International Telecommunication Union

Security needs in telemedicine

Philippe Feuerstein, MD
Centre Hospitalier de Mulhouse, France
feuersteinp@ch-mulhouse.fr

Workshop on Standardization in E-health
Geneva, 23-25 May 2003

ITU-T

Introduction

- New technologies widely improve the ability to electronically record, store, transfer and share medical data
- Sharing data by telemedicine is fast and cheap (at least, compared to classical methods)
- More and more participants are involved in this electronic data flow

E-health channels

- Physician/Physician
- Physician/Healthcare professionals
- Physician/Patient
- Physician/Government agencies
- Physician/Public health
- Physician/Law enforcement
- Physician/Insurance companies
- Physician/Registry office

ITU-T

Standardization

- When talking about standardization, hardware and software are taken into account
- Never underestimate the need of standardizing “manware”: if the different actors don’t have similar goals or expectations, nothing will have satisfactory results and security flaws will arise

Why security needs? (1)

- E-health must:
  - assure physical and logical data protection
  - preserve the use of data from obsolete technologies with a safe way to migrate from analog to numeric data
  - conform to legal and ethical rules: privacy, consent…

Why security needs? (2)

- E-health must:
  - protect health professionals whenever a medical case turns to a legal case
  - deal with the presence of third party: transfer operator, storage operator
  - protect copyright

Hardware Security

- Usual safety measures:
  - Hardware protection
  - Data backup
  - ...

Confidentiality (1)

- Keeping secure and secret information concerning an individual, guaranteeing his right to privacy
- Patient information is confidential and should not be disclosed without consent unless justified for lawful purposes

ITU-T

Confidentiality (2)

- Insurance companies obtaining medical information on policyholders could misuse it to deny coverage or claims
- Potential employers obtaining health information on current or potential employees could misuse it to fire or not employ a person
- Politician obtaining health information on opponents could misuse it for unfair attacks

ITU-T

Confidentiality (3)

- For most health professionals , confidentiality is an ethical duty
- In most countries, confidentiality is a legal obligation, but demanded level is variable:
  - Data Protection Act
  - European Data Protection Directive 95/46
  - Health Insurance Portability and Accountability Act

Confidentiality (4)

- Confidentiality can be obtained by use of cryptographic services
- In many countries, legal restrictions apply to cryptography materials
- Standardization challenge: to find a common algorithm, strong enough to be safe but law compliant in most if all countries

Authentication (1)

- For most documents, authenticity is bound to the presence of an authorized handwritten signature
- Even photocopies are worth nothing
- To find an equivalent of handwritten signature for a digital document is a difficult problem

Authentication (2)

- It is necessary to find a system, dealing with digital document, having these capabilities:
  - The receiver can verify that the issuer is really who he claims to be
  - The issuer cannot subsequently refute the document
  - The receiver, or any third party, cannot have made himself the document
  - A date stamp of the document creation is recorded

Authentication (3)

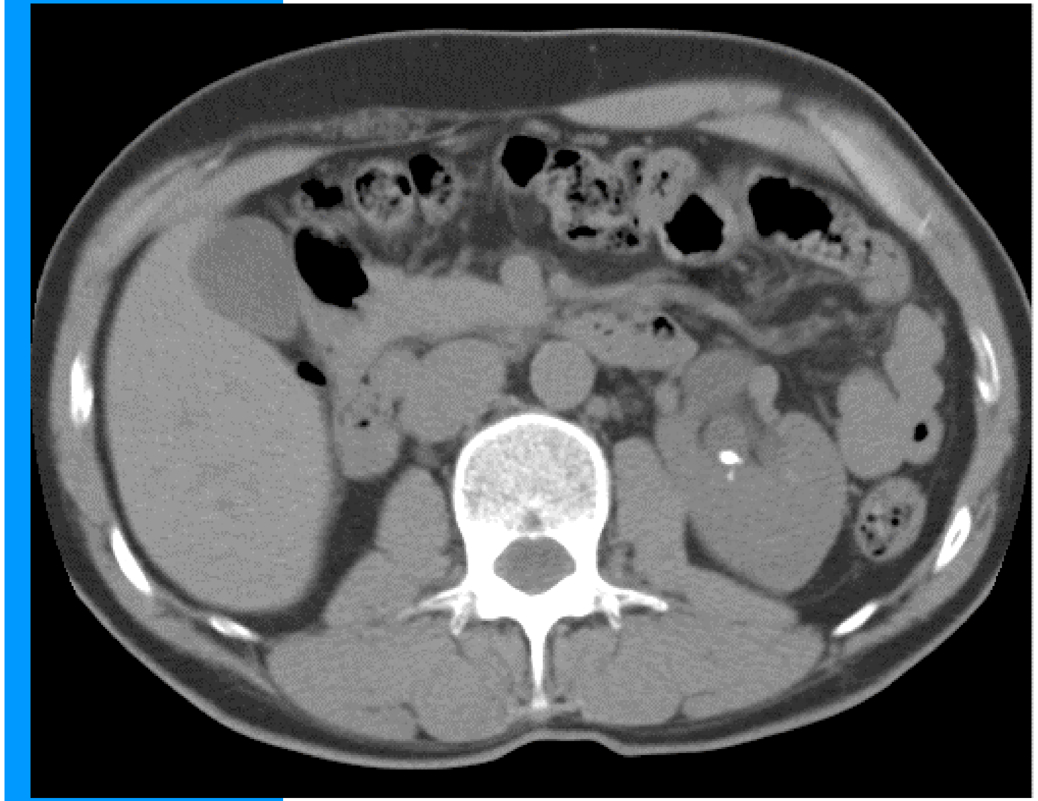
- Asymmetric public-key infrastructure (PKI) cryptography fulfills the needs
- Unfortunately, no PKI standard is universally recognized
- In more and more countries, the validity of digital signature is legally recognized if the system used meets defined criteria (e.g.: Electronic Signatures and Records Act)

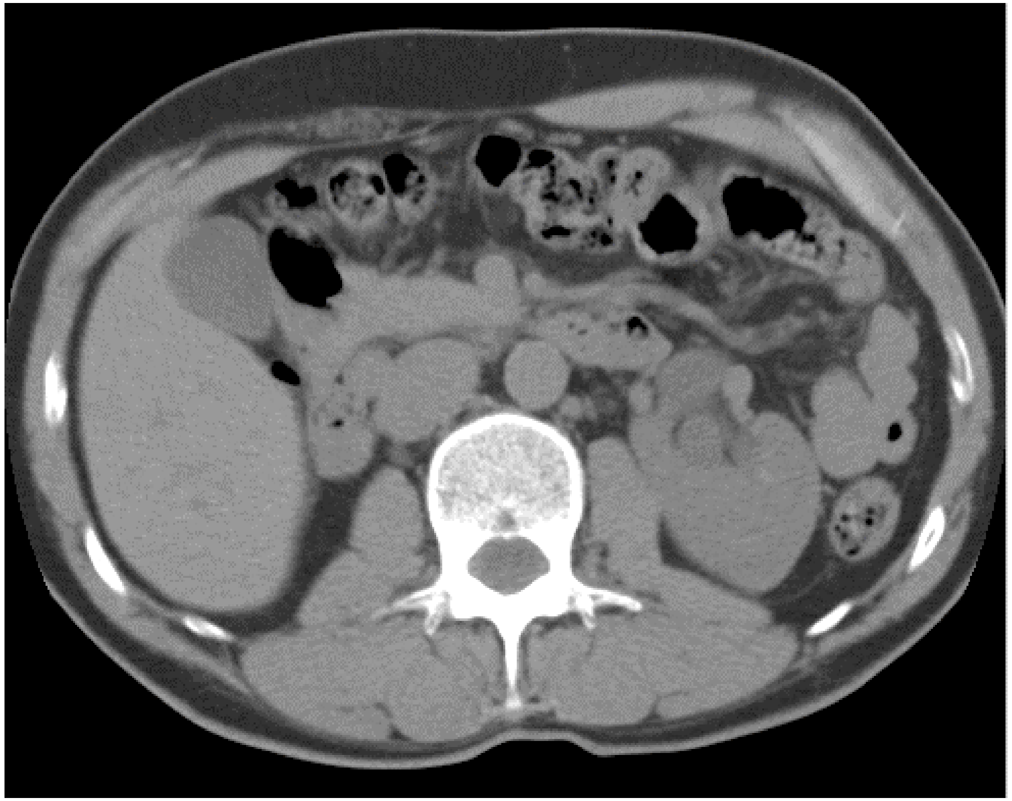
Integrity (1)

- During transfer or storage, data should not be modified voluntarily or accidentally
- Modification of conventional data are generally pretty obvious: erasing words in a letter, scratch on a plain film
- Situation is different with numerical data

Integrity (2)

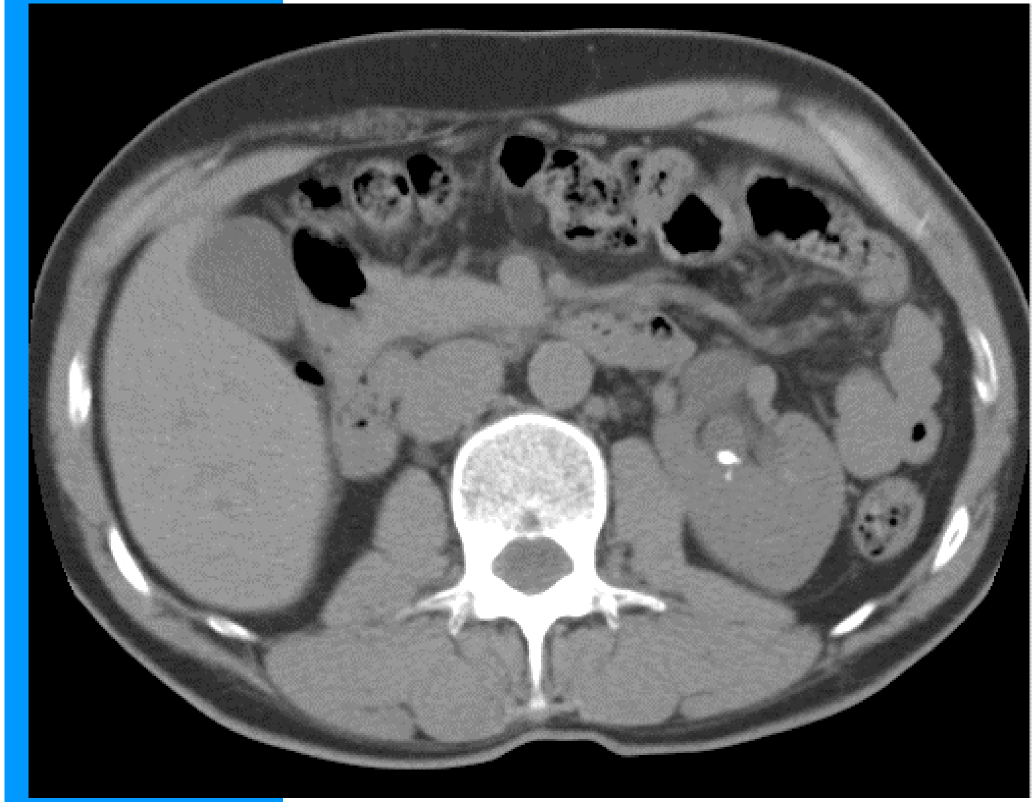
- Real kidney stone or graphical trick?

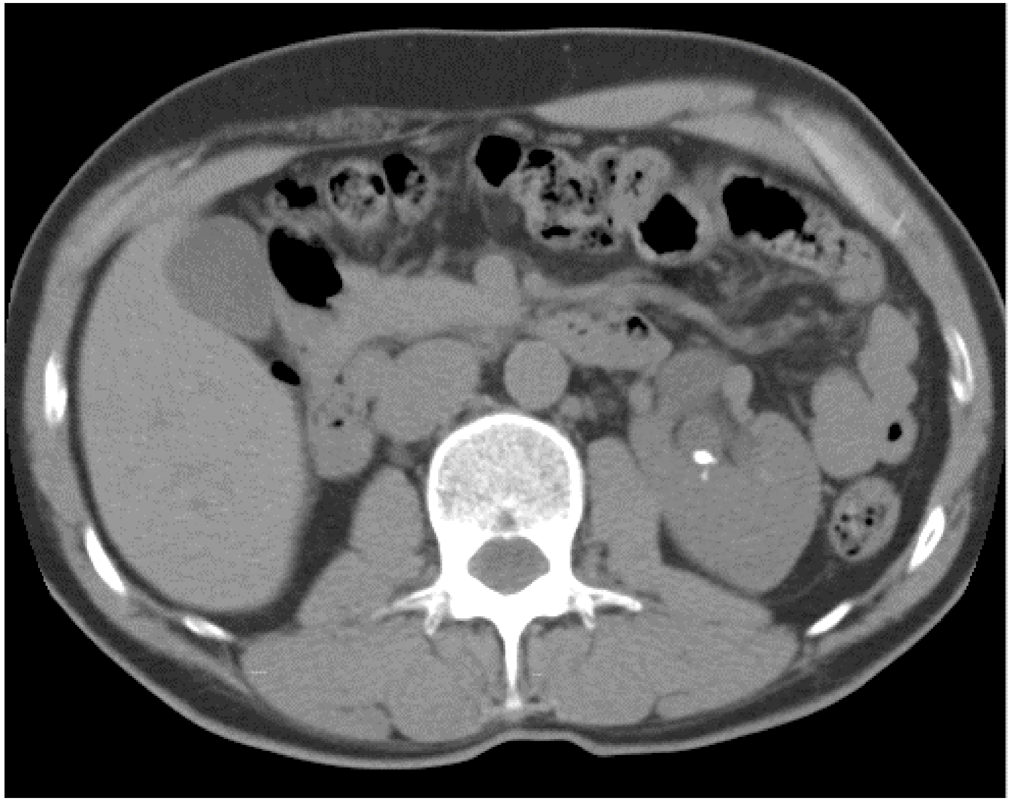




Integrity (3)

- Same document with 10% random noise





Integrity (4)

- Integrity can be compared to sending a postcard on which a plastic cover has been applied: everybody can read it, but nobody can modify it without leaving a visible mark
- Integrity of both data (misc. recording, imaging) and medical report is needed; ideally, they should be attached and inseparable

Availability

- Data must be accessible and usable upon demand by an authorised user, with an acceptable waiting time
- The time used include the whole cycle:
  - Data retrieving
  - Signature, encryption
  - Transfer
  - Decryption, integrity check

Auditability

- In the health multi-user environment, an authorized person may also access to information in situation when he is not concerned
- When transmitting, it is necessary to have a proof that sending, receiving and using data effectively occurred
- Timed chronology has also to be known

Anonymity

- Easily sharing data via telemedicine enable large scale multicentric studies
- Individual patient data are used for common benefit; privacy must be preserved and data anonymization is a basic rule
- A unique identifier is necessary but no standard exists on how to anonymize data

Copyright protection

- For educational or informational purpose, more and more data are available online
- It is often forgotten that something available online should not be systematically freely used by anyone
- Watermarking of document is a possible solution against « cyberplagiarism »

The ultimate security ?

- New technologies should be better than old ones
- In term of security, we wish a ”data auto destruction mechanism” in case of attempt of:
  - alteration (voluntary or accidentally)
  - theft
  - disclosure or any improper use

ITU-T

Conclusion

- Security issues are numerous and of primordial importance in telemedicine
- Circumventing them is one of the key point for the success of telemedicine
- Most of these issues can be addressed by cryptographic services and use of PKI
- Lack of standardization is a major drawback

Thank you for your attention!