PRINCIPLES OF DATA PROTECTION, SECURITY, PRIVACY, TRUST AND ETHICS FOR HEALTH DATA PROCESSING

PIRKKO NYKÄNEN

Professor emerita

Tampere University, Faculty of Information Technology and Communication Sciences

Pirkko.Nykanen@tuni.fi

FI-TZ eHealth workshop 16.6.2021

My background

- Senior researcher, VTT Medical Engineering Laboratory & VTT Information Technology 1975-2001, PhD on ‘Decision support systems from the health informatics perspective’
- Development manager in National Research and Development Center for Welfare and Health (STAKES/THL) 2002-2003, Health technology evaluation and assessment
- Professor in information systems science and health informatics in Tampere University 2003-2016, professor emerita 2017-
- Visiting researcher:
  - Universite de Lille, Centre for Medical Informatics, France, 1994
  - PennState University, School of Information Sciences, USA, 2000-2001,
  - Fudan University, Key Lab for HTA, PR China, 2007

SECURITY THEMES FOR WORKSHOPS

- **WS1: Principles of data protection, security, privacy, trust and ethics 16.6.2021**
- **WS2: Legal and regulatory frameworks for health data 4.8.2021**
- **WS3: Health care organisation - security and data protection management and control 1.9.2021**
- **WS4: Technological approaches for security and safety, threats and challenges 4.10.2021**

DATA PROTECTION

- Health-related personal data has to be protected for non-authorised access, use and disclose
- Data is sensitive and confidential
- Laws, normative rules and guidelines and standards define the framework

DATA SECURITY

- Hardware, software and communication networks have to be secured physically and technically and organisationally
- Risks need to be minimised, collection of means and actions for data security in normal and exceptional conditions

DATA SECURITY DIMENSIONS

- **Confidentiality**: data can be accessed only by those who have the right or permission / consent to access it
- **Integrity**: Data cannot be changed, corrupted, disappared, during input, processing, communication, storage
- **Authentication:** parties involved in data transfer, communication are those who they say they are
- **Non-repudiation: t**he party who sent the message cannot repudiate that he has not sent the data
- **Access control:** user access and user rights are restricted and controlled
- **Accessability:** data is accessible to those who have the right to access, disclose data (IETF, Internet Engineering Task Force)

CIA - Confidentiality, integrity, accessability

PHYSICAL DATA SECURITY

Control that no one can steal or destroy or do any harm to hardware, software, or any data storage and processing device or media or have non-authorised access to IT-premises

- No one can access the physical network and IT-premises without permission, copy/do harm for data or destroy the media
- Means, locks, access control, guarding, alarming systems
- All prints, storage devices and other materials have to saved/destroyed following the legal framework

TECHNICAL DATA SECURITY

- Éliminating all data security risks, or lackings in hardware or software
- User accounts, passwords, are means to control the users' access and rights on the data
  - Log-files to follow and monitor the access/use/disclose of data
- In open networks it is essential to secure that attacks from outside are prohibited
  - Firewalls, to isolate the local network; support for hybrid cloud environment
  - **Protection** from viruses, malware, cyber attacks, phishing etc with well-established security practises and security sw tools

ORGANISATIONAL DATA SECURITY

- Establishment of an security organisation and definition of rules, tasks and responsibilities for:
  - Security planning, security maintenance and follow up
  - Good practices for data processing and management
  - Means and systems to protect data and equipment, media and other facilities and premises,
  - Tools and resources for continuous security activities and monitoring of data management
    - Log –files and other activities to detect un-authorised access, security risks and potential attacks
    - Punishment system on data security violations

PRIVACY

Personal health information – confidential and sensitive, needs to be protected from un-authorised use, access and disclosure

PRIVACY

- Person's ability to control the collection, use and dissemination of one's personal information
- Persons, groups, institutions determine themselves WHEN, HOW and TO WHAT EXTENT information about them is communicated to others
- Privacy is personal and situation dependent concept

Privacy metrics - to assess the degree to which a particular application complies with privacy requirements

- no control, control over one kind of information, control over two kinds of information or three kinds
- Kinds of information: Contents, location, identity

THREATS FOR PRIVACY

- Multiple systems and authorities can collect, process, and share personal information and there can be autonomous and hidden information processing
- Rich contextual metadata is often collected and used, violating the Data Subject's privacy interests
- It is difficult (or even impossible) to destroy data stored in the information space, e.g. in social media services
- The business objectives, needs, interests, and policies of various stakeholders may be unknown for Data Subject
- It is not possible to know in advance the characteristics, rules, and regulations of secondary users in situation where secondary use is allowed
- Systems using ubiquitous computing have no mechanism for people to reflect their intentions, and informed consent is not possible in ubiquitous environments with a large amount of sensors
- **Without proper privacy controls health information systems may not reach their full potential!!!**

HOW TO MANAGE PRIVACY IN PRACTISE

- Privacy preferences can be implemented with **context-aware privacy policies**
- **Policies are computational rules explicitly stating privacy preferences on how information can be processed, used, (re-used), disclosed and shared**

1. Trust information which is a value of a system or environment specific calculation of regulatory compliance and trustworthiness
2. Sensitivity of the data
3. Situation of the information use
4. Purpose of the data collection or use

- **Policy formulation is a decision process** where an individual selects privacy rules and services and how much information can be traded when compared to offered service and the level of privacy attributes

HOW TO ACHIEVE GOOD PRIVACY STATUS

- Person, DS - data subject, has to be aware and have means to control
- Integration of regulated and non-regulated domains >>>Need to develop privacy services for non-regulated environments
  - To monitor and control privacy attributes
- Privacy management should be trust-information based, dynamic and be able to adapt to context information
- Privacy management architecture means management of data privacy by choosing personal context-aware privacy policies and supporting computational trust
- Privacy-by-design approach

TRUST INFORMATION

How much a person can trust on a system, how system's policy and technical architecture look like, and to what extent system's policies are compliant with domain-specific regulations and laws

- Trust information on systems' **measurable or observed attributes**
  - Individual (or a system) can predict system's willingness or ability to process one's personal health information legally and following the defined personal preferences
  - Attributes can be calculated from information the system has, or should have, published; however, some attributes may require direct observations

TRUST

- **Trust** is typically based on characteristics such as ability, integrity, and benevolence and should not be a blind guess
  - Benevolence is defined as the extent to which the trustor believes that the trustee is willing to do good things instead of harmful things/maximising profits
  - Integrity concerns honesty and sincerity
- Can be expressed either by value, rating, ranking or as probability or belief
- Trust attributes proposed include trustee's identifier, certificate, ability, predictability, trustee's privacy policy, legal requirements, and system's properties such as transparency, authenticity, confidentiality, and non-repudiation
- Several mathematical methods have been developed to measure the degree of belief, recommended trust or computational trust value

ETHICAL ISSUES

- Ethical issues of information technology and digital society refer to the society's opinions on the use of computers and the development of information systems and digital technologies, and the expected impacts of these technologies
- An important ethical principle for eHealth systems and applications is
  - **Personal health-related data should be protected with reasonable security safeguards against such risks as loss, un-authorized access, destruction, use, modification or disclosure of data**

Security, data protection, privacy, trust and ethics – important issues in eHealth

- Sensitive health related data, anonymisation, de/re-identification, consent management
- Reuse of data / Secondary use of personal health data - scientific, commercial
- Biobanks, biological samples + genetic data/profiles – donors' sovereignty and protection of privacy of the very sensitive data
- Data lakes/pools – collections of patient data from different organizational systems – integrated security solutions and privacy policies?
- CIA - Confidentiality, Integrity, Availability /Accessability - Trust building, privacy management and protection, privacy-by-design
- Legal frameworks in EU and Member States, GDPR – General Data Protection Regulation, 2018; National laws and regulations, Standards

Thank you for your attention!
Pirkko.Nykanen@tuni.fi

REFERENCE MATERIAL

- Van Deursen et al, **Monitoring information security risks within health care,** Computers & Security 37, 2013, 31-45
- N. M. Shrestha, A. Alsadoon, P. W. C. Prasad, L. Hourany and A. Elchouemi, **Enhanced e-health framework for security and privacy in healthcare system**, *2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC)*, 2016, 75-79,
- Jigna J. Hathaliya, Sudeep Tanwar, **An exhaustive survey on security and privacy issues in Healthcare 4.0**, Computer Communications, 153, 2020, 311-335,
- Juhee Kwon & M. Eric Johnson, **Health-Care Security Strategies for Data Protection and Regulatory Compliance**, Journal of Management Information Systems, 30:2, 2013, 41-66
- Karim Abouelmehdi, Abderrahim Beni-Hssane, Hayat Khaloufi, Mostafa Saadi, **Big data security and privacy in healthcare: A Review,** Procedia Computer Science, 113, 2017, 73-80,

•Wright D**, A framework for the ethical impact assessment of information technology**. Ethics Inf Technol 2011, 13:199–226

•A Seppälä, P Nykänen, P Ruotsalainen, **Privacy-related context information for ubiquitous health.** JMIR Mhealth Uhealth 2014 ; 2(1), e12.

•P Ruotsalainen, B Blobel, A Seppälä, P Nykänen, **Trust Enabled Privacy Management Architecture for Pervasive Health.** Journal of Medical Internet Research, 2013, 1(2), e23

EXERCISE

- Analyse at general level whether data protection and security issues are well-managed in Tanzania. If not, where you see/find problems or lackings?
- How are the patient privacy issues taken care in Tanzania? How important you see these issues?
- Do you think that health care professionals can trust on health information systems used in Tanzania? What bout citizens – do they have, or do they need to have trust on information technologies and systems?