

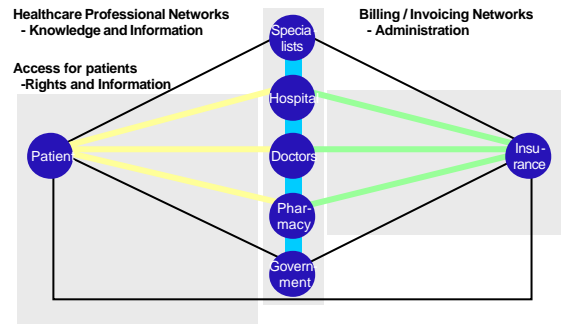
Security & Privacy in e-health care Networks

- _General Overview and actual Requirements
- _Regulatory Framework
- _Perspective and Goals
- _Challenges and Difficulties
- _Conclusions

General Overview

- _CHARACTERISTICS
- _small market of 7.5 Mio people (Bil 28 EUR)
- _high quality of health care system
- _high degree of social security
- _fragmented IT Structure with only few web-access based applications
- _fragmented interests between players along the path of medical treatment

The e-health care Network



Regulatory Framework

- _the patient is the owner of his medical record and data
- _the patient must allow any transaction and access to his record
- _no regulatory framework for the electronic signature applicable (2005)
- _strict regulatory framework for data protection is existing
- _no national / official CA existing or planned
- _regulation follows behind technological development

Requirements and Goals

- _patient empowerment by the use of a patient smart card with certificate (PKI)
- _guarantee privacy and identity (Confidentiality / Integrity / Authentication / Indisputability)
- _no data stored on the chip or in a centralized data base
- _security solutions are enabling the development of data networks
- _open networks, based on deployed client technology
- _independence of software solutions e.g. e-prescribing MD to Pharmacy

Challenges and Difficulties

- _nationwide technical solution without creating a centralized data base for medical records but an open network with adequate (legal) rules
- _get the acceptance and the thrust of citizens
- _re-financing by cost reduction
- _handling the logistic of a card enrollment with a face to face authentication

Conclusions

- _the technology is available
- _regulatory framework must follow
- _economical incentives will lead to changes in existing behavior of HCP and patients
- _privacy in health care is more than a technical issue, but a cultural one