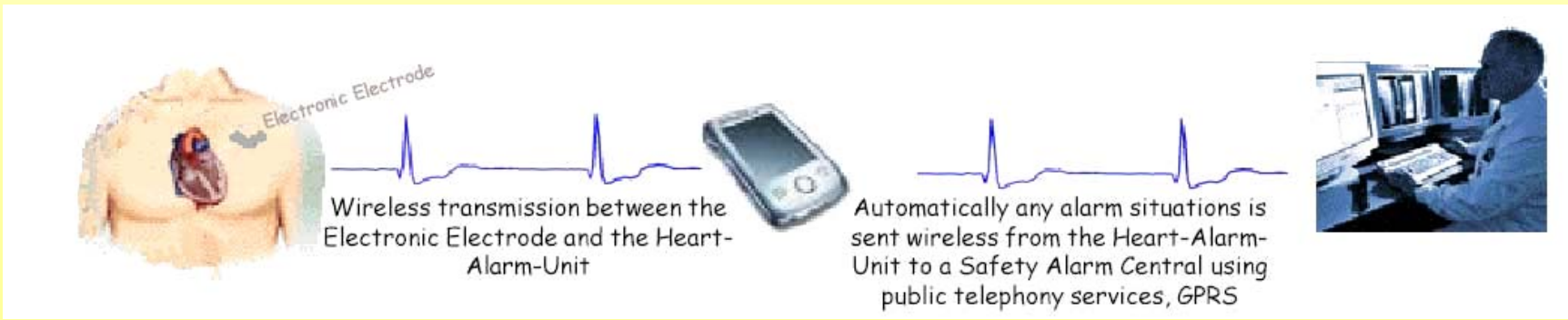
MOBILE MONITORING OF VITAL PARAMETERS WITHIN THE ELECTRONIC HEALTH RECORD (EHR)- MEDICAL, TECHNOLOGICAL AND LEGAL ASPECTS

Fensli, Rune[1] Gunnarson, Einar[2]

[1] Agder University College, Faculty of Engineering and Science, Grimstad, Norway

[2] Hospital of Buskerud, Department of acute medicine, Drammen, Norway



Abstract

- New wireless technology gives possibilities for measuring of vital parameters at home
  - Tele Home Health Care (THHC) is increasing
  - Recordings are sent electronically to the doctor
  - This information needs to be stored as a part of the EHR
  - Thus the patient need authorized access to his EHR
- It is unclear which security actions are needed
- It is a question who can create a “collective EHR”
- Some advises are given in developing solutions

Internet Health Services

- New Internet Health Services are developed
  - General medical advices – typical "doctor-online"
  - Patient oriented services – specific sensitive information with questions and to follow-up your disease/medication
    - New service are established in the Norwegian Health Network
    - "PasientLink" – an Internet based contact between the patient and the doctor (developed by NST and Well Communication)
  - 45% of patients wants to have e-mail based contact with their doctor using Internet solutions*

* Andreassen et al.: *"Nordmenns bruk av helsetilbud på Internett".* Tidsskr Nor Lægeforen, nr 17, 2002; 122; 1640-4.

National Strategies in Norway

"S@mspill2007" (Ministry of Health and Social Affairs, 2004)

- Improve the quality in health care using IT-solutions
- Use of electronic cooperation in order to achieve a comprehensive solution in the patient progress
  - Patient involvement in the treatment process
  - Electronic ordering of a session with the doctor
  - Electronic prescription of drugs directly to the chemist's
  - Electronically cooperation between hospitals, Regular General Practitioners (RGP) and The Municipal Health Care Providers
- Of importance for the patient and his relatives

- Develop solutions based on the patient's terms

Biomedical recordings in the THHC

- The patient have possibilities for adequate recordings of biomedical signals at home
  - ECG-recordings
  - Blood Pressure
  - Glucose analyses
  - Respiratory parameters

- The measuring equipment is mobile and by use of a mobile phone the recordings can be stored as a fragment of the EHR in a database

Juridical rights to access your EHR

Legal privileges to the patient:

- Personal Health Data Filing System Act, HA (Helseregisterloven)
  - ***The person responsible for the EHR*** can give access to co-workers who need the information in order to perform treatment
- The Patients´ Rights Act (Pasientrettighetsloven)
  - Contains the requirements of the patients access to the EHR
  - Based on the intentions of the act, one can claim that the patient himself is **"*THE PROPRIETOR*"** of information stored in his EHR
- Personal Data Act (Personopplysningsloven)
  - Have requirements to protect unauthorized access to the EHR
  - Based on the intentions of the act, one can claim this act is to ensure the persons need of protection – he can decide **how** to be protected and **to whom** give privileges to access the information

Who is responsible for the EHR?

- Norwegian Data Inspectorate have based on §13 in HA stated that **access to EHR only can be given to personnel within a hierarchic organisation context** *
  - This will prohibit direct access to the EHR from personnel outside a hospital's organization (e.g. Regular General Practitioners)
- The Managing Director of the hospital is the person responsible for the EHR and the security actions needed
  - He has to ensure that needed security requirements are fulfilled
  - Before sending electronic information from the EHR-system, he has to ensure that the receiving person/organization also have fulfilled all security recommendations
- The RGP - doctor has the same responsibility
- Within the municipal social and health care sector, this person probably must be the mayor or the city manager

* Norwegian Data Inspectorate. "Vedtak om pålegg til helse Bergen HF"; 2002 06.05-2003.

Exchange of medical information

- Health organizations are based upon a hierarchical security solution with a Managing Director as the top administrative responsible person (also for the EHR)

There are established secure mechanisms for exchange of sensitive medical information with solutions based on XML and secure message handling

But a RGP-doctor is not allowed to logon to a hospitals internal EHR system simply because the doctor is outside of the hospitals security responsibility

Integrated solutions are desirable

- Information exchange needs to be within a distributed system with an integrated portal to all necessary medical records

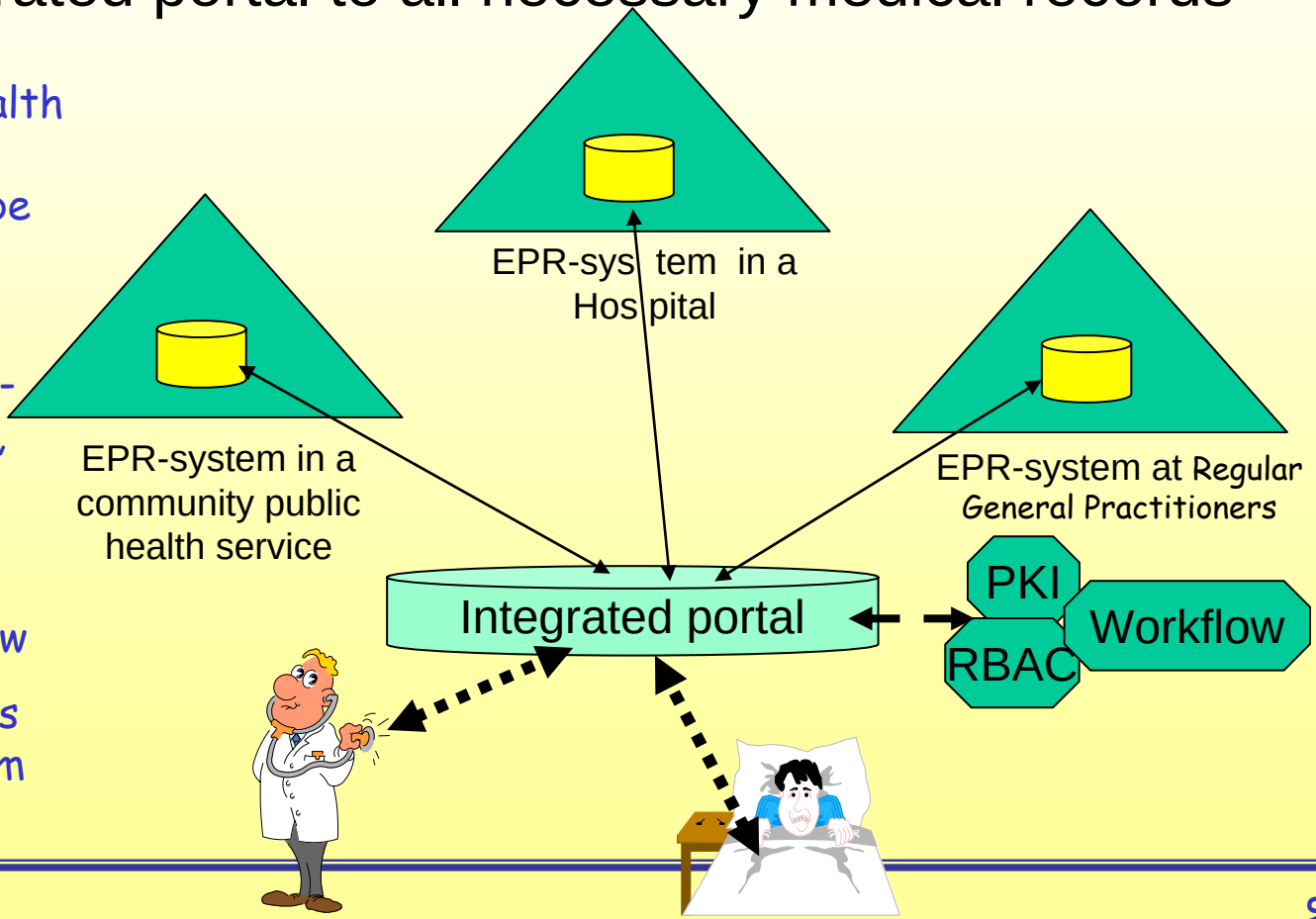
Both patients and health care workers need a dedicated access to be able to share the information

PKI- Public Key Infra-structure (DigitalID),

RBAC – Role Based Access Control

and Dynamic Workflow

are technical solutions to the security system requirements



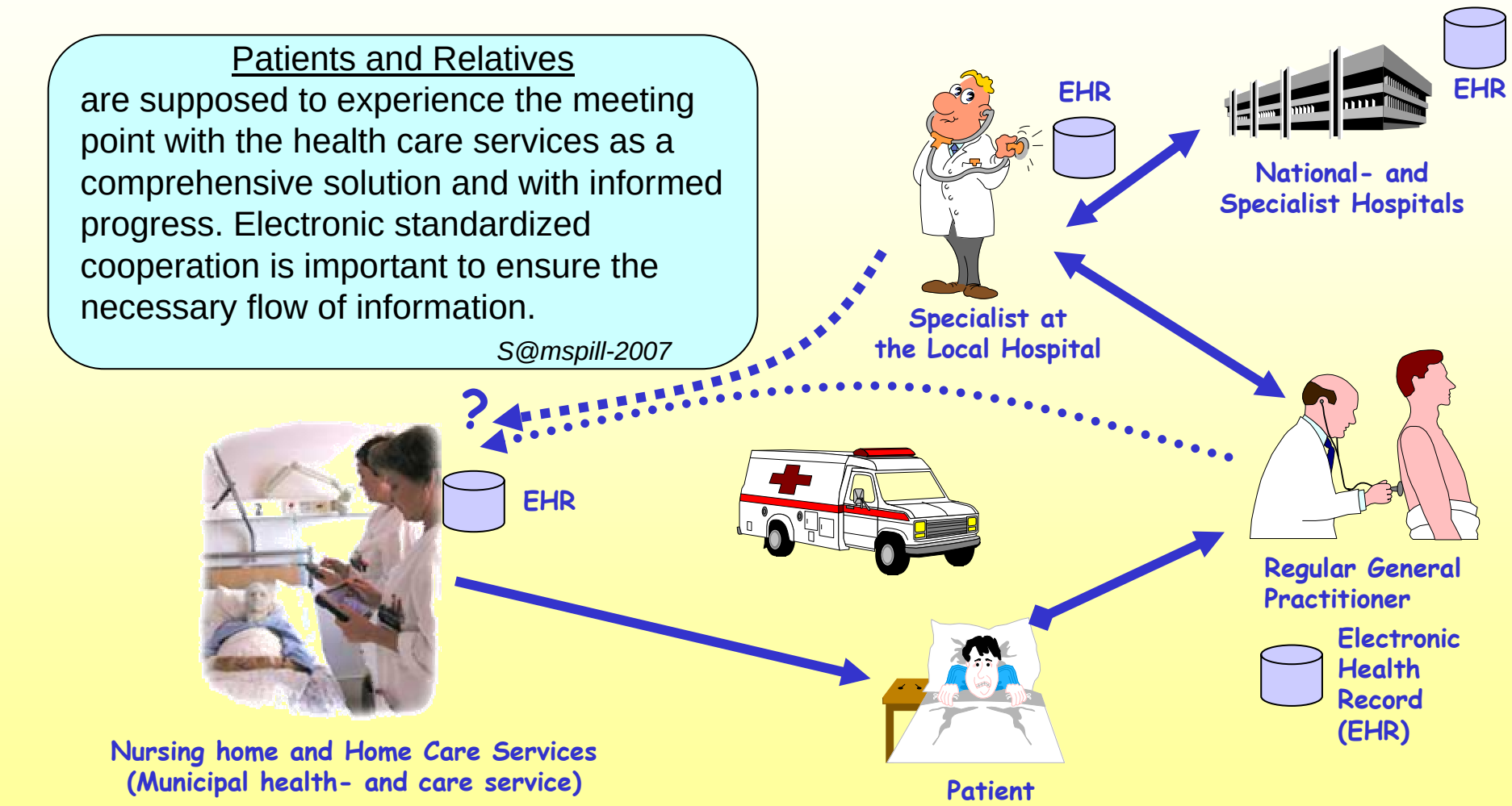
Security recommendations

- Norwegian Data Inspectorate have stated:
  - 2 different barriers to protect Health Networks against attacks from insecure networks (Internet and wireless communications)
  - Encryption using at lest 124 bit 3DES
  - A reference model illustrates needed security barriers
- It is supposed to achieve acceptable security architecture based on the technical solutions:
  - Digital ID with strong authentication using AAA-server
  - VPN – IPSec message integrity with secure encrypted tunnels
  - Authorization based on Role Based Access control and Workflow
  - Client/server protocols in order not to store EHR-info unsecured
  - The patient's sanction to get privileges for accessing the EHR

EHR-Interaction in health care sector

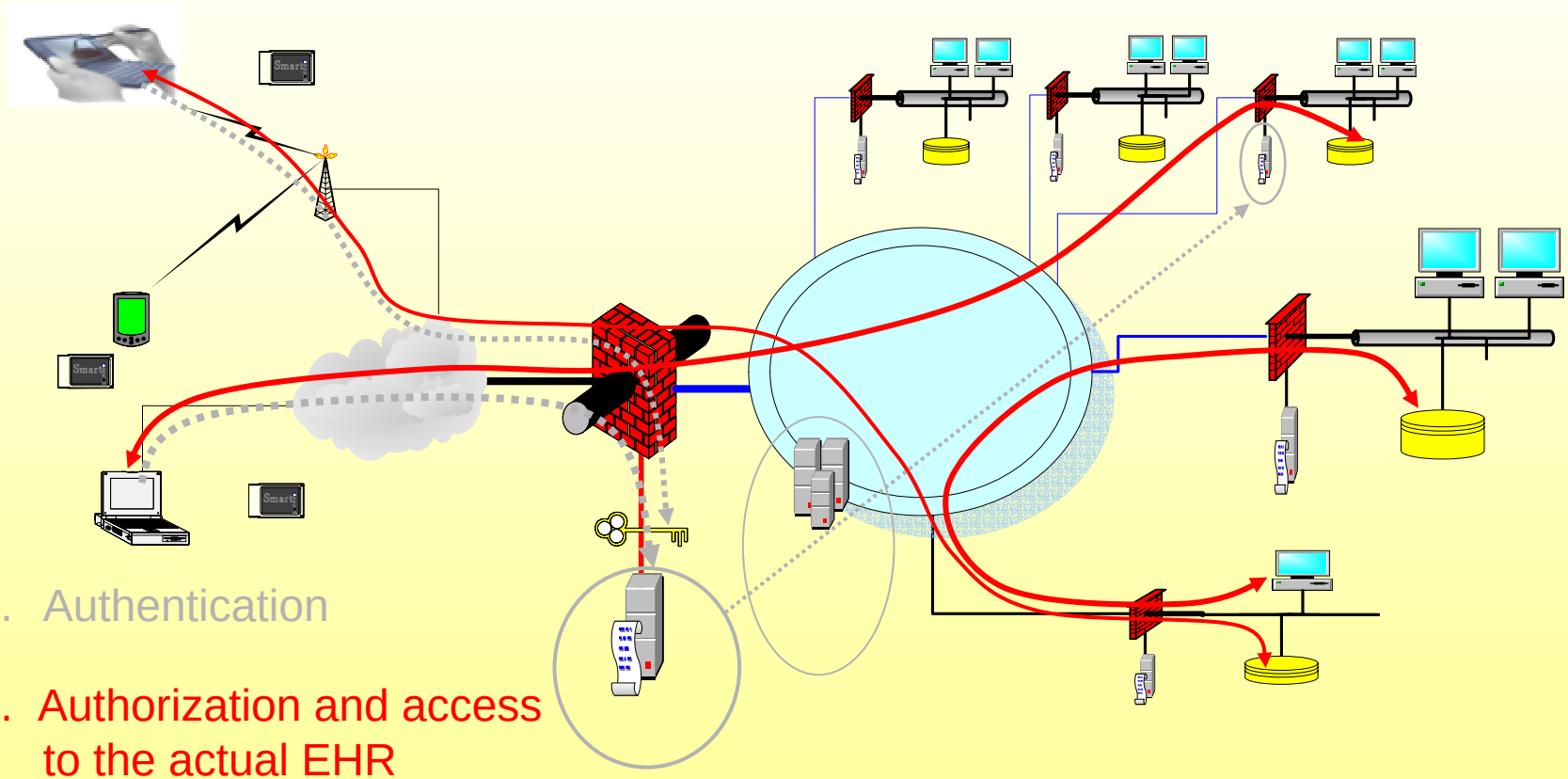
Patients and Relatives
are supposed to experience the meeting point with the health care services as a comprehensive solution and with informed progress. Electronic standardized cooperation is important to ensure the necessary flow of information.

S@mspill-2007



Integrated Portal for EHR-access

Based on Digital-ID, RBAC, Workflow management
with distributed LDAP-server Authentication



1. Authentication

2. Authorization and access to the actual EHR

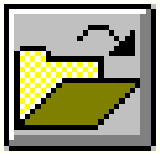
Patient Health Portal – Security Aspects

Use of Digital-ID with secure authentication & authorization

- Medical – gives flexibility and access to information
- Technical – possible to implement
- Administrative – difficult to update users and authorizations with unlimited users and EHR-systems
- Juridical – not clarified who is responsible for the EHR and the security actions needed with updating each access-list on the different LDAP catalogues

Conclusion:

- Impossible to adopt these ideas today



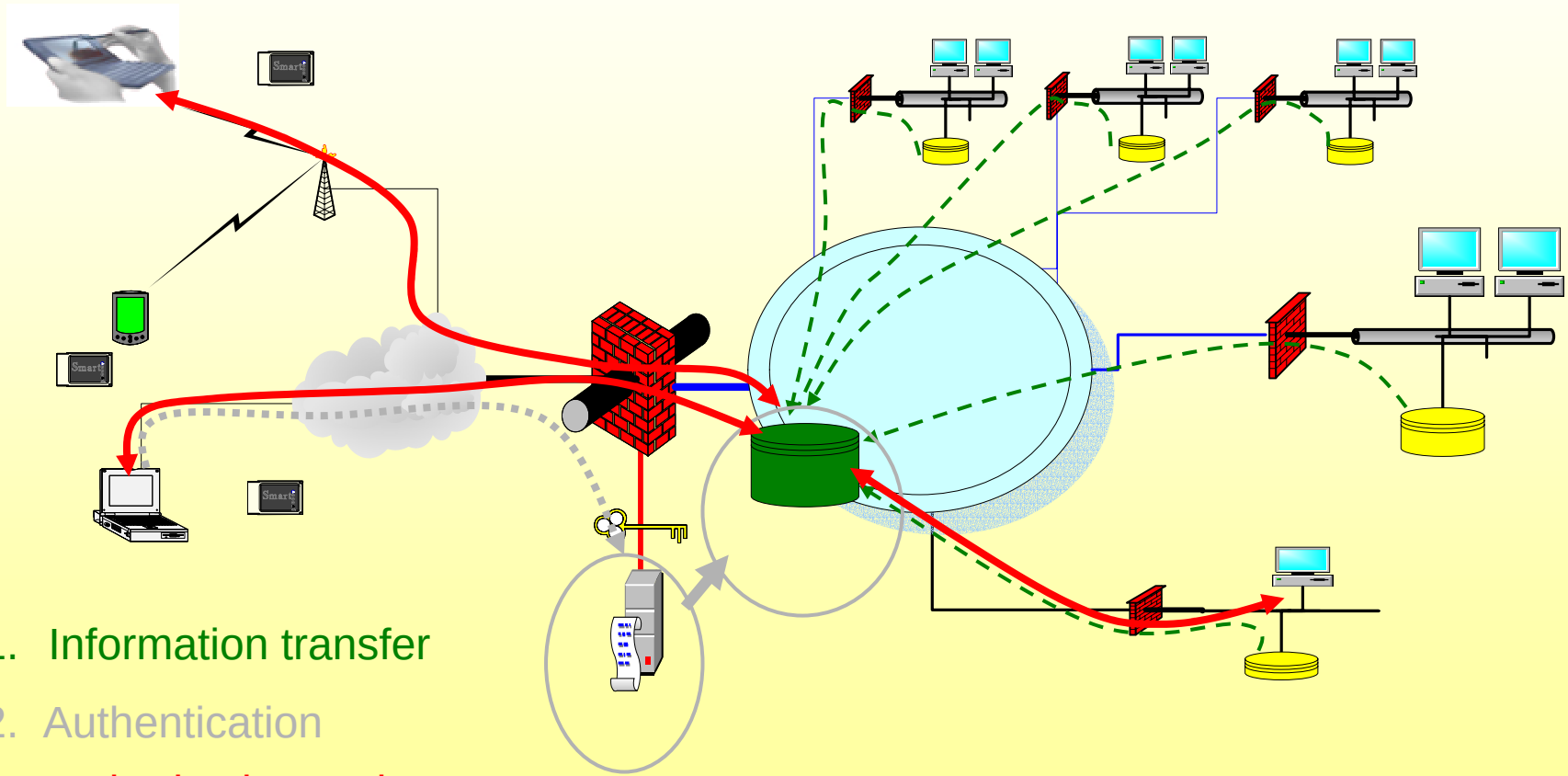
”PatientSite” (Helsemappe)

- On establishing a “PatientSite”, important information of the patient's health conditions are stored separately
- Patient – RGP(doctor) – Specialists – Home-care-services
  - Accessible from other hospitals in case of acute illness
  - Everyone have to pass over important information from local EHR
- Unclear juridical questions have to be clarified
- The patient is the proprietor of information stored in his EHR and he can decide **to whom** he gives privileges to access this information (sanctioned authorization)
  - Public health care services can establish this new service
  - A private company can establish this service (Trusted Third Party), where the patient have to pay a monthly fee

European Health-Card is established from 2007, contains important medical information

”PatientSite” with sentralized EHR-server

Based on a Personal Health Information Management System



1. Information transfer
2. Authentication
3. Authorization and access to the actual EHR

"PatientSite"– Security Aspects

Establish a centralized server with minimum common info

- Medical – poor flexibility with limited access to information
- Technical – possible to implement
- Administrative – regulations are needed for what kind of information to send from all EHR to the centralized server
- Juridical – unclear juridical questions have to be clarified with respect to how to administering users and access

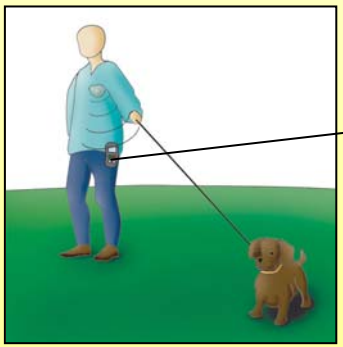
Conclusion:

- Possible to adopt today

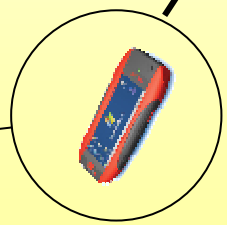
Freedom of mobility with supervised alarms

- Wireless monitoring gives the patients a better quality of life
- Automatic recording of ECG with an integrated alarm system
- Cardiac events are stored within the EHR in order to be followed-up

Security recommendations:
- Digital ID stored at the handheld
- VPN - IPSec encrypted tunnel
- Client/server protocols on TCP/IP



WPR wireless ECG-sensor



Hand-Held device for receiving the ECG-signals from the wireless sensor, with automatic arrhythmia detection

GPRS/ GSM

Base station for Mobile telephone

Wireless transfer of encountered alarm situations

Internet connected server with EHR

Remote Alarm Station at the hospital

Recommendations

- Recordings of biomedical signals using mobile phone/ PDA
  - Secure communications with Digital ID in the SIM card
  - Use of encrypted VPN tunnels for secure data transfer
- Access to the EHR from a stationary PC at home
  - Secure authentication using Digital ID
  - Encrypted communication using VPN tunnels based on IPSec
- Establish a solution based on a "PatientSite"
  - Contains recommended/desired information from different EHR´s
  - The patient can decide to whom is giving access to the information

It is a question who can deliver a "PatientSite" (Helsemappe) to an affordable price and quality