The Danish Debate on Research using Health Data and Biological Material

Key values, challenges and ways forward as seen by the Danish Council of Ethics

Danish Research Infrastructure

Databases:

- Medical records
- The National Health Databases
- Research databases
- Secondary data from previous and ongoing studies
- Databases with data from clinical trials

Biobanks:

- PKU Biobank
- The Patobank (pathology data bank)
- Capital Region Biobank
- SSI's diagnostic samples
- Danish Cancer Biobank

Note:

- All Danes have a SSN allowing for linkage across databases and biobanks

Legal regulation

Legal definitions and requirements:

- Anonymous data, i.e. a person cannot be identified, is not protected by law.
- Non-sensitive personal information such as name, age, gender, SSN etc. can be used for scientific research if *necessary* and if the use is in the *interest of society*.
- Sensitive personal information such as health information can be used for scientific research if consent is provided or if the data is *necessary* and of *significant value to society*.
- A biobank is considered a manual database with personal and sensitive information.

Protective 'bodies':

- Handling of personal and sensitive information in relation to research – public or private – must be approved by the **Danish Data Protection Agency**.
- Acces to medical records must be approved the **National Board of Health** (Ministry).
- Research on biological material must be approved by a **Research Ethics Committee**.

Utility and Solidarity

Protects/speaks for:

- Extensive collection of data with the purpose of improving therapy.
- Citizens making their health data available for research purposes.

Challenges:

- In general there are limits to the violations of principles of privacy and autonomy we will accept in order to postpone death and generate better health/quality of life.
- Individual or organizational failure to embody solidarity in the exchange of health data.
- Commercialization of data generated in a public (private?) health care system.

Recommendations:

- Promoting a research culture with deeply rooted respect for privacy and autonomy.
- Require open sharing of data and results of research on data between citizens, researchers, institutions and companies.
- Avoid commercialization of data (not commercial exploitation of data).

Privacy and Confidentiality

Protects:

- Against negative emotional reactions (fear), stigmatization and discrimination.
- Against social pressure from groups/State to conform to others' norms of healthy living.
- Confidentiality promotes trust in health care professionals.

Challenges:

- More data is collected, stored and exchanged between systems. Very little is destroyed.
- More health professionals get access to data, and the data is used for more purposes.
- Anonymisation is increasingly difficult and IT-security turns out to be flawed.

Recommendations:

- Right to correct/withdraw data. Anonymisation > Pseudonomisation. Encryption of data.
- Restricting number of people with access. Data only used for purpose. Proportionality.
- Continous monitoring of data protection by authorities. Harder sanctions?

Trust

Protects:

- Trust is a quality of human relations that we value in itself.
- Trust is a precondition of sharing information, and therefore in turn for adequate therapy.

Challenges:

- Disappointment of expectations concerning quality of therapy and patient protection:
  - Scandals of all sorts in the health care system, and in particular scandals involving loss or illegal collection of sensitive health data.
- Lack of transparency concerning use of personal and sensitive health information.

Recommendations:

- Transparency concerning …:
  - Who has access to data (which groups of health care professionals?)
  - For what purposes (therapy, research, quality-assurance?)
  - Under what conditions (anonymised, time-span, level of security?)
  - Unauthorised access, loss or misuse of data (who, for what, when?)

Autonomy and Informed Consent

Protects:

- An individual against suffering physical harm.
- An individual's ability to form and pursue his or her own goals and plans.
- An individual's ability to define a sphere of privacy.

Challenges:

- Routinisation of consent.
- Practical problems associated with obtaining informed consent.
- Consent bias.

Recommendations:

- Development and use of IT-platforms for obtaining consent.
- New models of consent: Specific, broad, open, presumed and meta consent.

Thank you!

Meta consent

Meta Consent		Form							
Content		**Dynamic**		**Broad**		**Blanket**		**Refusal**	
EPR									
Tissue									
Health Databases									
Linkage to non-health data									
Context		**Dynamic**		**Broad**		**Blanket**		**Refusal**	
Private	Public								
Commmercial	Non-commercial								
National	International								