment plans.

But with the benefits of electronic medical records, there also come the risks of health information exposure and misuse.

8.4.1.3 Why Security and Privacy Are Important to Healthcare Information.

Security is important in the healthcare industry for two major reasons. It enables the business side of healthcare to conduct electronic commerce, and to reap its benefits, while minimizing the business costs of dealing with electronic attacks, such as falsifying billing claims—prosecutable under false-claims laws for the private health countries.

From the patient side, security is important to improve the reliability of data used in medical decisions, while protecting the privacy of healthcare information. There is also an issue of personal safety—and even of population safety—that is tied to the security of healthcare information.

There has never before been as urgent a need to protect medical information; hackers, crackers, pranksters, and busybodies are now showing why this is so important.

Some examples of problems arising from inadequate privacy and security for healthcare information have been reported in the consumer advocacy media.

While not as life threatening, it was reported that over 100 hospital employees pried into the medical records of a renowned athlete receiving treatment. In another incident, a governor's health records—as well as nearly all the records associated with a list of registered voters in a large city—were retrieved from a database of state employee health insurance claims, using birth date and ZIP code data obtained from a voters' database. Cross-referencing and merging snippets of semisensitive data can create highly sensitive, cradle-to-grave medical histories subject to abusive commercial data-mining, while making targeted healthcare consumers feel violated.

The need for security within a healthcare organization is not restricted to medical information. Inventory records, human resources data, and financial reports, for instance, might be tempting targets. All are subject to data protection legislation, but medical records, with their vital characteristics, also require unique controls.

Medical records may be accessed by the state, by a private hospital at which the subject is an inpatient or outpatient, or by a neighbourhood physician or dentist. In conjunction with other records, possibly anonymized, they might be used in bulk by health authority administrators for cost analysis, prediction, and other valid purposes.

They may be seen by a partner organization, such as a social work department or a law enforcement agency, in a case conference. Medical records contribute, usually in anonymized or semi-anonymized form, to a multitude of research projects. There is evidently a need for a wide range of legal and quasi-legal restraints, reflecting the intra and extra organizational uses to which they may be put.

Medical records may be defined as those that are used for medical purposes, which can include preventive and curative treatments, diagnosis, research, and administration.

All of these functions require stringent security measures, but even non-medical documentation can have security implications, as a basis for social engineering attacks, for instance.

8.4.1.4 Impacts of Information Technology

The healthcare sector has been slower than other industries to embrace business-sector–specific automation technology. Many in the sector have been late adopters of information technology (IT) and e-business principles as means of improving their organization, increasing its efficiency, differentiating its services, and cutting its costs of doing business. Now technology is increasingly becoming a priority for the healthcare industry, especially to help deal with the dramatic changes being brought about by decreasing revenues and increasing costs. More and more, the healthcare industry is relying on networked information systems to conduct its essential, day-to-day business, but these new technologies tend to bring new risks and vulnerabilities.

As the healthcare industry gets increasingly networked, medical data distribution among multiple parties becomes more widespread. Data collected by healthcare providers is increasingly reported electronically to numerous government and institutional agencies for applications such as state and federal disease control; research project analyses; government and private health insurance premiums and claims; medical claims clearinghouse operations; hospital discharge records; outpatient encounter tracking; registries of births, deaths, immunizations; and so on. Healthcare data also can be obtained from commercial databases such as those maintained by pharmacies, rehabilitation facilities, and medical supply stores, as well as from databases where consumers might least expect personal, medically relevant, healthcare information to be extracted, such as information derived from catalogue orders, warranty registrations, consumer questionnaires, and the like. As more and more sensitive healthcare information is accumulated and made accessible, there is a greater chance that it can be exposed to abuse, that the potential for breakdowns of medical services increases, and that catastrophic economic loss becomes more feasible.

With each new information technology introduced into the healthcare field, there come increased risks and vulnerabilities. For example, new decision-support technologies to help combat fraud and abuse and to identify patterns of potentially fraudulent behaviour provide tempting targets to those who would perpetrate fraud. Furthermore, the advent of sophisticated IT capabilities, such as data warehousing and data mining, which support information fusion, information convergence, and information analysis also brings new privacy and security problems. Information merger across private and public databases can lead to the creation of confidential personal medical information from distributed pieces of less sensitive data. The possibilities loom large to link the disparate medical records databases with other personal information databases that house shopping and credit card information to create data warehouses that aggregate disturbing amounts of personal and medical information. Use of the attack-prone Internet and Internet-related technologies to communicate and process healthcare transactions escalates the risks of security breeches. For example, the pervasiveness of Web technology now allows competitive, online healthcare companies to set up personal electronic medical records that can be accessed via the Internet, and managed, amended, and corrected online, both through portals for healthcare providers and portals for healthcare consumers. Not only does file sharing and transaction processing on the Internet escalate risks of security breeches to medical records, but also the vast number of individuals who have access to the Internet greatly escalates system vulnerabilities.

As new Internet technology features and protocols are adopted, more vendor implementations of such new technologies need to be trusted both for their ability to be implemented correctly and for assurance that they can prevent new risks and exposures. Trust must be established that there are no vendor implementation flaws that allow unauthorized information to be entered into or extracted from medical records. Matters pertaining to trust, with respect to healthcare IT products and systems, are the focus of attention of the Forum of Privacy and Security in Healthcare, described later.

As networking, IT processing and storage capabilities, and online transactions take an increasingly more essential role in the delivery of healthcare and in the success of the healthcare enterprise, the

consequences are that privacy and security become vital to the success and stability of the enterprise. However, given the industry's slowness to accept IT, it can be expected that healthcare industry attention to IT security also may be slow.

8.4.1.5 Information and IT Security Challenges

Many security challenges are somewhat unique to healthcare information. Some of the more significant ones include:

- Wireless communication of orders and patient information to and from the bedside can be prone to disclosure, modification, and eavesdropping by roaming medical information thieves.
- Because the healthcare industry is such a fragmented industry, with a multitude of different players and stakeholders, it literally takes an act of Congress to coordinate the industry in matters such as IT and IT security.
- As the healthcare industry is a relative latecomer to using IT, it tends to lack experience in concepts such as IT security, strategies, and procedures, such as security help desks, Public Key Encryption (PKI), and cryptography.
- Electronic commerce among supply-chain trading partners provides potential points of entry to medical systems. Trading partners must establish trust in the security provided by parties that they may never have met or spoken with.
- The Gartner Group consulting house has indicated that by the year 2004, healthcare providers will be submitting 40 percent of all claims directly to healthcare payers via the Internet, with enormous increases in the associated risk of security incidents.
- The proliferation of government, institutional, and commercial databases that house medical information, coupled with factors such as the large number of people involved in settling a health insurance claim and the possibility of unauthorized access to records, as well as the number of people, authorized and unauthorized, who can access a person's medical information, all act to increase the likelihood that medical information will be used improperly.

In addition to the unique challenges, many issues facing healthcare are entirely like those facing any other market sector. For example:

- Unauthorized modem access to an enterprise's central data stores from remote locations raises the need to prevent unauthorized access to the data network side of an enterprise from the telephony network side of an enterprise.
- Multiple data replications and multiple data users accessing the data elevate the risks of data exploitation.
- Mischievous access to information pertaining to the business operations of an enterprise is as serious a problem as access to data associated with products and services.
- Reliance on a single IT, or networking vendor's, product line can be deleterious since if hackers can get through into one part of the enterprise, they may be able to hack an enterprise's entire security architecture.

It is believed that the costs associated with deliberate and accidental security breaches in the healthcare industry are large. Hard costs of losses are difficult to determine. However, they can be inferred to be much over USD 100 billion per year since, according to a report in Information Week, all businesses worldwide were estimated to have lost USD 1.6 trillion in 1999 because of security breaches, virus attacks, and related downtime.

This USD 100 billion figure is reasonable because the healthcare industry represents a large fraction of many national economies.

Soft costs attributed to security losses are even harder to estimate. They are mainly caused by the decrease in revenues that follow a loss of consumer confidence in the privacy and appropriate use of their healthcare information after reports of data being stolen or otherwise inappropriately used.

8.4.1.6 Core Security Model in Healthcare Context

The classic model of information security is built on availability, confidentiality, and integrity:

- Availability—information has to be available to those who are entitled to see it or to process it, at the time when they need it. Conversely, those who do not need the information, in the performance of their duties, must not be able to access it. Threats to availability arise from denial of service (DoS) attacks and from deliberate or accidental infrastructural damage to networks, hardware, and software.
- Integrity—information needs to be defended against accidental or deliberate corruption and modification. Threats include viruses, non-replicating malware (e.g., Trojan horses), unauthorized or accidental modification, errors in structural integrity, logical corruption, and fraudulent misuse.
- Confidentiality—information should not be available to those who are not entitled to see or otherwise process it. Threats include unauthorized access and disclosure by hackers or by careless disregard for the rights of privacy. Solutions include access management, passwords, and encryption. To some extent, this is the glamour area of security: The problem is implementing it without compromising availability and integrity.

Often, a fourth leg is added: accountability. This is not just a matter of assigning blame, although that may be necessary. It is also a safeguard against anyone's denial of some specific action; in security parlance it is called non-repudiation. It is not possible to establish a viable security architecture without determining who is responsible for what. A security incident may be nobody's fault, but it could be a major problem if prevention is nobody's job. Only when individual responsibility is a matter of record can appropriate action be taken including the assignment of blame and additional training.

This model is not the only favoured view of security: the Parkerian hexad adds possession, authenticity, and utility to integrity, availability, and confidentiality.

In the aggregate, these qualities form the essential underpinnings for ensuring trust in medical information during its storage, processing, and transmission.

Information security is primarily and literally about keeping information safe, not only from intrusion but from corruption and from becoming inaccessible to those who should be able to process it. Here are some typical attacks and other security issues, all of which have implications for the entry and maintenance of medical records:

- Unauthorized access may result in inadvertent errors by untrained personnel or in deliberate alteration of such records as drug dispensing or billing charges. Password stealing and piggybacking are two means of gaining unauthorized access. The results may be loss of confidentiality and integrity, with damage to any and all medical records.
- Unauthorized modification destroys the integrity and authenticity of any affected record and impairs its utility. Even one instance can introduce doubt as to the integrity of the entire database.

- Malware is software introduced for the specific purpose of damaging or destroying a database or particular medical functions. Malware may be used to affect adversely any of the characteristics of the security model.
- Denial of service is a malicious effort to bring all of an organization's data communications or computer operations to a complete halt by making the services unavailable.
- User error can inadvertently affect the integrity and authenticity of medical records. In an extreme case, administrator error can bring down an entire system.
- Programming errors can be trivial, or, like malware, they may damage or destroy any of the security model's desired characteristics.

There are always tradeoffs: Emphasizing one aspect of the security model often has negative implications for other aspects. Emphasis on confidentiality usually impacts adversely on availability, if only because physical and electronic access controls tend to complicate legitimate access. In combination with other factors—for instance, human error, or hardware or software failure—efforts at preserving confidentiality may result in data becoming less accessible. Medical information security measures need to be tailored to each specific healthcare environment.

8.5 Conclusion

This section described most of the medical and technological security problems that can be found in telemedical services. Currently, the major issue is the need of **integration** between all systems and applications available for each purpose must be reinforced. This integration will solve many problems due to the new relation that it will provide between applications. Once the integration is made, a new problem search should be done to seek the problems still remaining and the needs to be fulfilled.

The ISO / TC215 group has made great efforts in the application of security standards on health informatics. Its Working Group 4 is the one in charge of standardisation of security matters with the following results:

- TS 17090-1:2002 Health Informatics – PKI framework and overview (WG4)
- TS 17090-2:2002 Health Informatics – PKI certificate profile (WG4)
- TS 17090-3:2002 Health Informatics – PKI management of certificate authority (WG4)
- ISO 21549-3:2004 Health informatics – Patient healthcare data - Part 3: Limited clinical data (WG5)
- ISO 22857:2004 Health informatics – Guidelines on data protection to facilitate trans-border flow of personal health information (WG4)

9 Clinical Data Representation, Clinical Standards and Standards for managing multilingual reference terminologies

Table 1 is based in the description from http://www.ulb.ac.be/esp/emd/classifications.htm and summarizes the classifications, nomenclatures, terminologies and coding systems in use in medical computerized registration systems. This table represents a compilation of the state of the art in international coding related to health. For further information about the coding systems, the URL is being included in the description.

Table 1: International codifications in healthcare data

Shorthand	Classification	Institution
ATC	Anatomical and therapeutically classification http://www.whocc.nmd.no/	WHO http://www.who.int
BNF	British National Formulary http://www.bnf.org/	RPSGB http://www.rpsgb.org.uk/
BRAUN	Braun Kasugraphie *Braun RN (ed). Pratique, critique et enseignement de la médecine générale. Paris: Payot, 1979* http://gretec.chez-alice.fr/Casugraphie_fichiers/Casugraphie_Braun.pdf	-
CIM	Classification Internationale des Maladies, *see entries for IDC below*	WHO
CDMI	Codes pour un Dossier Médical Informatisé http://www.sesa.ucl.ac.be/SesaWeb/logiciels/log.htm#cdmi	SESA-UCL http://www.sesa.ucl.ac.be/SesaWeb/index.htm
CFTMEA	New edition of the French classification for child and teenager mental diseases (*Nouvelle édition de la Classification française des troubles mentaux de l'enfant et de l'adolescent*) http://psydoc-fr.broca.inserm.fr/biblo_bd/cftmea/	Psycho-doc http://psydoc-fr.broca.inserm.fr/biblo_bd/cftmea/
CLUE	Clinical coding engine http://www.clinical-info.co.uk/clue.htm	CIC http://www.clinical-info.co.uk/index.htm
Cyber+LE	Cyber plus language engine http://www.healthlanguage.com/whatle.html	HL http://www.healthlanguage.com/index.html
DRC	Dictionnaire des Résultats de Consultation http://www.sfmg.org/dico.html	SFMG http://www.sfmg.org/
DRG	Diagnosis Related Group glossary http://www.wido.de/Krankenhaus/drg/Grundbegriffe/contentengl.html	WIdo http://www.wido.de
DSM-III-R	Diagnostic and Statistical Manual of Mental Disorders, Third Edition (1987) http://www.psy.med.rug.nl/0023	APA http://www.psych.org/main.html
DSM-IV	Diagnostic and Statistical Manual of Mental Disorders, Fourth Edition http://www.psych.org/clin_res/library.html	APA http://www.psych.org/main.html
DSM-IV PC	Diagnostic and Statistical Manual of Mental Disorders, Fourth Edition Primary Care version http://www.psych.org/clin_res/dsm_iv_pc.html	APA http://www.psych.org/main.html
ENCODE-FM	ICPC-2 classified vocabulary http://www.insite-fm.com/Products/ENCODE-FM/index.htm	Insite FM http://www.insite-fm.com

Shorthand	Classification	Institution
Galen	Advanced terminology systems for clinical information systems http://www.opengalen.org/open/manifesto/manifesto.html	Open Galen http://www.opengalen.org/index.html
ICD-9	International Classification of Disease Ninth revision http://web.aafp.org/fpm/961000fm/icd9indx.html	AAFP http://web.aafp.org/
ICD-9-CM	International Classification of Disease Ninth revision Clinical modification http://icd-9-cm.org/index.html	AHA & NCHS http://www.aha.org/default.asp
ICD-10	International Classification of Disease Tenth revision http://www.who.int/whosis/icd10/	WHO http://www.who.int/
ICD-10-AM	International Classification of Disease Tenth revision, Australian Modification http://www.cchs.usyd.edu.au/ncch/ICD10AM_2nd_edition.html	NCCH http://www.cchs.usyd.edu.au/ncch/
ICD-10-PC	Diagnostic and Management Guidelines for Mental Disorders in Primary Care http://www.who.int/msa/mnh/ems/icd10/icd10pc/icd10phc.htm	WHO http://www.who.int/
ICD-10-CM	International Classification of Disease Tenth revision Clinical modification	NCHS http://www.cdc.gov/nchs/default.htm
ICD-10-PCS	International Classification of Disease Procedure Coding System http://www.hcfa.gov/stats/icd10/icd10.htm	HCFA http://www.hcfa.gov/
ICHA	International classification of Health Accounts http://www.oecd.org/els/health/sha/	OECD http://www.oecd.org/
ICHPPC-2-d	International Classification of Health Problem in Primary Care second revision, defined	WONCA http://www.wonca.org/
ICF	International Classification of Functioning and Disability. http://www.who.int/icidh/	WHO http://www.who.int/
ICPC	International Classification of Primary Care (1987) http://www.ulb.ac.be/esp/wicc/table-en.html	WONCA http://www.wonca.org/
ICPC-2	International Classification of Primary Care, second revision (1998)	WONCA http://www.wonca.org/
ICPC-2-E	International Classification of Primary Care, second revision, electronic version (2000)	WONCA http://www.wonca.org/
ICPC-e	International Classification of Primary Care, European version (1993)	WONCA http://www.wonca.org/

Shorthand	Classification	Institution
ICPC-2 Plus	ICPC-2 classified vocabulary http://www.ulb.ac.be/esp/wicc/icpc2.html	FMRC http://www.fmru.org.au/intro.htm
LOCAS-2	Terminologie classifiée (French)(CISP-2/CIM-1O) http://www.ulb.ac.be/esp/cisp/locas.html	Care Editions http://docpatient.net/care/
Mesh	MeSH hierarchy. (English - French- German) http://www.hon.ch/HONselect/Browse.html	HON http://www.hon.ch/
MIQUEST	Health query language http://www.clinical-info.co.uk/miquest.htm	CIC http://www.clinical-info.co.uk/index.htm
NTS	National Triage Scale http://www.acem.org.au/open/documents/triage.htm	ACEM http://www.acem.org.au/open/documents/home.htm
OPCS-4	Classification of Surgical Operations and Procedures Fourth Revision http://www.coding.nhsia.nhs.uk/prod04.htm	NHS http://www.coding.nhsia.nhs.uk/index.htm
OXMIS	Oxford Community Myocardial Infarction Incidence Study http://www.admin.ox.ac.uk/oxro/by.htm	Oxford-PHC http://www.admin.ox.ac.uk/oxro/by.htm
RCC4	Read Clinical Codes (4 byte) http://www.cams.co.uk/readcode.htm	
RCC5	Read Clinical Codes (5 byte) http://www.cams.co.uk/readcode.htm	
SNOMED	Systematised Nomenclature of Medicine http://www.snomed.org/	CPA http://www.cap.org/
SNOMED CT	Systematised Nomenclature of Medicine Clinical terms http://www.cams.co.uk/snomedct.htm	CPA and NHS http://www.cap.org/
UMLS	United Medical Language System http://www.nlm.nih.gov/pubs/cbm/umlscbm.html	NLM http://www.nlm.nih.gov/nlmhome.html
Zero to three	ZERO TO THREE: Diagnostic Classifications http://www.zerotothree.org/diagnostic.html	WAIMH http://www.msu.edu/user/waimh/new_waimh/Page_1x.html

9.1 State of the art in medical standards for patient's information exchange

9.1.1 Standardisation Organisations

There are three main organizations that create standards related to Electronic Health Records- CEN TC 215, HL7 and ASTM E31. HL7, operating in the United States, develops the most widely used health care-related electronic data exchange standards in North America, while CEN TC 215, operating in 19 European member states, is the pre-eminent healthcare information technology

standards developing organization in Europe. There is a memorandum to intensify collaboration between the two groups and move toward the development of technically identical and interchangeable U.S. and European standards. Both HL7 and CEN collaborate with the ASTM that operates in the United States and is mainly used by commercial laboratory vendors.

9.1.2 CEN/TC 251

CEN/TC 251 establishes priorities based on healthcare market priorities and identifies both publicly available specifications (PAS) and outputs from R&D programs which are suitable for rapid transformation into standards. When the market is not providing the solutions, CEN/TC 251 generates, through consensus-building suitable standards. The objectives of CEN/TC 251 are the organisation, the coordination and the follow-up of standards' development, including testing standards in Healthcare Informatics and Telematics, at a European level. These major objectives of CEN/TC 251 are reflected in its structure of Working Groups and in its Project-Teams' activities.

9.1.2.1 Information models (WG I)

The scope of WG I is the development of European standards to facilitate communication between independent information systems within and between organisations, for health related purposes.

Such standards are essential if healthcare services are to obtain the benefits of open systems and avoid the constraints of proprietary interfaces. The standards are based on information models - generic models of aspects of health care or health care information. WG I will therefore develop domain model based reference architectures for evolvable information systems. These will facilitate optimized health care processes for maximum patient perceived quality satisfaction, workflow oriented polycentric care and approaches to archiving healthcare information that are not time limited.

An important area of WG I work is standards for the Electronic Healthcare Record. These will include a record architecture establishing the principles for representing the information content and record structure, a set of concepts and terms for record components, and rules and mechanisms for sharing and exchanging records. A domain model representing a formal description of the context within which the healthcare records are used, will be established to document requirements for these standards.

Another important area of WG I work is that of standards for messages to meet specific healthcare business needs for the communication of healthcare information. While some messages may have a broad initial scope, WG I will also validate, refine and profile these and other messages to ensure they are applicable to specialist domains with particular requirements. WG I will also address the maintenance, revision and harmonization of existing message standards.

In addition, WG I will address standards for the information requirements that may be applicable to other media for the storage and transfer of healthcare information, including patient data cards.

WG I will seek to provide workable standards that identify and meet immediate healthcare specific requirements for communication between independent systems. These requirements will be identified by consulting Healthcare Professionals, Healthcare Managers & Institutions and Healthcare Information System Developers & Vendors. The consultation should cover but need not be exclusively limited to CEN Member Countries.

The standards developed by WG I should enable the information that supports patient care to be communicated unambiguously in order to enhance the quality of care. Therefore, WG I will liaise with WG II to ensure that terminology standards are taken into account and appropriately utilized in standards for healthcare communication. The Standards developed by WG I should enable sensitive clinical information to be communicated for the benefit of the patient whilst minimizing risks of errors and any threats to patient confidentiality. WG I will, therefore, liaise with WG III to ensure

that the solutions developed to aid communication take proper account of security and safety Standards. WG I will define its Standards in ways that take account of what is technically feasible but will avoid making any non-essential stipulations about the technical environment in which these standards are to be implemented. WG I will cooperate with WG IV to assist the development of relevant technology specific standards that meet the underlying user requirements identified in WG I standards.

9.1.2.2 Terminology and knowledge bases (WG II)

The objectives of CEN/TC 251 WG II are the semantic organization of information and knowledge so as to make it of practical use in the domains of health informatics and telematics and the provision of information and criteria to support harmonization. This encompasses clinical, managerial and operational aspects of the medical record and enabling access to other knowledge.

The actual work items focus on:

- Terms, Concepts and the interrelationship of concepts.
- Structures for concepts systems including those for multi-axial coding schemes.
- Guidelines for the production of coding systems and knowledge bases.

9.1.2.3 Security, safety and quality (WG III)

The current European and national legislation emphasize the importance of quality, safety and security. It provides a statutory framework to ensure that information systems used in healthcare have appropriate levels of quality, safety and security. Major Pan-European documents that provide a basis for CEN/TC 251 are the recommendations from the Council of Europe which apply to all CEN nations and the European Union Data Protection Directive finally adopted in 1995 to be implemented in the member states by October 1998.

It must be emphasized that standards for security, safety and quality must be developed in parallel with the basic informatics standards for e.g. health care communication or electronic record systems. Without considering these important regulatory aspects, the technical possibilities for important efficiency improvements using health telematics can not be fully exploited.

Security of information systems is usually defined as: the prevention of breaches of confidentiality, integrity and availability. In healthcare information systems, the main reason for the major concern with confidentiality is the protection of privacy of the individuals. The patients have to trust health care establishments to care for the very sensitive information they give them. Systems are to be understood in a wider sense, including the surrounding procedures.

The safety of systems can be defined as: the expectation that systems do not, under defined conditions, enter a state that could cause human death or injury. In this definition however, a 'system' will include the software, the hardware, the users of the system and the procedures and practices related to the working of the system. It is not sufficient to analyze a software system without considering how it is used and the environment in which it is used. Software does not actually kill or injure people - it is the associated hardware or the actions of inaccurately informed staff that may cause harm.

Quality is defined as: the totality of features and characteristics of a product, process or service that bear on its ability to satisfy its stated or intended needs. Two important features of the overall quality of such systems are the safety and the security of the systems, and these elements will become even more important as information systems are increasingly used for safety- and security-critical applications.

It is expected that future development of IT security will take place in the following arenas:

- Development of protection profiles for various sectors or application areas.
- Development of detailed protocols for various core security services.
- Evaluation and certification of IT products.
- Evaluation, certification and accreditation of IT systems.

The term protection profile is used here to include specification of various countermeasures to preserve security also when these can not be referenced from existing international standards. The need to view quality, safety and security issues in close relation should also be reflected in these arenas. This means that the scope of protection profiles as it is today should be broadened to encompass quality and safety objectives and requirements.

It also means that evaluation and certification schemes for the three areas should be harmonized, aiming for the possibility of performing a single evaluation and certification per product/system covering quality, safety and security requirements.

The previous work of the WG has been focused on developing a security categorization and a system of basic protection profiles associated with these categories, ENV 12924. The group also developed a specification for an algorithm for digital signature services, ENV 12388. The working group has also been able to produce draft technical reports for "A framework for security of health care communication" and on "A framework on security requirements for intermittently connected devices." A draft ENV for Secure user identification using passwords has also been produced.

Of course, care should be taken to include ethical and juridical notions in these considerations. Although no clear framework exists for this, it could be said that WG III should 'audit' other work within the sphere of CEN/TC 251, to identify and give advice on all relevant security, safety and quality related issues and ensure that issues of a general nature are developed as application independent standards in WG III to achieve consistency.

The current work plan contains the completion of the above mentioned advanced drafts and in addition work will be started on the following standards:

- Secure User Identification for Healthcare - Strong Authentication using microprocessor cards (ENV).
- Security for Healthcare Communication (ENV).
- Security requirements for intermittently connected devices (ENV).
- Safety and Security Related Software Quality Standards for Healthcare (CR).
- Framework for formal modelling of healthcare security policies (CR).
- Safety procedures for identification of persons and related objects (CR).

Although many of these aspects will be relevant to other CEN/TC 251 Working Groups, special links can be noted for Security of Healthcare Communication and WG I working on ‘Electronic Healthcare Record Communication. Part 3. Distribution rules’.

9.1.2.4 Technology for Interoperability (WG IV)

The aim of this WG is to develop and promote standards that enable the interoperability of devices and information systems in health informatics.

The scope covers three main areas:

- Intercommunication of data between devices and information systems.
- Integration of data for multimedia representation.

- Communication of such data between source departments and other legitimate users elsewhere in the healthcare sector, in order to facilitate electronic healthcare record provision.

The main concern of the WG is technology for interoperability. In addressing this, the issues of methodology, quality, security and architecture will require liaison with the other WGs, other standards bodies and integration activities.

Devices include, for example: clinical analyzers, medical imaging and Intensive Care Unit equipment, clinical workstations and cards.

9.1.3 ASTM

Founded in 1898, ASTM (American Society for Testing and Materials) International is a not-for-profit organization that provides a global forum for the development and publication of voluntary consensus standards for materials, products, systems, and services. Over 30,000 individuals from 100 nations are the members of ASTM International, who are producers, users, consumers, and representatives of government and academia. In over 130 varied industry areas, ASTM standards serve as the basis for manufacturing, procurement, and regulatory activities. Formerly known as the American Society for Testing and Materials, ASTM International provides standards that are accepted and used in research and development, product testing, quality systems, and commercial transactions around the globe.

To be the foremost developer and provider of voluntary consensus standards, related technical information, and services having internationally recognized quality and applicability that promote public health and safety, and the overall quality of life; contribute to the reliability of materials, products, systems and services; and facilitate national, regional, and international commerce.

The strategic objectives of the ASTSM are:

- To provide the optimum environment and support for technical committees to develop needed standards and related information.
- To ensure ASTM products and services are provided in a timely manner and meet current needs.
- To increase the awareness of the ASTM consensus process, the benefits of participation, and the value of ASTM standards and services in the global marketplace.
- To strengthen both the national and international acceptance and use of ASTM products and services.
- To make the ASTM process, resources, skills, and facilities available to the marketplace to accommodate its changing needs.
- To ensure the fair representation and participation of key stakeholders in ASTM activities to secure technically sound standards.
- To maintain ASTM's fiscal stability in order to fulfil the Society's mission.

9.1.3.1 Committee E31 on Healthcare Informatics

ASTM Committee E31 on Healthcare Informatics develops standards related to the architecture, content, storage, security, confidentiality, functionality, and communication of information used within healthcare and healthcare decision making, including patient-specific information and knowledge. Its scope is the promotion of knowledge and development of standard classifications, guides, specifications, practices, and terminology for the architecture, content, storage and communication of information used within healthcare, including patient-specific information and

medical knowledge. Standard also address policies for integrity and confidentiality and computer procedures that support the uses of data and healthcare decision making. The Committee's activities will be coordinated with those of other relevant committees and organizations internal and external to ASTM.

Subcommittees highlighted:

- E31.17 Privacy, Confidentiality, and Access.
- E31.19 Electronic Health Record Content and Structure.
- E31.20 Data and System Security for Health Information.
- E31.22 Health Information Transcription and Documentation.
- E31.23 Modelling for Health Informatics.
- E31.28 Electronic Health Records.

9.1.3.2 Published standards under the jurisdiction of E31.17

- E1869-97 Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records.
- E1986-98 Standard Guide for Information Access Privileges to Health Information.
- E1987-98 Standard Guide for Individual Rights Regarding Health Information.
- E1988-98 Standard Guide for Training of Persons who have Access to Health Information.
- E2017-99 Standard Guide for Amendments to Health Information.
- E2147-01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems.

9.1.3.3 Published standards under the jurisdiction of E31.19

- E1239-00 Standard Guide for Description of Reservation/Registration-Admission, Discharge, Transfer (R-ADT) Systems for Electronic Health Record (EHR) Systems.
- E1384-01 Standard Guide for Content and Structure of the Electronic Health Record (EHR).
- E1633-02 Standard Specification for Coded Values Used in the Electronic Health Record.
- E1715-01 Standard Practice for An Object-Oriented Model for Registration, Admitting, Discharge, and Transfer (RADT) Functions in Computer-Based Patient Record Systems.
- E1744-98 Standard Guide for View of Emergency Medical Care in the Computerized-Based Patient Record.

9.1.3.4 Published standards under the jurisdiction of E31.20

- E1714-00 Standard Guide for Properties of a Universal Healthcare Identifier (UHID).
- E1762-95 Standard Guide for Electronic Authentication of Health Care Information.
- E1985-98 Standard Guide for User Authentication and Authorization.
- E2084-00 Standard Specification for Authentication of Healthcare Information Using Digital Signatures.
- E2085-00a Standard Guide on Security Framework for Healthcare Information.
- E2086-00 Standard Guide for Internet and Intranet Healthcare Security.

9.1.3.5 Published standards under the jurisdiction of E31.22

- E1902-97 Standard Guide for Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records.
- E1959-98 Standard Guide for Requests for Proposals Regarding Medical Transcription Services for Healthcare Institutions.
- E2117-00 Standard Guide for Identification and Establishment of a Quality Assurance Program for Medical Transcription.
- E2185-01 Standard Specification for Transferring Digital Voice Data Between Independent Digital Dictation Systems and Workstations.

9.1.3.6 Published standards under the jurisdiction of E31.23

- E2145-01 Standard Practice for Modelling in Health Informatics.
- Published standards under the jurisdiction of E31.28
- E2182-02 Standard Specification for Clinical XML DTDs in Healthcare.
- E2183-02 Standard Guide for XML DTD Design, Architecture and Implementation.
- E2184-02 Standard Specification for Healthcare Document Formats.
- New Standard: Specification for GEM: A Document Model For Clinical Practice Guidelines.

9.1.4 HL7

Health Level Seven (HL7) is one of several ANSI-accredited Standards Developing Organizations (SDOs) operating in the healthcare arena. Most SDOs produce standards (sometimes called specifications or protocols) for a particular healthcare domain such as pharmacy, medical devices, imaging or insurance (claims processing) transactions. Health Level Seven’s domain is clinical and administrative data. Our mission is to: "To provide standards for the exchange, management and integration of data that support clinical patient care and the management, delivery and evaluation of healthcare services. Specifically, to create flexible, cost effective approaches, standards, guidelines, methodologies, and related services for interoperability between healthcare information systems."

"Level Seven" refers to the highest level of the International Standards Organization's (ISO) communications model for Open Systems Interconnection (OSI) - the application level. The application level addresses definition of the data to be exchanged, the timing of the interchange, and the communication of certain errors to the application. The seventh level supports such functions as security checks, participant identification, availability checks, exchange mechanism negotiations and, most importantly, data exchange structuring.

There are several health care standards development efforts currently underway throughout the world. Why then, embrace HL7? HL7 is singular as it focuses on the interface requirements of the entire health care organization, while most other efforts focus on the requirements of a particular department. Moreover, on an ongoing basis, HL7 develops a set of protocols on the fastest possible track that is both responsive and responsible to its members. The group addresses the unique requirements of already installed hospital and departmental systems, some of which use mature technologies.

While HL7 focuses on addressing immediate needs, the group continues to dedicate its efforts to ensuring concurrence with other United States and International standards development activities. Argentina, Australia, Canada, China, Czech Republic, Finland, Germany, India, Japan, Korea, Lithuania, The Netherlands, New Zealand, Southern Africa, Switzerland, Turkey and the United

Kingdom are part of HL7 initiatives. Moreover, HL7 is an American National Standards Institute (ANSI) approved Standards Developing Organization (SDO). HL7 strives to identify and support the diverse requirements of each of its membership constituencies: Users, Vendors, and Consultants. Cognizant of their needs, requirements, priorities and interests, HL7 supports all groups as they make important contributions to the quality of the organization. The committee structure, balanced balloting procedures and open membership policies ensure that all requirements are addressed uniformly and equitably with quality and consistency.

9.1.4.1 Technical committees

9.1.4.1.1 Arden Syntax

This SIG support the HL7 mission to create and promote its standards by maintenance and further development of the Arden Syntax for Medical Logic Systems, a standard for representing and sharing clinical knowledge in procedural format.

9.1.4.1.2 Attachments

This SIG standardizes the supplemental information needed to support health care insurance, and other e-commerce transactions. Its purpose is to encourage the use of HL7 for uniform implementation of this supplemental information. An important effort as guided by the Board of HL7 is to work jointly with ASC X12N (Insurance), to assist in the implementation of the Administrative Simplification provisions of HIPAA mandates, to provide on-going support, and to represent HL7 in the HIPAA Designated Standards Maintenance Organization (DSMO) efforts.

9.1.4.1.3 Blood Bank

The primary purpose of the Blood Bank SIG is to standardize the transmission of blood bank related information for patients, tissue, blood products, tests and services concurrent with evolving international standards. The scope will include the areas of patient identification, medical records, orders and observations, financial management and home health and will also address donor collections, processing and management.

9.1.4.1.4 CCOW

This technical committee developed from the Clinical Context Object Workgroup (CCOW), formerly a stand-alone organization. The group focuses on the collaboration among visual (GUI-based) applications on a clinical workstation. It works to use software component technologies and reduce the reengineering costs in order to bring its benefits to the industry as rapidly as possible. The group publishes standards for the visual integration of cooperative interaction among independently authored health care applications at the point of use. CCOW joined HL7 as the Special Interest Group on Visual Integration with the intent of revising its standard and publishing it as an HL7 standard.

9.1.4.1.5 Clinical Decision Support

The Technical Committee will focus on issues related to single-patient-focused health care decision support messaging. The committee will focus on development of messages independent of any implementation of clinical logic. The TC will also be responsible for support and development of Arden Syntax for Medical Logic Systems. These will serve as test cases in the development of general messaging schemes.

9.1.4.1.6 Community Based Health

This SIG supports the message development effort for Community Based Health Services within the framework of HL7 Standards, in order to promote adequate information exchange between Community Based and Acute Care service domains. The scope of the CBHS – SIG includes but is

not limited to home health, hospice, long term care, mental health and other community based providers.

9.1.4.1.7 Conformance

This SIG supports the HL7 mission to create and promote its standards by providing a consistent mechanism to specify conformance via HL7 V2.x message profiles. The Conformance SIG will also act in an advisory role to the HL7 Modelling & Methodology Technical Committee regarding conformance topics.

9.1.4.1.8 Control/Query

The Control/Query committee is responsible for defining the details of the message transport services including encoding rules and auxiliary protocols, maintenance of common datatypes, definition of the query framework, and definition of the framework for master files support.

9.1.4.1.9 Education and Implementation

This group's mission is to develop and update the Implementation Support Guide and coordinate HL7-sanctioned training. The guide provides assistance to health care institutions, hospital information system vendors, consultants, and other support groups that are considering system development and implementation activities using the HL7 protocol. The guide will be published in conjunction with each version of the HL7 standard.

9.1.4.1.10 Government Projects

The goal of the government projects SIG is to coordinate the integration of government Health Informatics requirements into the HL7 standards.

9.1.4.1.11 Guideline Interchange Format

The HL7 Guideline Interchange Format (GLIF) Initiative is proposed as a special interest group of HL7 to create the standard electronic representation for the specification of clinical practice guidelines for purpose of interchange and to facilitate their integration into the healthcare systems, computer-based medical records, and a variety of applications.

9.1.4.1.12 Imaging Integration

Imaging Integration collects, review, develops and documents use cases, information structures and message content related to ordering and reporting of non-textual data and associated information, including images themselves. Imaging Integration promotes the interoperation of imaging systems, PACS and associated radiological oriented systems with information systems that use HL7.

9.1.4.1.13 Laboratory, Point of Care and Automated Testing

The goal of the "Laboratory, Automated, and Point of Care Testing SIG" is to meet the needs for communication among automated clinical lab systems, instruments, devices, and information systems in various implementations of clinical lab, point of care, and automated testing by developing interoperable messaging.

9.1.4.1.14 Medical Records/Information Management

The goal of the Medical Records/Information Management Technical Committee is to define messages to support the functional messaging needs of the Information Management or Medical Records Department. The Committee is comprised of individuals representing vendors of information systems (computer based systems), health information management professionals, and other stakeholders including other allied health professionals and physicians.

9.1.4.1.15 Modelling and Methodology

The Modelling and Methodology Committee is responsible for creating and maintaining the HL7 message development methodology and facilitating its use, and maintaining a Reference Model that reflects the shared models that are developed and used by the HL7 Functional Committees.

9.1.4.1.16 Orders and Observations

The goal of the Orders and Observation Technical Committee is to define messages to support the order communication and observation reporting processing requirements among the stakeholders in the health care organization regarding patients, non-patients, people, other species, or inanimate objects. These messages are not limited to intra-organizational transactions, but may cross organizational boundaries.

9.1.4.1.17 Patient Administration and Financial Management

The goal of the Patient Administration and Financial Management (PAFM) Technical Committee is to define messages to support the "administrative" (that is, patient management, ADT) and "financial" (that is, patient accounting, billing) processing requirements of healthcare providers.

The Patient Administration projects will define the messages needed to support the identification, maintenance and movement of patients throughout the healthcare provider environments. This explicitly includes coordination with the X12 subject domain and other national and international standards organizations and third party entities (e.g. payers and government).

9.1.4.1.18 Patient Care

The goal of Patient Care is to define messages to support the needs for communicating information regarding the creation, management, execution and quality of diagnostic and therapeutic care.

9.1.4.1.19 Patient/Provider Messaging

This group supports the HL7 mission to create and promote its standards by ensuring that HL7 specifications for systems that empower health care providers and patients to communicate efficiently exist and are broadly implemented within health care.

9.1.4.1.20 Personnel Management

This group supports the HL7 mission to create and promote its standards by providing messages to communicate information about health professionals, i.e. health-care providers and support staff.

9.1.4.1.21 Scheduling and Logistics

The goal of the Scheduling and Logistics Technical Committee is to define messages required to support the flow of logistics information such as scheduling and materials management information in the Health Care environment.

9.1.4.1.22 Security and Accountability

This group supports the HL7 mission to create and promote its standards by identifying the needs and technical means for security and evidence of accountability for information communicated according to the HL7 standards.

9.1.4.1.23 Structured Documents

This Technical Committee will produce a comprehensive architecture to facilitate exchange and processing of electronic healthcare documents. The TC will support HL7 through education in the development, evolution, and use of structured document specifications. The specifications created by this committee will follow the HL7 Development Framework.

9.1.4.1.24 Templates

This group supports the HL7 mission to create and promote its standards by creating the procedures for creation and management of HL7 Templates. An HL7 template is a data structure, based on the HL7 Reference Information Model that expresses the data content needed in a specific clinical or administrative context.

9.1.4.1.25 Vocabulary

The mission of the Technical Committee is to identify, organize and maintain coded vocabulary terms used in HL7 messages.

9.1.4.1.26 XML

This group supports the HL7 mission through recommendations on use of Extensible Markup Language (XML) standards for all of HL7's platform- and vendor-independent healthcare specifications.

9.2 Data architectures for EHR sharing

9.2.1 GEHR Project

The Good European Healthcare Record (GEHR) project was established within the EU Telematics Research and Technology Development program to develop a comprehensive and widely applicable common data structure for using and sharing electronic healthcare records (EHCR) within Europe. The information environment in which such architecture might be used includes all sites capable of creating and maintaining clinical or clinically related data. The GEHR architecture provides a framework which can support the full diversity of clinical data storage, retrieval and communication required by clinicians. It has been formulated to encompass the requirements of the different disciplines of primary and secondary health care, for use by doctors, nurses and other professionals in all European countries. In the work of the project have been included new multimedia aspects of the record. Examples specifically addressed include X-ray and photographic images, bio-signals, clinical drawings as well as textual information. The latter includes, for example, clinical observations and laboratory data in the form of coded terms and free text. The architecture provides a framework upon which systems may be built to support the core ethical and legal requirements of good clinical practice.

The GEHR architecture is described in three ways:

- A functional description of the architecture.
- A formal object model: the GEHR Object Model (GOM).
- A physical encoding of the model structures: the GEHR exchange format (GEF).

An additional aim of GEHR was to prototype software tools providing a logical level of access to medical software applications. They include data queries and integration, as well as conversion utilities to/from standard messages (laboratory, images, etc.).

A very specific methodology was adopted for the GEHR project, based upon the evolution and testing of prototypes within a comprehensive framework of requirements established across all sectors of health care. The starting point for this series of prototypes was an existing health record architecture, the Current Healthcare Record Architecture (CHRA: developed by Health Data Management Partners, Brussels). The CHRA and a commercial product (Health One) based upon it, were extensively tested and analyzed.

9.2.1.1 Architectural Components

The principal architectural components evolved by GEHR are summarized below. Each of these is further elaborated using Attributes which address aspects of identification, content and context. They are consistent with the structures apparent in existing records and fulfil the requirements identified by the project of the EHCR.

The Electronic Health Care Record (EHCR) which provides the container for all data about a particular patient. The EHCR is the electronic record for one patient on one system (which is regarded as EHCR_SOURCE). There is only one EHCR for each patient at this EHCR_SOURCE. Everything which is contained in this EHCR is deemed to be about the patient except when modified by a collection (as described below). In technical terms, the HCR is the top level containment structure, and would be composed of one or more Transactions, together with some data enabling the record to be identified.

The Transaction which provides the majority of the features needed for the medico-legal aspects of health care data and the mechanism for the control of amendments. It also represents the smallest amount of data which can safely be transferred between EHCR systems. A key clinical requirement is the ability to record details of each clinical encounter as a special grouping of items for medico-legal reasons. The transaction is defined as the information recorded about the patient by a single author in one institution at one point in time. It represents the data entered in one interactive session with a patient record. This could result from a consultation or other contact with a patient, or perhaps from the filing of a test result or letter.

The Health Record Item (HRI) which provides the structure for recording the content values of EHCR entries. While data can be entered in HCRs in many different formats (reports, laboratory result sheets, forms, etc.), it has proven useful to define an elemental unit of data entry. HRI is the smallest unit of information which remains meaningful as an entry in a HCR. At the logical level a HRI can be regarded as the unit of information which can be obtained as the result of one specific measurement, question, observation, discussion, or other investigation mechanism. The HRI has adopted by CEN TC/251 (PT011) as the basic unit of health information within the record.

The HRI Collection which provides for aggregation of HRIs and other HRI Collections. It also provides the means of changing the scope (data subject) of the data. Collections with their subordinate HRIs and/or Collections are user to express the component parts of clinical concepts in the correct structural relationship appropriate to the clinical concept, and to assign values to their component parts. The general term Collection is used here to indicate a structure that contains groups of Observations.

The heading provides a means of grouping or labelling combination of Collections/HRIs. It allows instances of clinical concepts, expressed through Collections and HRIs, to be related to the context of healthcare for the patient. Headings do not change the scope of the data.

The refinement of the architecture of the GEHR project was focused in two areas: the GEHR Object Model and the GEHR Exchange Format.

9.2.1.2 Object Model

Proposing the architecture as an object model was necessary to ensure that the requirements laid down by the clinical users could indeed be implemented in real applications using the GEHR architecture. It was necessary to examine the architecture minutely for integrity, consistency, and simplicity whilst remaining faithful to the original clinical requirements. It was clearly recognised that software developers needed to be left as free as possible creatively to implement the architecture in as many different applications as possible. The work necessitated closing the gap between the architectural concepts of Health Record Items expressed clinically and which clinicians could readily understand, and the formal architectural components required by application

developers. The options were extensively debated through documents and at GEHR meetings. Only a few issues remain to be resolved. These include various expressions of containment of the data, optimal ways to model assessment values and coded data, and parallel ways to express unique data identifiers.

9.2.1.3 Exchange Format

The GEHR Exchange Format is a key component to maintain an accurate and effective transfer of clinical information within the clear and demanding requirements of the clinical group of the GEHR project. It will also enable many legacy implementations to communicate with others which have implemented the GEHR architecture.

ASN.1 was proposed as a standard notation for syntax and a standard set of encoding rules. Thus the GEHR concepts and standards can be expressed in ASN.1 and the encoding rules applied to create the exchange format. Some members of the consortium tested converting whole electronic health care records into the GEF for presentation in ASN.1

9.2.2 OpenEHR

The openEHR Foundation is a non-profit organization bringing together an international community of people working towards the realization of clinically comprehensive, ethic-legally sound and interoperable electronic health records to support seamless and high quality patient care. Its aim is to promote and publish the formal specification of requirements for representing and communicating electronic health record information, based on implementation experience, and evolving over time as health care and medical knowledge develop; promote and publish EHR information architectures, models and data dictionaries, tested in implementations, which meet these requirements; manage the sequential validation of the EHR architectures through comprehensive implementation and clinical evaluation; maintain open source "reference" implementations, available under license, to enhance the pool of available tools to support clinical systems; and collaborate with other groups working towards high quality, requirements-based and interoperable health information systems, in related fields of health informatics.

Approach

9.2.2.1 Requirements

OpenEHR undertakes the collation of requirements for the design, implementation and deployment of interoperable EHRs:

- To support the seamless sharing and continuity of health care.
- To enable EHR systems to interface with medical knowledge, evidence of best practice and other systems needed to deliver safe, secure and effective health services.

Requirements developed by openEHR are shared with all relevant international standards initiatives.

9.2.2.2 Information Architecture

OpenEHR publishes information architectures comprising reference models (RMs), archetype models (AMs), archetypes, service specifications and interfaces for interoperable EHR systems. These specifications are underpinned by requirements and by the results of implementation and deployment of previous versions, to enable the ongoing development of evidence-based information architecture. OpenEHR specifications are supportive of diversity in areas of innovation or where evidence of best practice has yet to be accumulated, (...to enrich experience of a diversity of approaches.)

9.2.2.3 Implementation

OpenEHR facilitates the engineering of interoperable components to rigorous design and development methodologies, with exemplar solutions to provide proof-of-concept verification of the information architecture. Such implementations will be accompanied by migration interfaces to former openEHR, GEHR, Synapses specifications and implemented standards, in support of "durable" patient record information.

9.2.2.4 Evaluation

Members of openEHR will seek avenues (including funding) to implement software components conformant to the architecture, and opportunities to validate these in clinical demonstration settings in order to verify the requirements and inform the ongoing refinement of the information architecture.

9.2.2.5 Open Source

OpenEHR recognizes the value of open source as a means of fostering a community of developers, and of prototyping and evaluating components in a field of innovation such as the EHR. OpenEHR endeavours to produce reference implementations of the information architecture as soon as is practical, and to make these available through an open source license, in order to foster a network of demonstrator sites contributing to the evaluation process and to a global community of EHR use. OpenEHR will also collaborate openly with commercial software developers seeking to adopt the openEHR specifications, and will foster inter-vendor collaboration.

9.2.2.6 Standards

OpenEHR is committed to supporting legislative and industry standards as a means of encouraging the wide-scale adoption of interoperable EHRs. Members of openEHR work closely with standardisation bodies, including ISO, CEN and HL7, and project teams on national and international levels.

9.2.2.7 Education

OpenEHR is committed to supporting the education of clinical, technical and managerial persons about good quality EHRs. It aims to progressively accumulate a library of available teaching materials and to identify members willing to engage in delivering these.

9.2.2.8 Collaboration

OpenEHR recognizes that the vision of interoperable and high quality EHRs cannot be realized by any one organization, and also that the EHR cannot exist as an informatics solution independently of a wide range of other knowledge, care process, security and health service informatics solutions. It will seek to collaborate widely and whole-heartedly with other groups engaged in similar or parallel activities.

9.3 Healthcare records

9.3.1 Relevant ASTM Standards

ASTM Subcommittee E31.19 is organized to develop, maintain and refine the vocabulary for the computer based patient record. Patient record content standards are proposed in standard E1384 (Description for Content and Structure of the Computer-based Patient Record). First published in 1991, it proposes content for computer-based patient records in all clinical settings. The content was organized into 14 segments of patient information categories that reflect historical access. One segment was organized into sub-segments to capture ongoing encounters and episodes of treatment in a manner analogous to the way unit records have been traditionally organized. The original

segments were identified after an analysis of established national data sets including the Uniform Discharge Data Set, Uniform Ambulatory Core Data Set, and Minimum Data Set for Long Term Care as well as a number of medical record accreditation standards that were proposed for a variety of health care organizations.

9.3.1.1 E1239-00 Standard Guide for Description of Reservation/Registration-Admission, Discharge, Transfer (R-ADT) Systems for Electronic Health Record (EHR) Systems

This guide identifies the minimum information capabilities needed by an ambulatory care system or a resident facility R-ADT system. This guide is intended to depict the processes of: patient registration, inpatient admission into health care institutions and the use of registration data in establishing and using the demographic segments of the electronic health record. It also identifies a common core of informational elements needed in this R-ADT process and outlines those organizational elements that may use these segments. Furthermore, this guide identifies the minimum general requirements for R-ADT and helps identify many of the additional specific requirements for such systems. The data elements described may not all be needed but, if used, they must be used in the way specified so that each record segment has comparable data. This guide will help answer questions faced by designers of R-ADT capabilities by providing a clear description of the consensus of health care professionals regarding a uniform set of minimum data elements used by R-ADT functions in each component of the larger system. It will also help educate health care professionals in the general principles of patient care information management as well as the details of the constituent specialty areas.

9.3.1.2 E1384-02 Standard Guide for Content and Structure of the Electronic Health Record (EHR)

This guide covers all types of healthcare services, including those given in acute care hospitals, nursing homes, skilled nursing facilities, home healthcare, and specialty care environments as well as ambulatory care. They apply both to short term contacts (for example, emergency rooms and emergency medical service units) and long term contacts (primary care physicians with long term patients). At this time, the standard vocabulary reflects more traditional care. As the standard evolves in the next revisions, the vocabulary will more adequately encompass the entire continuum of care through all delivery models, health status measurement, preventive case, and health education content.

This guide has five purposes.

- The first is to identify the content and logical structure of an Electronic Health Record (EHR). The record carries all health related information about a patient over time. It includes such things as observations or descriptions of the patient (for example, the physician's or nurse practitioner's history and physical, laboratory tests, diagnostic imaging reports), provider's orders for observations and treatments, documentation about the actions carried out (for example, therapies or drugs administered), patient identifying information, legal permissions, and so on.
- The second goal is to define the relationship of data coming from diverse source systems (for example, clinical laboratory information management systems, order entry systems, pharmacy information management systems, dictation systems), and the data stored in the Electronic Health Record. Recalling that the EHR is the primary repository for information from various sources, the structure of the EHR is receptive to the data that flow from other systems.
- Third, in order to accelerate the adoption of EHRs, this guide provides a common vocabulary, perspective, and references for those developing, purchasing, and implementing EHR systems, but it does not deal either with implementation or procurement.

- Fourth, this guide describes examples of a variety of views by which the logical data structure might be accessed/displayed in order to accomplish various functions.
- Fifth, this guide relates the logical structure of the EHR to the essential documentation currently used in the healthcare delivery system within the United States in order to promote consistency and efficient data transfer. It maps to the clinical data currently in existing data systems and patient care records.

9.3.1.3 E1633-02 Standard Specification for Coded Values Used in the Electronic Health Record

This specification covers the identification of the lexicons to be used for the data elements identified in Appendix X1 of Guide E 1384. It is intended to unify the representations for: (1) primary record of care data elements, (2) the data elements identified in other standard statistical data sets, (3) data elements used in other healthcare data message exchange format standards, or (4) in data gathering forms for this purpose, and (5) in data derived from these elements in order that data recorded in the course of patient care be exchangeable and be the source of accurate statistical and resource management data. This specification is applicable to all paper and automated systems.

9.3.1.4 E1715-01 Standard Practice for an Object-Oriented Model for Registration, Admitting, Discharge, and Transfer (RADT) Functions in Computer-Based Patient Record Systems

This practice is intended to amplify Guide E 1239 and to complement Guide E 1384 by detailing the objects that make up the reservation, registration, admitting, discharge, and transfer (RADT) functional domain of the computer-based record of care (CPR). As identified in Guide E1239, this domain is seminal to all patient record and ancillary system functions, including messaging functions used in telecommunications. For example, it is applicable to clinical laboratory information management systems, pharmacy information management systems, and radiology, or other image management, information management systems. The object model terminology is used to be compatible with other national and international standards for healthcare data and information systems engineering or telecommunications standards applied to healthcare data or systems. This practice is intended for those familiar with modelling concepts, system design, and implementation. It is not intended for the general computer user or as an initial introduction to the concepts.

9.3.1.5 E1744-98 Standard Guide for View of Emergency Medical Care in the Computerized-Based Patient Record

This guide covers the identification of the information that is necessary to document emergency medical care in a computerized patient record that is part of a paperless patient record system. The intent of a paperless patient record system will be to improve efficiency and cost-effectiveness.

This guide is a view of the data elements to document the types of emergency medical information that would be valuable if available in the computerized patient record. The patient's summary record and derived data sets will be described separately from this guide.

As a view of the computerized patient record, the information presented will conform to the structure defined in other ASTM standards for the computerized patient record. This guide is intended to amplify Guides E1239, E1384, and F1629 and the formalisms described in Practice E1715. It details the use of data elements already established in these standards for use during documentation of emergency care in the field or in a treatment facility and places them in the context of the object models for health care that will be the vehicle for communication standards for health care data.

The codes for the data elements referred to in this guide will be developed in consideration of national or professional guidelines whenever available. The EMS definitions are based on those

generated from the national consensus conference sponsored by NHTSA and from ASTM F30.03.03 on EMS Management Information Systems. The Emergency Department (ED) definitions will consider those recommended by the CDC workshop on ED definitions scheduled for January 1996. The hospital discharge definitions will be developed in consideration of existing requirements for Medicare and Medicaid payment.

The ASTM process allows for the definitions to be updated as the national consensus changes. When national or professional definitions do not exist, or whenever there is a conflict in the definitions, the committee will recommend a process for resolving the conflict or present the various definitions within the document along with an explanation for the purpose of each definition.

This guide reinforces the concepts set forth in Guides E1239 and E1384 that documentation of care in all settings shall be seamless and be conducted under a common set of precepts using a common logical record structure and common terminology.

The computerized patient record focuses on the patient. In particular, the computerized patient record sets out to ensure that the data document includes:

- The occurrence of the emergency.
- The symptoms requiring emergency medical treatment.
- The medical/mental assessment/diagnoses established.
- The treatment rendered.
- The outcome and disposition of the patient after emergency treatment.

The computerized patient record consists of subsets of the data computerized by multiple care providers at the time of onset/scene and *en route*, in the emergency department, and in the hospital or other emergency health care settings.

The computerized patient record focuses on the documentation of information that is necessary to support patient care but does not define appropriate care.

9.4 Medical Imaging

9.4.1 Past review

Starting in the 1970's, but mainly in the last decade, diagnostic medical imaging has embarked on a transformation. Until recently, specialists such as radiologists and cardiologists primarily worked with images captured on film and videotape. But today numerous and diverse healthcare facilities have made the move to digital filmless imaging systems making use of digital images and associated data for the communication of patients' biomedical diagnostics and therapeutic information.

Even though the many existing standards related to imaging, none of them was perfectly suitable for medical purposes. Thinking about the enormous number of medical images produced everyday by a single radiology laboratory, the problem of classifying this large amount of data, and the need to connect uniquely the image with the patient's identity and other test results; the adoption of traditional formats like jpeg or gif implied a high risk of information lost. The need of a new standard covering these points was therefore easily detected.

9.4.2 Present situation

It is crucial that healthcare professionals have fast and efficient access to digital diagnostics data for use in medical review and at the same time, organizations must maintain security and privacy measures for patient records. Thus, the interconnection and interaction of the equipments, the

transfer and process of data in an identical format and the need of an appropriate storing and managing what invariably became a sprawling and ever-expanding collection of enormous data files led the American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) to form a joint committee with the main objective of creating a standard method for the transmission of medical images and their associated info: DICOM.

9.4.2.1 DICOM

DICOM which stands for “Digital Imaging and Communication in Medicine” is nowadays practically ubiquitous. It is largely the most expanded method of communication for medical imaging devices, while other standards like CIAS remain in a second plane only appropriate for areas in which the image quality is not expected to be high. DICOM is used by virtually every medical profession that utilizes images within the healthcare industry. These include dentistry, endoscopy, mammography, ophthalmology, orthopaedics, pathology, paediatrics, surgery, veterinary, etc, but mainly radiology and cardiology. DICOM as de facto standard has also been adopted by the majority of medical hardware manufacturers and imaging products suppliers. The adoption of DICOM in PACS and diagnostic workstations has been overwhelming, allowing the development of many best practices which make a profit from the advantages of the DICOM standard.

It represents a progress in that it makes it possible to predict the interconnection of various imaging modalities, through a Document of Conformity or "Conformance Statement" emitted for each device following this standard. The standard makes it possible remote communication through a network or a media by ensuring the compatibility of the equipment and by eliminating proprietary formats obtaining the images of the patient and all epidemiological information associated with, in an identical format.

A great attention was devoted to establishing working relationships with other related standard initiatives throughout the world. And solid cooperation with other standardisation groups like CEN, HL7, ISO TC 215 among others was achieved. Attention was also focused to the evolution of standards linked to Internet. After adopting the TCP/IP architecture model in the 1993, DICOM policy regarding Internet Recommendations was to integrate them as soon as they are stable and largely disseminated in consumer commercial products.

At the present time, the pressing needs in DICOM, tackled by various working groups of the DICOM Standards Committee, are to address issues relating to security, performance, new modality technology, and workflow management. These needs are being successfully addressed adopting proven international, industry or de facto standards. Accordingly, network confidentiality and peer authentication in DICOM are provided by the use of either TLS or ISCL. Rather then develop medical-image-specific compression schemes, DICOM adopts standards developed by ITU-T / ISO/IEC JTC 1/SC 29/WG 1 such as JPEG (ITU-T T.80 series | ISO/IEC 10918) and JPEG 2000 (ITU-T T.800 series | ISO/IEC 15444). For interchange media, standard file systems compatible with conventional software such as ISO 9660 and UDF are used.

A brief overview of Parts 2, 3, 4, 5, 6, 7 and 8 which are referenced in the normative technical requirements of the DICOM specification is provided here.

9.4.2.1.1 Part 2: Conformance

Part 2 of DICOM defines principles that implementations claiming conformance to DICOM shall follow:

- Conformance requirements. Part 2 specifies the general requirements which must be met by any implementation claiming conformance. It references the conformance sections of other Parts of DICOM.

- Conformance Statement. Part 2 defines the structure of a Conformance Statement. It specifies the information which must be present in a Conformance Statement. It references the Conformance Statement sections of other Parts of DICOM. The use of privately defined extensions to DICOM is also addressed.

Part 2 does not specify a testing/validation procedure to assess an implementation's conformance to DICOM. A Conformance Statement consists of three major Parts specifying:

- An implementation model which provides an overall description of the Application Entities.
- A set of Service Classes supported by this implementation and the corresponding Information Objects.
- A set of communication protocols which this implementation supports.

9.4.2.1.2 Part 3: Information Object Definitions

Part 3 of DICOM specifies a number of Information Object Definitions which provide an abstract data model applicable to the communication of medical images and related patient data. The Attributes of an Information Object Definition describe its properties. Each Information Object Definition does not represent a specific instance of real-world data, but rather a class of data which share the same properties. An Information Object Definition does not specify values for its Attributes.

Two types of Information Object Definitions are specified: normalized and composite.

Normalized Information Object Definitions include only those Attributes inherent in the real-world entity represented. For example, the study Information Object Definition, which is defined as normalized, contains study date and study time attributes because they are inherent in an actual study. Patient name, however, is not an Attribute of the study Information Object Definition because it is inherent in the patient on which the study was performed and not the study itself. When an instance of a Normalized Information Object Definition is exchanged, the context of that object instance is provided through the use of pointers to related normalized object instances.

Composite Information Object Definitions may additionally include Attributes which are related to but not inherent in the real-world entity represented. For example, the Computed Tomography Image Information Object Definition, which is defined as composite, contains both Attributes which are inherent in the image (e.g. image size) and Attributes which are related to but not inherent in the image (e.g. patient name). When an instance of a Composite Information Object Definition is exchanged, the context of that object instance is provided within that object instance itself.

To simplify the Information Object Definitions, related Attributes are grouped together into Modules. Modules represent a higher level of semantics than individual Attributes. These modules may be reused by other Information Object Definitions.

To represent an occurrence of a real-world entity, an instance of an Information Object is created, which includes values for the Attributes of the Information Object Definition. The Attribute values of this Information Object instance may change over time to accurately reflect the changing state of the entity which it represents. This is accomplished by performing different basic operations upon the Information Object instance to render a specific set of services defined as a Service Class. These Service Classes are defined in Part 4 of DICOM.

Part 3 also is related to other parts of the DICOM Standard in that:

Part 5, Data Structures and Encoding, defines the Data Set structure and encoding of DICOM Information Object Instances.

Part 6, Data Dictionary, defines the individual DICOM Data Elements which convey the Information Object Attributes defined in Part 3.

9.4.2.1.3 Part 4: Service Class Specifications

Part 4 of DICOM defines a number of Service Classes. Service Class Specifications are made of one of more Service-Object Pair (SOP) Classes related to a specific function to be performed by communicating Application Entities. A Service-Object Pair associates an Information Object Definition with one or more DICOM services (Operations and/or Notifications) to be performed upon that object.

The selection of SOP Classes is used by Application Entities to establish an agreed upon set of capabilities to support their interaction. A SOP Class is the elementary building block of the Standard for which conformance may be claimed. A SOP Class states requirements for applicable Operations/Notifications and how they may be applied to Information Objects. Service Class Specifications state requirements for both Service Class Users (often called clients) and Service Class Providers (often called servers).

The body of Part 4 of the DICOM Standard defines the characteristics shared by all Service Classes and their specific SOP Classes. This is followed by a number of normative annexes which describe individual Service Classes and each one of their SOP class in detail.

9.4.2.1.4 Part 5: Data Structure and Encoding

Part 5 of DICOM specifies how DICOM Application Entities construct and encode the Data Set information resulting from the use of any one of the Information Objects and Services Classes defined in Parts 3 and 4 of DICOM. The support of a number of standard compression techniques (JPEG lossless and also lossy) is specified.

Part 5 addresses the encoding rules necessary to construct a Data Stream to be conveyed in a Message as specified in Part 7 of DICOM. The various Value Representations available to represent values of Data Elements are specified, including specific constraints (character sets, length, etc.). This Data Stream is produced from the collection of Data Elements making up the Data Set. Data Sets may be nested to transfer in "one package "the content of more complex Information Objects, offering a folder capability.

9.4.2.1.5 Part 6: Data Dictionary

Part 6 of DICOM is the centralized register which defines the collection of all DICOM Data Elements available to represent information. For each Data Element, Part 6:

- Assigns it a unique tag, which consists of a group and element number.
- Gives it a name.
- Specifies its Value Representation (character string, integer, etc.) and its Value Multiplicity when a Data Element may contain more than a single value.

Part 6 also includes the register of Unique Identifiers used to unambiguously label SOP Classes and Transfer Syntaxes standardized by DICOM.

Part 6, in conjunction with Part 5, are used to construct Data Sets, and to represent Information Objects as Data Sets.

9.4.2.1.6 Part 7: Message Exchange

Part 7 of DICOM specifies both the DICOM Message Service Element (DIMSE) and protocol used by an Application Entity in a medical imaging environment to exchange Operation and/or Notification Messages over the communication support services defined in Part 8. A Message is

composed of a Command Set as defined in Part 7 followed by an optional Data Set as defined in Part 5. This Part specifies:

- The rules to establish and terminate associations provided by the communication support specified in Part 8, and the impact on outstanding transactions. In particular, it specifies as part of the Association establishment the negotiation of the SOP Classes and associated encoding (Transfer Syntaxes).
- The Operation and Notification Services (DIMSE Services) made available to Service Classes defined in Part 4.
- The protocols that govern the exchange of Command requests and responses which provide these DIMSE services;
- The encoding rules necessary to construct Command Streams and Messages.

9.4.2.1.7 Part 8: Network Communication Support for Message Exchange

Part 8 of DICOM specifies the communication services and the upper layer protocols necessary to support, in a networked environment, the DICOM Application Message Exchange as specified in Parts 3, 4, 5, 6, and 7. These communication services and protocols ensure that the DICOM Application Message Exchange is performed in an efficient and coordinated manner across the network.

The communication services specified in Part 8 are a proper subset of the services offered by the Presentation Service (ISO 8822) and of the OSI Association Control Service Element (ACSE) (ISO 8649). They are referred to as the Upper Layer Service, which allows peer Application Entities to establish associations, transfer messages and terminate associations.

9.4.3 Future scope:

It is clear that the use of DICOM objects and services in common information technology applications will grow in the future. The appliance of the DICOM standard in new medical specialties should be focused by the creation of new working groups. With the rapid evolution of most of the information and communication technologies attention should be paid to them in order to accomplish best to the ever increasing requisites of quality, security, accessibility and cost effectiveness for the imaging diagnostic purposes. Over 90 supplements have been published up to now covering detected needs on different parts of the DICOM standard where currently priorities are principally related to security, procedure reports, the enhancement of SOP classes and new technologies. This work needs to go on. Taking into account the position of the stakeholders involved and the feedback of end users the DICOM standard should find the way to face future challenges and fulfil new trends. Finally, maintaining coordination efforts with other standardisation groups should continue being a priority.

9.5 Healthcare Information Interchange

Healthcare is an information-intensive and a communication-intensive business. The volume of information exchanged between departments within hospitals and between primary and secondary care providers is large. Some 15% of a hospital’s running costs and 25% of the time of doctors and nurses are devoted to information processing.

9.5.1 EDI

EDI stands for Electronic Data Interchange. EDI is the interchange of standard formatted data between the computer application systems of trading partners with minimal manual intervention. The data in a business transaction often have a paper equivalent such as an order or invoice. It is formatted according to specified standards and structures, into agreed messages. EDI concerns

communication within a company and between companies, excluding communications from data entry or dump terminals to host computers. EDI can be implemented across a wide range of business activities, including all areas of commerce, such as manufacturing, finance, construction, and tourism. EDI messages cover all aspects of transport and government functions such as customs and excise. EDI implies the need for interchange agreements between the business partners, to establish and agree the message structures and communications being used.

9.5.2 EDIFACT

Computer communication needs a common language or system of interpretation. Interpretation or data conversion between two trading partners may work well, but with more partners the conversion process becomes unmanageable. EDI provides a common language for business communication. This common language, or EDI standard, consists of a grammar (syntax and rules for structuring the data) and a vocabulary (contained in the directories of data elements, composite data elements, segments, and messages). However, it is practically impossible to achieve a single global standard in the information technology industry. Several EDI standards have been developed over the last few years, although there is now a move towards the single standard, EDIFACT. EDIFACT has been established as the international standard. It has been developed from a combination of standards: UN/TDI under the auspices of the ECE with European and North America input; and the American National Standards Institute (ANSI X12). Industry-specific EDI associates include: ODETTE (Organization for Data Exchange by Tele-transmission in Europe), CEFIC-EDI (European Chemical Industry Federation), EDIFICE (Electronic Data Interchange Forum for Companies interested in Computing and Electronics), EAN-COM (International Article Numbering Association EDI project.

Various countries carried out separate standardisation activities, resulting in different standards. The UK and French developments were merged under the UN/ECE and the resulting standard, known as Trade Data Interchange (TDI), gained general approval. However, the United Nations European Economic Commission (UN/ECE) required an international standard for trade and administrative projects. In November 1985, a joint working group was set up by European and American EDI experts (UN/JEDI) and its aim was to bring together the ANSI X12 and UN/ECE GTDI work to create a full standard. Their discussions produced the UN/EDIFACT standard. The UN/EDIFACT standard ISO 9735 document details the syntax rules and its appendices provide descriptions of service segments. These syntax rules have to be combined with other UN derived documents to produce operational EDIFACT messages.

9.5.2.1 EDIFACT Interchange

The components of an EDIFACT system are:

Date Elements (Simple and composite).

- Segment.
- Message.
- Functional Group.
- Interchange.
- Syntax rules.
- Message Design Guidelines.

Data elements are the vocabulary of the language of an EDI communication. Data elements identify an individual field or item of data designed for a specific purpose, such as a product code, postal code, unit price, expiration date. These single items are simple data elements and can be combined

to form composite data elements. Most data is in fact represented in composite data elements. For example, a composite data element could be a monetary amount, made up of the component data elements of the monetary amount and the currency.

Segments are functionally related and logical groups of data. Messages are communications of particular business functions. Functional groups are groups of messages of the same type, within an interchange.

9.5.3 HL7: Version 3.0

Version 3 represents a significant departure from "business as usual" for HL7. Offering lots of optionally and thus flexibility, the V2.x series of messages were widely implemented and very successful. These messages evolved over several years using a "bottom-up" approach that has addressed individual needs through an evolving ad-hoc methodology. There is neither a consistent view of that data that HL7 moves nor that data's relationship to other data. HL7's success is also largely attributable to its flexibility. It contains many optional data elements and data segments, making it adaptable to almost any site. While providing great flexibility, its optionality also makes it impossible to have reliable conformance tests of any vendor's implementation and also forces implementers to spend more time analyzing and planning their interfaces to ensure that both parties are using the same optional features. Version 3 addresses these and other issues by using a well-defined methodology based on a reference information (i.e., data) model. It will be the most definitive standard to date. Using rigorous analytic and message building techniques and incorporating more trigger events and message formats with very little optionally, HL7's primary goal for Version 3 is to offer a standard that is definite and testable, and provide the ability to certify vendors' conformance. Version 3 uses an object-oriented development methodology and a Reference Information Model (RIM) to create messages. The RIM is an essential part of the HL7 Version 3 development methodology, as it provides an explicit representation of the semantic and lexical connections that exist between the information carried in the fields of HL7 messages.

The initial release of Version 3 use only XML encoding.

9.5.4 ENV1306 part 4

The pre-standard ENV 13606 part 4 “Messages for the exchange of information” specifies messages that enable exchange of electronic healthcare record information between healthcare parties responsible for the provision of clinical care to an individual patient. There are three types of messages: request EHR message, provide EHR message, and EHR notification message. All messages contain the attributes: identification of message by originator, issue date and time of message, urgency of message, message receipt acknowledgment request, and optionally the attributes: comment on message, and language. All messages contain the classes: EHR source, EHR destination, patient matching information, and optionally the classes: EHR message related agent, healthcare agents’ directory, and message reference.

The Domain Information Model (DIM) is a set of classes that consist of the conceptual model describing common concepts and their relationship for all EHR messages. The DIM is divided to eight subsystems such as communicating parties’ subsystem, message subsystem, structured record subsystem, etc. Specialization of the DIM is provided by a General Message Description (GMD) which contains a subset of the DIM prescribing the information content and semantic structure of a message used to meet one or more identified information interchange requirements.

There is a separate GMD for each type of message that shows the hierarchical decomposition of each message into its main classes.

9.5.5 E31 ATSM Committee

E31-ASTM has several standards for messaging in the healthcare domain as follows:

9.5.5.1 ASTM E1238-97 “Standard Specification for Transferring Clinical Observations between Independent Computer Systems”

This standard is used by most of the largest commercial laboratory vendors in the US to transmit laboratory results. This standard has been transferred to NCCLS and is now published as an ANSI accredited standard numbered LIS03-A.

9.5.5.2 ASTM 1394-97 “Clinical Laboratory Instruments to Computers”

It has been developed by a consortium consisting of most US manufacturers of clinical laboratory instruments and is being implemented in the current laboratory instruments generation.

This standard covers the two-way digital transmission of remote requests and results between clinical instruments and computer systems. It is intended to document the common conventions required for the interchange of clinical results and patient data between clinical instruments and computer systems. This standard specifies the message content for transferring information between a clinical instrument and a computer system. It enables any two such systems to establish a logical link for communicating text to send result, request, or demographic information in a standard and interpretable form. This standard does not necessarily apply to general analytical instruments in an industrial analytical nor research and development setting.

This standard specification is intended to apply to the structure of messages exchanged between clinical instruments and computer systems by means of defined communications protocols. Low-level communications protocols and data transfer requirements are beyond the scope of this standard. A separate specification is available from ASTM detailing a standard for low-level data transfer communications.

This standard specifies the conventions for structuring the content of the message and for representing the data elements contained within those structures. It is applicable to all text oriented clinical instrumentation. It has been specifically created to provide common conventions for interfacing computers and instruments in a clinical setting. It would also be applicable to interfacing instruments in clinical practice settings, such as physicians' offices, clinics, and satellite laboratories.

9.5.5.3 ASTM E1467-94 (2000) “Standard Specification for Transferring Digital Neurophysiological Data Between Independent Computer Systems”

This standard defines codes and structures needed to transmit electrophysiologic signals and results produced by electroencephalograms and electromyograms. The standard is similar in structure to ASTM 1238 and HL7, and is being adopted by all of the EEG systems manufacturers.

This specification covers transmission of digitally recorded electro-physiologic waveform data and related textual annotations between laboratories or clinics, or between computer systems in a given laboratory or clinic. This includes all electro-neurophysiology (EN) studies such as electroencephalograms (EEG) and magneto-encephalograms (MEG), polysomnograms (PSG) and multiple sleep latency tests (MSLT), evoked potentials (EP) and evoked magnetic fields (EMF), event-related potentials (ERP), electro-myograms (EMG) and nerve conduction studies (NCS), and many others in either a clinical or research environment. Although this specification is concerned primarily with electro-neurophysiology, the methods used for encoding waveform and related data would be suitable for other tests involving waveforms, such as electrocardiograms (EKG), vascular/intracranial pressure monitoring, oximetry, or gastrointestinal motility studies.

It also defines a format for waveform data based on Specification E 1238 (developed in cooperation with HL7), with extensions to support the transmission of multi-channel time-series waveforms.

It may be applied either to two-way transmission of data over medium- to high-speed data communication networks, or one-way transmission of data by recording on and later playback from

magnetic or optical digital storage media. It defines the blocked stream of data, called a message, which is transmitted over a network connection or recorded on a storage medium. It does not define the hardware or software network protocols or storage media formats needed for message transmission (for example, see ISO 8072), or the formats used to store data internally by the sender or receiver.

Recognizing, however, that some standardisation in storage media format and network protocols would help to promote exchange of data between computer systems with diverse hardware and software, it is suggested that readily available universal media and formats be used, when possible, for data exchange. An example suitable for transmission of large amounts of digital waveform data would be the use of industry-standard magnetic tape or digital audio tape (DAT), with ANSI standard tape labels, employing variable length blocked records (lines) with a maximum block size of 4092 bytes. Individual lines within the blocks would be terminated by carriage return characters, Code 13 in the American Standard Codes for Information Interchange (ASCII). As another example, for the transmission of moderate amounts of digital waveform data, floppy disks written in MS-DOS (1) format (or another commonly used directory and file structure) would be appropriate; the data would be contained within a single sequential file on the disk, with lines within the file delimited by carriage return (ASCII 13) or carriage return followed by linefeed (ASCII 10) characters. An example of network hardware and software suitable for transmission of waveform data would be Ethernet (2) and the TCP/IP (3) protocol.

9.5.5.4 ATSM E1712-97 "Standard Specification for Representing Clinical Laboratory Test and Analyte Names"

This specification covers the construction of elected laboratory test and analyte names, because data concerning clinical laboratory tests must identify these tests in a common fashion if such data are to be transferable between databases or to be recognized in lookups or searches. It details the representations of test and analyte names as they are used in the clinical laboratory and in either the patient care record or the messages that exchange requests for those tests and analytes and return results to the requestor for insertion into the record. This specification details the form of the elected standard test name and resulting analytes in records and messages. It was written to unify several existing conventions that have been published for the identification of laboratory procedures or other billable or cost management items. It is intended to produce an explicit identifier not only of the test but also of each of the constituent results for each unique analyte. It is applicable to those situations that refer to the names of either the tests or the analytes resulting from clinical laboratory testing. These situations may include the following: Computer-based Patient Record Systems (CPR), Clinical Laboratory Information Management Systems (CLIMS), billing systems, cost identification and management systems, clinical decision support systems, epidemiologic registries and databases, and clinical research information management systems. The mnemonics of that name and the codes to be used as unique identifiers for the names of either the tests or resulting analytes are given as examples in a non-normative appendix.

9.5.5.5 ATSM E1713-95 "Standard Specification for Transferring Digital Waveform Data between Independent Computer Systems"

This standard defines transferring digital waveform data between independent computer systems.

9.5.6 SCP-ECG

The electrocardiogram (ECG) is a recording of voltage changes transmitted to the body surface by electrical events in the heart muscle, providing direct evidence of cardiac rhythm and conduction, and indirect evidence of certain aspects of myocardial anatomy, blood supply and function. During its propagation to the surface, extra-cardiac tissues may intervene and influence the ECG. It is estimated that more than 100 million standard ECGs are recorded yearly in the European

Community (EC) for routine diagnostic and screening purposes at an estimated cost of more than 1.2 billion ECU per year.

Almost all newer electrocardiographs nowadays use digital recording, interpretation and communication techniques. These stand-alone, microcomputer based machines can be connected to each other, and to larger minicomputer-based management servers for long-term storage and serial comparison. To this end, various manufactures have used different techniques.

To enable the inter-connectivity of various systems it was of utmost importance that a standard communication protocol for computer-aided electrocardiography (SCP-ECG) had to be established, as defined in the present document. The primary aim of this standard is to ensure that ECG reports and data from any vendor's computerized ECG recorder can be transmitted on a direct connected serial line to any other's vendor central ECG management system. The same standard should also allow standardized transmission of digitized ECG data and results between various computer systems.

ECG computer processing can be reduced to 3 principal stages:

- Data acquisition, encoding, transmission and storage.
- Pattern recognition and feature extraction, i.e. ECG measurement.
- Diagnostic classification.

In each of these stages there are important needs for standardisation and quality assurance testing. The scope of SCP-ECG standard is confined to the first of these stages. It covers the two-way digital transmission of remote requests and results between digital electrocardiographs (ECG carts) and heterogeneous computer systems (hosts). It documents the common conventions required for the cart-to-host as well as cart-to-cart interchange of specific patient data (demographic, recording, etc.), ECG signal data, ECG measurement and ECG interpretation results.

This standard specifies the content and structure of the information which is to be interchanged between digital ECG carts and computer ECG management systems (ECG DBMS), as well as other computer systems where ECG data can be stored. It enables any two such systems to establish a logical link for communicating ECG-related data in a standard and interpretable form.

Interoperability in Digital Electrocardiography

The mission of the OpenECG project is to promote the consistent use of format and communications standards for computerized ECGs and to pave the way towards developing similar standards for stress ECG, Holter ECG, and real-time monitoring. OpenECG, coordinated by an interdisciplinary, highly motivated consortium, will attract membership from healthcare authorities, cardiologists, integrators, engineers, standardisation bodies, manufacturers, and the public.

Its specific goals with regard to computerized ECG standards are:

- To raise the level of awareness.
- To organize information days, workshops, and a programming contest.
- To consolidate expertise, assist integration and support correct implementations.
- To provide feedback to standardisation bodies.
- To prepare the ground for interoperability in other ECG-related examinations.

At the same time, OpenECG will collaborate with other groups that are working to formulate and implement standards in cardiology. OpenECG plans to bring the SCP (Standard Communications Protocol) to life by supporting specific implementations and applications. This ECG Standard is the result of an EU supported project that European, American and Japanese Manufacturers and Users

have jointly worked and agreed on (1989-1990). In 1993 it became a European ENV, later positively balloted within AAMI (AAMI EC71), and is currently a new work item proposal to IEC TC/SC 62 WG1 and ISO TC215.

The OpenECG portal will present news, reviews, and success stories. Registered members will have access to discussion groups, a help desk, and a collection of tools for handling SCP-ECG data (analyzers, converters, viewers, etc.). A database containing annotated samples of real SCP implementations will provide further help in the proper implementation of the SCP-ECG standard by manufacturers and integrators. Finally, analysis has already started for an on-line SCP-ECG certification and conformance testing service that will also be available to members of the OpenECG portal.

The creation of a network that builds on the experience and vision of the early adopters is expected to facilitate the open exchange of high quality computerized ECGs, making lack of interoperability an obscure problem of the past and setting an example for other diagnostic examinations in the domain of cardiology.

9.6 Patient identification

ATSM E1714-00 "Standard Guide for Properties of a Universal Healthcare Identifier (UHID)" covers a set of requirements outlining the properties of a national system creating a universal health care identifier (UHID). Use of the UHID is expected to be limited to the population of the United States.

This guide sets forth the fundamental considerations for a UHID that can support at least four basic functions effectively:

- Positive identification of patients when clinical care is rendered;
- Automated linkage of various computer-based records on the same patient for the creation of lifelong electronic health care files;
- Provision of a mechanism to support data security for the protection of privileged clinical information; and
- The use of technology for patient records handling to keep health care operating costs at a minimum.

This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.

9.7 Healthcare Identifiers

To standardise the players across the healthcare spectrum like:

- Healthcare Professionals: physicians, nurses, dentists
- Healthcare Provider Organisations: hospital, clinics, nursing homes, rehabilitation centres, PHCs
- Support Service Providers: pharmacies, diagnostic centres, blood banks, laboratories
- Individuals
- Employers
- Payers: Insurance firms, Third Party Administrators TPA, brokers

9.8 Minimum Data Sets

Finding a widely agreed upon and generally accepted set of terms and definitions making up a core of data acquired disease in a standard format like:

- MDS common across all diseases such as referrals and demographics
- Specific to some diseases such as risk factors, complications and treatment

To initiate the standardisation activity, minimum data sets could be recommended for the most common diseases.

9.9 Billing Formats and financial and health care transactions

Regarding the eight important transactions that take place in the health insurance sector to be standardised with mandatory fields to be used across various stakeholders:

- Enrolment and disenrolment in a Health Plan
- Health Plan Premium Payments
- Eligibility Check/ Credit Authorisation
- Billing for Covered Services
- Claim Submission for Covered Services
- Healthcare Claim Status Query
- Health Care Payment and Remittance Advice
- Payment for Covered Services

10 Conclusions

This document presents a quite complete vision of standardisation applied to different fields in the e-health and telemedicine. Some fields are still missing as contributions have not been received for those topics. Those gaps shall be covered in the following version of this roadmap.

Meanwhile, some reflections rise from this document:

Dealing with **clinical devices**, standards exist for device managements and data exchange although its use is not common due to vendor's policies. However, users have to ask for them and use them as they do really exist.

For **real time group work and videoconference**, no specific standard for e-health and telemedicine is needed in addition to the existing ones although higher QoS and tools to manage QoS are usually requested. Therefore, a consensus about the minimum QoS required for different e-health activities is highly recommended (i.e. minimum bandwidth for a tele echography session in real-time). The same concerns apply to **communication** techniques where common standards are also valid for e-health and telemedicine applications.

Messaging standards is also a topic where standards are available, being XML and the web services the key issues for most of these standards. It has been assumed that more than one messaging standard shall be present in the e-health market although interoperability seems guaranteed with CEN, HL7, and IHE, etc.

Security needs are properly covered with existing standards and technologies although there is a problem in the harmonization of laws dealing with e-health and security at international level. That makes impossible more common standardisation efforts in this area as needs to fulfil the law are different in each country.

For **clinical data representation, clinical standards and terminology** an extended state of the art analysis has been performed. Again, problem for the standardisation in e-health is not due to the absence of standards (they do exist and there are best practices to show their benefits and performance) but the absence of proper policies to extend in a coherent and homogeneous way these standards all over the world.

Since the formal starting of Q.28/16 in ITU-T SG 16 for standardisation in e-health, various related initiatives have appeared, such as the e-Health Standardisation Coordination Group (**eHSCG**), the Telemedicine Alliance (**TMA**) Project, the Integrating the Healthcare Enterprise initiative (**IHE**), the **ISS-CEN** eHealth Standardisation Focus Group. Most conclusions from such initiatives are consistent with those of this roadmap, showing alignment among all SDOs in the e-health field in order to not reinvent the wheel and avoid duplicated efforts. For example, recommendations to the EU Member States from the **ISS-CEN** eHealth Standardisation Focus Group are summarised in the following lines.

- establish an interoperability platform
- improve access to records
- promote e-prescribing
- control the safety of health informatics products
- produce standards on metadata to ensure quality of information
- standardise workflow models and clinical pathways
- promote the electronic transfer of prescriptions
- guarantee the information exchange to support cooperation
- provide tools of underpinning coding systems for diagnoses and procedures
- identify the priority indicators of quality of care
- improve the availability of standards
- develop an international multilingual reference terminology
- promote the use of health cards
- use standards for patient identification and information access

This roadmap has identified the gaps to be covered with new standards and how to use existing standards to promote interoperability at different levels in a multimedia e-health framework. The following version of this roadmap shall also include recommendations and activities to carry out in order to harmonize and coordinate these efforts and future evaluation strategies across projects and initiatives in order to fulfil the real needs of standardisation.

Future versions of this roadmap will aim at improving the existing descriptions and adding other relevant ones, based on feedback from experts.

Annex A:
List of interoperability studies

This Annex compiles documents, studies and reports dealing with interoperability in e-health that can provide a valuable input to reach the goals of ITU-T Question 28/16.

A. Report from the CEN/ISSS eHealth Standardisation Focus Group: Current and future standardisation issues in the eHealth domain: Achieving interoperability[23]

This report covers five strategic aims which appear to have particular prominence and commonality within Europe namely:

- improving access to clinical records;
- enabling patient mobility and cross border access to health care;
- reducing clinical errors and improving safety of patients;
- improving access to quality information on health for patients and health professionals;
- improving efficiency of healthcare processes.

B. Telemedicine Alliance – a bridge towards coordinated e-health implementation: Interoperability Study Report[24]

This Interoperability Study Report from the TMA-Bridge provides background material on achieving interoperability concerning trans-border issues of national health services with emphasis on the citizen. It is targeted to support decision-makers in the European commission and the European Member States, especially with regard to trans-national e-Health.

C. eHSCG standards list[25]

This compilation collects the most important standards in all technical and non-technical areas of e-health. The document is broken into two sections – the 'table-of-contents', and a more detailed description. Each description is bookmarked, and tied to the table-of-contents entry.

D Telecommunication Development Bureau, ITU-D[26]

D.1 Document RGQ14-1/2/047-E: Telemedicine and Biometrics

The biometric methodologies and effects on telemedicine are discussed in this paper. ITU-D feel that the optical sensor (face, iris, and retina) using the videophone system is a promising biometrics system for telehomecare.

ITU-D proposes the inclusion of optimized biometric methodologies and guidelines as a theme of ITU's E-Health standardisation.

---

[23] Availableat http://www.centc251.org/FocusGroup/eHealthStandardizationExecutive%20summaryFinalversion2005-03-01.pdf

[24] Available at http://www.esa.int/SPECIALS/Telemedicine_Alliance/SEM0CASMD6E_0.html

[25] Available at http://www.ehscg.org/

[26] Available under request to ITU-D Q14-1/2 by E-mail: leonid.androuchko@ties.itu.int

D.2 Document RGQ14-1/2/046-E: A proposal of telemedicine reference model for standardisation

This contribution proposes a telemedicine reference model for standardisation. The necessity of the telemedicine reference model has been recognized by ITU-T/D to realize telemedicine equipment portability internationally. Specifically, just in the case of Tsunami disasters on 26 December 2004, wide regional areas in Indian Sea were attacked and more than 273,000 people died. In such a disaster, international medical team co-operations should be necessary, and actually many medical teams came to rescue the wounded.

Telemedicine equipment has also been utilized, but portability of the medical equipment was difficult because of the different interfaces.

Therefore, it is necessary to have the standardisation of the interface between medical equipment and telecommunication systems. In this contribution, requirements for the telemedicine reference model are discussed, then a proposed functional reference model is illustrated and finally an example physical implementation is summarized.

E. Document RGQ14-1/2/034-E: Metadata Standardisation for telemedicine

In this document is proposed the metadata standardisation as the resolution of interoperability issue of telemedicine systems. In telecommunication process of telemedicine systems, the difference outside the scope of medical information standards and the different kinds of transferring data methods and terminals can cause operational problems. ITU-D suggests that if the information of these differences can be gathered and exchanged as metadata, smooth communication can be achieved.

F. Document RGQ14-1/2/045-E: A proposal for telemedicine package standardisation

This contribution describes necessities for the telemedicine package standardisation to facilitate quick and efficient medical treatment for various disastrous cases.

Appendix I:
Terrestrial links

Table I.1 summarises key features of terrestrial link technologies that can be used in e-health applications.

Table I.1: Comparison between terrestrial links

Terrestrial Link	Typical Speed	Transmission Technologies	Related Standards
ADSL	**12Mbit/s (Downstream)**	**FDM on metallic line**	**G.992.x**
Cable	**30Mbit/s**	**hybrid fiber coaxial**	**J.112, J.122**
PON	**622Mbit/s 1000Mbit/s**	**TDM and WDM on optical fiber**	**G.983.x, G.984.x IEEE1000BASE-PX**
FR	**2Mbit/s**	**Switched Packet**	**X.25**
ISDN	**64Kb (generic) 2Mb International**	**B(64kb)-Channels association**	**G.960 G.962**
ATM	**155.52Mbit/s**	**Fixed length TDM cell**	**I.432.x**
SDH/SONET	**155.52Mbit/s**	**TDM frame**	**G.707/Y.1322**
Ethernet (Fast Ethernet)	**100Mbit/s**	**Variable length TDM frame**	**IEEE100BASE-TX (For metallic cable) IEEE100BASE-FX (For optical fiber)**