

IMPORTANCE 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 10.11.2021

DATA PROTECTION

- Health-related personal data has to be protected for non-authorized access, use and disclosure
- 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, disappeared, during input, processing, communication, storage
- **Authentication**: parties involved in data transfer, communication are those who they say they are
- **Non-repudiation**: the 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
- **Accessibility**: data is accessible to those who have the right to access, disclose data (IETF, Internet Engineering Task Force)

CIA - Confidentiality, integrity, accessibility

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-authorized 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 be 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-authorized 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-authorized 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

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

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

EU – GDPR: GENERAL DATA PROTECTION REGULATION, effective from May 2018

- **Purpose - Harmonize privacy and data protection laws across Europe**
 - **to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business**
 - GDPR was driven by the concern that individuals' personal information was being exploited in ways that undermined privacy and, by extension, democracy
- **Digital economy should operate with the informed consent of users and clear rules for companies who seek to do business in the European Union**
- <https://gdpr.eu/what-is-gdpr/>

GDPR applies to you even when you're not in the EU

- *1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*
- *2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
 - *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
 - *(b) the monitoring of their behaviour as far as their behaviour takes place within the Union*
- *3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law*

Thank you for your attention!

Pirkko.Nykanen@tuni.fi