Drag and drop task, Moodle H5P

Data protection terminology

Privacy and data protection are basic rights secured in *Finnish and international legislation*, which set the basis and boundaries for legal data processing. Processing the personal data always requires *lawful basis*. Basic principles in personal data processing include for example *data minimization*, purpose limitation, transparency and securing integrity and *confidentiality* of the data. *General data protection regulation* (GDPR, 2018) is the main regulation concerning processing of the personal data in European Union. It applies to both private and *public* section by setting *the rights and obligations* for processing patient and other personal data. Data protection applies to data throughout its whole life cycle from *recording* to *erasing*.

Personal data means any information relating to a person who can be recognized with *direct* identifiers (e.g. full name) or *indirect* identifiers (e.g. age, physiological, cultural, etc. factors). *Pseudonymization* refers to protection of personal data by removing direct identifiers of the data. If all additional information is erased and no other information is available, after a careful evaluation that information may be considered *anonymous*.

Any structured set of personal data (e.g. patient record) is considered as a *filing* system. Data *controller* (e.g. a health care unit) determines the purposes why and the means how the personal data should be processed. The controller has the obligation to ensure that *processing of personal data* is legal. Technical supervision for ensuring security include e.g. logging data processors and *processing events*.

Data protection in health care

Data protection is important in health care because of the *concealed* nature of patient information and the frequent and *large-scale* processing of the data. Patient data refers to all information about the patient's *health and other personal data*. Only relevant information to patient's care, such as information about health, illness, or treatment, *examination results*, and medicine and allergy information, is allowed to be recorded into *patient record*.

Patient data can be processed only with a specific right which has an obligation to maintain *professional secrecy*. In order to provide proper and safe medical care without compromising patient privacy, patient data has to be secured from those not involved in patient care or care-related tasks (=*outsiders*) but it has to be *accessible* to those with the rights to process the data. Employees at health care unit are bound by *confidentiality*. It is also important to understand that *access* to patient information does not create right to process the data – *purposes and means* determined by the controller have to fulfill. Third party members are authorized to process the data if they have *a contract* with the health care unit and *a written consent* secures confidentiality.

Health care unit can share patient data leaning on two basis: with *legal basis* (either on right or obligation to disclose the data) data can be shared to e.g. insurance companies, *authorities* or scientific research. With *patient's consent* data can be shared e.g. to other health care units and *biobank*.