Privacy in the e-Health and Welfare Services

NTNU Dept. of Information Security and Communication Technology

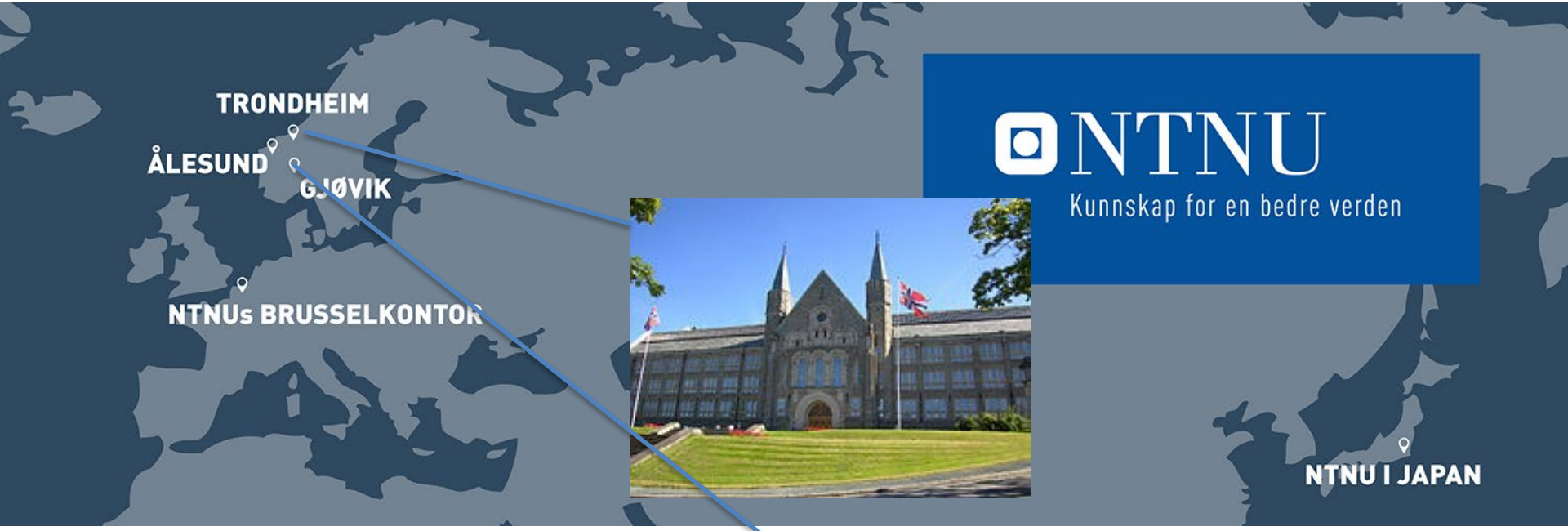
Bian Yang, eHWS, 04 February 2022

Agenda

- About NTNU and eHWS
- Privacy models and paradox
  - privacy definitions and models
  - privacy paradox
- Privacy in e-health and welfare services
  - health data privacy
  - privacy protection
  - real-life examples

About NTNU and eHWS

Norwegian University of Science and Technology (NTNU)

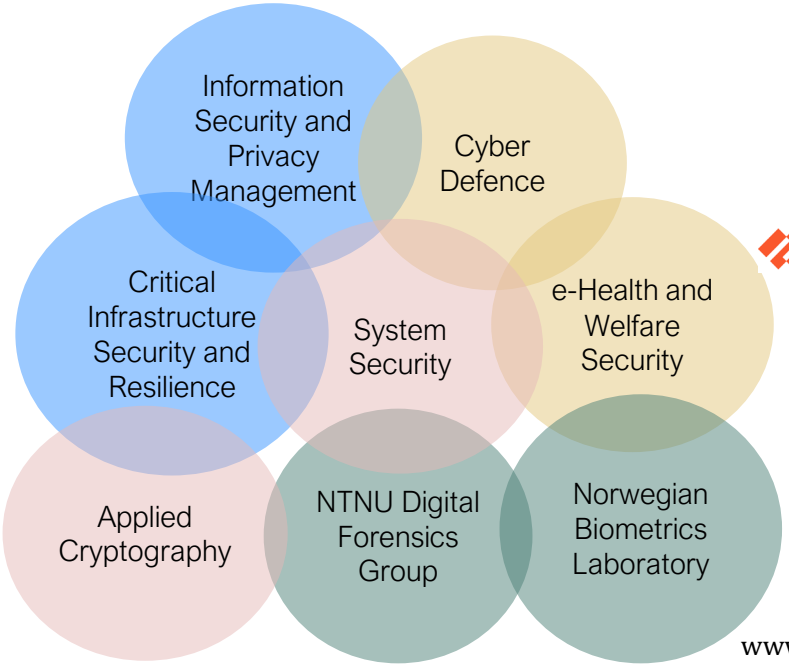


- Trondheim
- Ålesund
- Gjøvik

NTNU CCIS

Center for Cyber and Information Security

Our research groups



Our partners

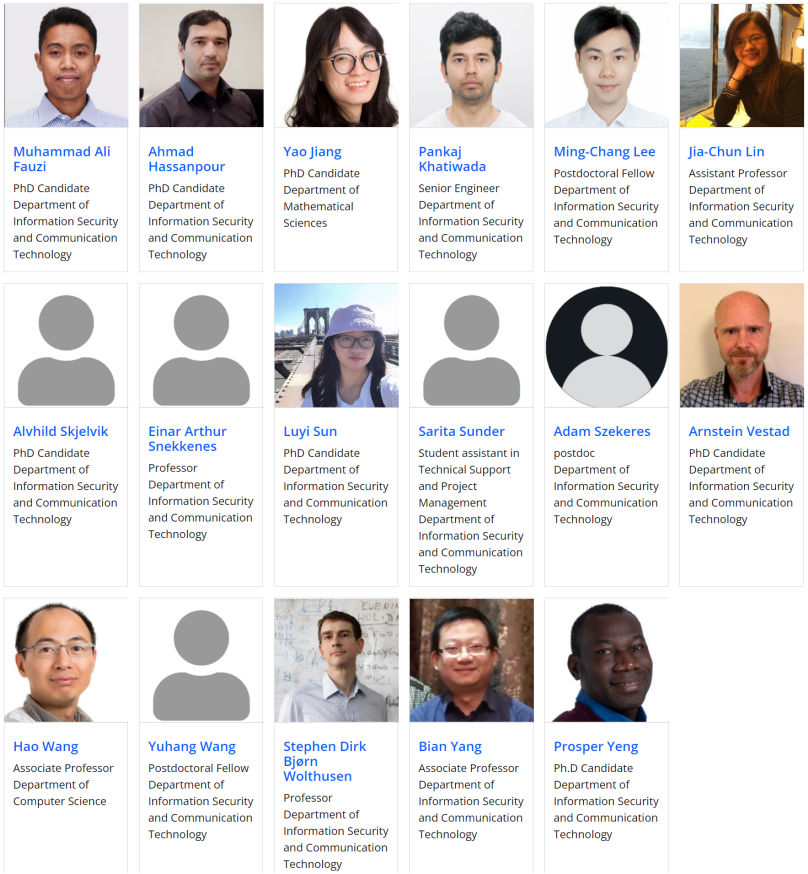
NC-SPECTRUM

buypass, cisco, Government of Iceland, Ministry of Transport and Local Government, IBM, KRIPOS, sopra steria, tieto EVRY, bouvet, KiNS, Datatilsynet, Digdir, Statkraft, Cyberforsvaret, NorSIS, paloalto NETWORKS, ATEA, telenor, WATCHCOM, A COMBITECH COMPANY, NORMA CYBER, KLUGE, mnemonic, Securing your business., KPMG, FFI, POLITIET, OSLO POLITIDISTRIKT, accenture, pwc, Statnett, Sykehuset Innlandet HF, ØKOKRIM, THALES, Nasjonalt ID-senter, NASJONAL SIKKERHETSMYNDIGHET, POLITIET, Capgemini, Innlandet fylkeskommune, Eidsiva, PST, POLITIHØGSKOLEN, DNV, Skatteetaten, HØGSKOLEN i INNLANDET, Forsvarets høgskole, NORGES DOMSTOLER, Cyberingeniørskolen

www.ccis.no

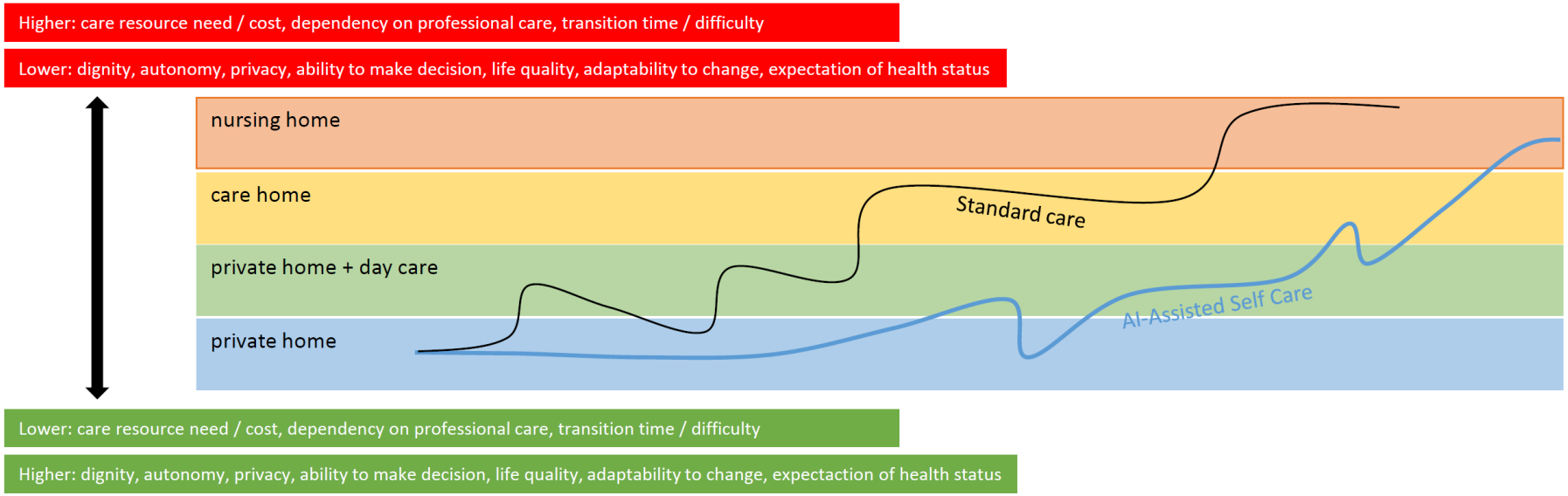
The eHealth and Welfare Security Research Initiative at CCIS / NTNU

- https://www.ntnu.edu/iik/ehws#/view/about
- Established eHWS June 2016
- Strategic funding from Helse- og omsorgsdepartementet, national “mandate”
- Project collaboration with Direktoratet for e-helse, Norsk Helsenett, Sykehuset Innlandet, Oslo universitetssykehus, Senter for Omsorgsforskning (NTNU)
- Core member: 5 permanent staff, 4 PostDoc, 7 PhD, 1 engineer, 13 adjunct members + 17 external advisors



Privacy Definitions

A little about care trajectory we envision in next decades …



Objectives:

1. Longer and healthier stay at lower levels of the care staircase
2. Lower time and difficulty in transitions between care staircase levels
3. Better management of patient's expectation and thus higher controllability along the care trajectory
4. Smoother transformation of roles of patients and their next of kin along the care trajectory

Essence of Privacy

Two essential elements underlying the concept of Privacy, particularly in the healthcare context

- Autonomy
  - Within a **private zone («personal space» in Altman book)** of personal and social activities, a person can think, decide, and behave on his/her own
- Human dignity
  - Respect from others on one's own body, thinking, relationship, belonging, and personal acitvities
    - self-determined control the **output** from the private zone
  - Respect from others to be let alone and free from unwanted disturbance
    - self-determined control the **input** to the private zone

Approaches to Defining Privacy

- The effort to define privacy: **What should privacy be?**
- **Descriptive approach**: to characterize and define privacy using features as best as we can
  - E.g., Gavison (1980) «Privacy and the Limits of Law»
  - Pros: laying down a relatively stable concept to cover core values
  - Cons: not flexible to map to different and dynamic practical cases
- **Normative approach**: to define privacy in a way to adapt the concept to social norms, personal values, and varied contexts
  - Altman (1975) «The environment and social behavior: privacy, personal space, territory, crowding»: a dialectic and dynamic process of constantly negotiating personal boundaries and territories inside social systems. (a concept of managing relationships)
  - Solove (2008) «Understanding privacy»: control over personal information towards others
  - Nissenbaum (2004) «Privacy as contextual integrity»: privacy attitude and decision are context-based.
  - Pros: flexible to capture the contextual factors in real-life scenario
  - Cons: complex to make judgement; too flexible to minimise the risk brought to individuals

Approaches to Defining Privacy

- The normative approach is currently a dominant approach to defining and characterise the concept of privacy.
- However, be careful with its flexibility which could bring unexpected risk to data subjects

e.g., Jensen (2005) «Privacy practices of Internet users: self-reports versus observed behavior»: individuals tend to exhibit overconfidence in their skills and knowledge in privacy setting configuration.

Brandimarte (2013) «Misplaced confidences privacy and the control paradox»: users given with more control tend to reveal more personal information

Reasonable Expectation

M.Taylor and J.Wilson (2019) Reasonable Expectations of Privacy and Disclosure of Health Data.

- Implied consent (e.g., usually for direct care)
  - Convenient, no negotiation room
  - Most patient respecting professionals and authority blindly (e.g., Milgram experiment, 1960s)
- Informed and active consent (e.g., for clinical trial / research)
  - high cost in operation and risk of **not real** consent
- The challenge: fuzzy boundary of direct care and other purposes when new care tech and services emerge:
  - genomic medicine
  - Healthy life style promotion (e.g., sensor + App)
  - Health digital twin
- The solution …
  - the principle of No Surprise ?

Reasonable Expectation

M.Taylor and J.Wilson (2019) Reasonable Expectations of Privacy and Disclosure of Health Data.

- How is resonable expectation determined?
  - Is NOT a personal expectation!
  - Three perspectives:
    - receiver (e.g., a clinician),
    - 3rd party (e.g., a reader of newspaper), and
    - a reasonable person in a position of the data subject.
  - Context: attributes of the claimant, the nature of the activity, the place of the activity, the nature of the purpose, the absence of the consent and whether it is known (or can be inferred) by the data subject, the effect on the data subject, etc.
  - Triviality: whether it is considered to be private but trivial (e.g., a visible sickness of the public figure)
  - Internal vs external approach: the underlying values (dignity and autonomy) vs public interest / special needs

Reasonable Expectation

M.Taylor and J.Wilson (2019) Reasonable Expectations of Privacy and Disclosure of Health Data.

- For further research
  - What quality of notification is sufficient
  - How is acceptance to be judged
  - How to balance the three perspectives, and other factors
  - How to check the consistency of the consents given from the same subjects (changes in individual and group expectation)
  - How to evaluate the performance in shaping good practice of data sharing

Social license

P.Carter, G.Laurie, and M. Woods. (2015) "The social license for research: why care.data ran into trouble".

- Care.data: extracting identifiable primary care data to a centralized register by NHS in 2014, stopped due to public concern in privacy, and finally abandoned in 2016. Another version was proposed in 2021 but paused again due to public concern.
- Fact:
  - Social licese (Hughes (1958)): social license to operate as the expectations of society regarding the conduct and activties that og beyond the requirements from regulations. E.g., mining industry needs to earn a social license and maintain it, by behaving in a trustworhty and responsible way. (AI is facing the similar challenge?)
  - Social license goes "beyond the compliance".
  - The cara.data was compliant to the Health and Social Care Act 2012
- The lessons
  - Insufficient communciation and discussion in general public
  - Concern in equal distribution of the benefit from the secondary use
  - No clear idea how the researchers can be held to account.

Social license

P.Carter, G.Laurie, and M. Woods. (2015) "The social license for research: why care.data ran into trouble".

- The principles to follow to get a social license
  - Reciprocity in both communication (involving the data subject in discussion and decision) and benefit (if possible prioritise the data subjects in health benefit)
  - Non-exploitation in terms of informed consent and patient empowerment (risk snd benefit are evenly distributed among the patients and users)
  - Service of the public good

Personal Privacy Model

Luyi Sun (2022) "Privacy Predictive Models for Homecare Patient Sensing" (Springer)

- Machine learning model for personal privacy preferences
- Demographic Information

Gender, Age, Income, Education Background, Religion

- Step 1: An explorative approach - Focus Group
- Step 2: A scenario-based questionnaire method
- Step 3: ML based mapping between scenarios and preferences
- Step 4: in-situ questionnaire / observational studis
- For
  - Automated privacy setting for new devices and services
  - Curation of personal preference history for future digital twin

Privacy Models

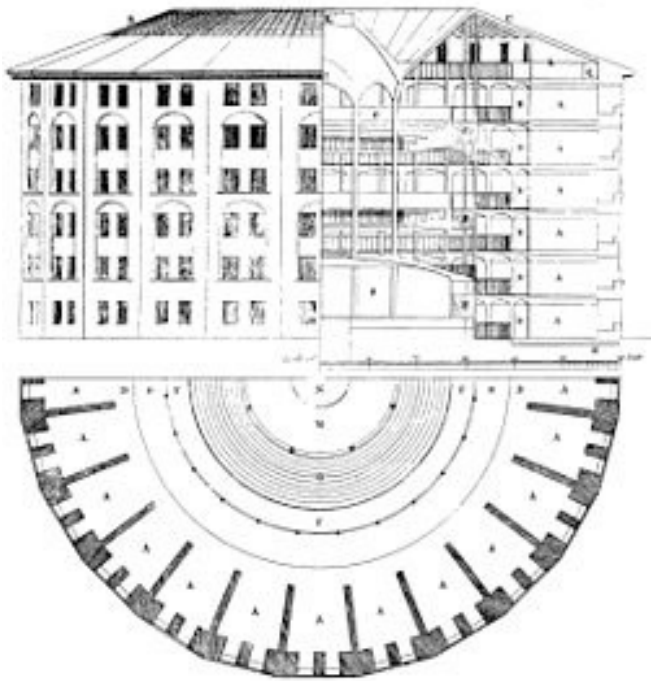
Models of Privacy

- The effort to model privacy: **What does privacy look like?**
- **Model** is an **abstract knowledge** people follow and use as a tool to understand an unfamiliar concept
- It's about a way chosen to understanding a concept.
- (Oetzel and Gonja, 2011) Theory of Social Representation: an individual person understand new concepts based on established conceptual schemes, through the processes of **objectification** and **anchoring**.
  - "What is 'Lykke'?" "That is a weekend spent in cabin with coffee and a novel…" "Ah, I see." -> objectification
  - "What is WeChat?" "It is a Chinese version of Facebook + Messenger + Vipps." "Ah, I see." -> anchoring

Models of Privacy

Mai (2016) «Three models of privacy»

- **The Panopticon model** (Jeremy Bentham, 18th century)
- "Surveillance model": one-way watching, little communciation among the watched



https://en.wikipedia.org/wiki/Panopticon

USA. Illinois. 2002. Stateville Prison. F house.
https://prisonphotography.org/tag/doug-dubois/

Models of Privacy

Mai (2016) «Three models of privacy»

- **The capture model:** personal information and activities collected, structured, and stored without clear purposes.

  It looks like a model fitting the situation of 1980-2010 while computer and communication technologies penetrate the society with personal data scattered

- **The datafication model**: anonymous creation of new personal data, statistical inference, AI, big data, etc. Looks like 2010-now.

The challenge everyone is facing: how the conventional privacy approaches (descriptive and normative) can sustain the datafication model, e.g., how an average citizen can make optimal decisions to control his/her personal data

Privacy Paradox
- How People Perceive and Behave

Privacy Paradox

Brown (2001) “Studying the Internet Experience”

“ *This uncovered something of a "privacy paradox" between users complaints regarding privacy and their use of supermarket loyalty cards.* ”

Acquisti (2003) “Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior”

“ *Surveys report that most individuals are concerned about the security of their personal information and are willing to act to protect it. Experiments reveal that very few individuals actually take any action to protect their personal information, even when doing so involves limited costs.* ”

The dichotomy of **information privacy attitude** and actual behavior has been coined the term “**privacy paradox**” (Brown, 2001; Norberg et al., 2007)

Theories to Explain

Kokolakis (2015) “Privacy attitude and privacy behavior: a review of current research on the privacy paradox phenomenon”

- **Privacy calculus theory**: individuals perform a calculus between the expected loss of privacy and the potential gain of disclosure. Their final behaviour is determined by the outcome of the privacy trade-off.
  - “*Would you use the service B instead of A if B does not track your browsing activities? But B cost 7 USD more than A monthly*.”
- **Social theory**: People who in order to maintain their social lives must disclose information on them despite their privacy concerns, e.g., social collective individuals are willing to provide information and data about themselves as this is an implicit part of being a member of the community
  - “*I have to show up in the Facebook group. That’s my everyday social life! And so far I am okay (not attacked or not aware of any cyberattack).*”

Theories to Explain

- **Cognitive biases and heuristics in decision-making**: e.g.,

Optimism bias*(*the consistent tendency of individuals to believe that they are less at risk of experiencing a negative event compared to others*), "So many people doing this … it cannot be me!"*

Overconfidence(individuals tend to exhibit overconfidence in their skills and knowledge) "I share my data in this way successfully for many years …"

Benefit immediacy (if a person sees the benefit can be immediate by disclosing personal information, he tends to perceive the risk is lower.).

Theories to Explain

- **Decision-making under bounded rationality and information asymmetry conditions**: Most people are lacking the cognitive ability to calculate privacy risks and disclosure benefits and do not have access to all necessary information in order to make informed judgments.
- **Quantum theory homomorphism**: Flender and Müller (2012) engage concepts from quantum theory to provide an understanding for the privacy paradox. This new perspective allows incorporating effects like indeterminacy, i.e. the **outcome of a decision making process is determined at the time the decision is made but not prior to it**, ...

Potential Methods to Address the Paradox

Two dimensions to examine the paradox

1. cross-people: compare one's attitude and behaviour with another one's, e.g., *will a person who shows stronger intent to protect her privacy actually behave better in privacy practice*?

2. cross-time: compare the same person's attitude and behaviour at different times, e.g., *will a person behave in better privacy practice when she expresses stronger intent*?

Privacy in health data

Health Data Privacy

What are health data?

- Personal data = health data?

- Health data:
- Direct care
  - Lab test
  - Medical records
  - Prescription
  - Insurance
- Public health & health research
  - Clinical trial
  - Health register
- Patient-generated health data
- Others
  - Environment
  - Life, economic, behaviour and social -> physical and digital footprints

Health Data Privacy

Concerns on health data privacy (Ethics and governance of artificial intelligence for health: WHO guidance, 2021)

- Discrimination based on health data
- Dignity if sensitive data are disclosed to others or public
- Prone to cyber attack and ransomeware
- Rights of children, which could include future discrimination based on the data accumulated about a child
- “behavioural data surplus”, which is health data collected by technology providers, exceeding what is required and that such excess data
- Re-identification of “anonymised data”
- Loss of autonomy and control over their data for future profit and benefit

Health Data Privacy Protection

How to protect?

- Consent, explicit and specific consent
- Shared decision making: patients should be involved in the important decision making process what, when, and how their health data are to be processed
- De-identification (anonymization)
- Pseudonymisation
  - very hard for highly distinguishable biometrics such as genome sequences, or public figures, or personalised care which is built on rich and thus linkable data
- Trust relation
  - Traditonal between the doctor and patient but now have AI a role in possibly different opinions, which could negatively impact on patient's trust on their GP or a specific care professional from hospital or LTCF. This impact on trust may impact on privacy relation too. (Kumli er at. BMC Health Services Research (2020))

Health Data Privacy Protection

- Privaxcy literacy: learning from stories via friends, family, and media (Rader et al. Stories as informal lessons about security, SOUPS 2012)
- Community of Practice e.g., at a patient association (e.g., obervation->participation->in-situ practice on their own, D. Hung, Preserving Authenticity in CoLs and CoPs: proposing an aenda for CSCL, CSCL 2005.)
- Treat others as one would like others to treat oneself (Oosterveld-Vlug et al. Nursing home staff's view on residents' dignity: a qualitative interview study. BMC Health Services Research 2013
- Technical approach
  - Transformation (statistics, feature selection, etc.)
  - HME
  - MPC
  - DP
  - FL
  - Autoencoder / GAN
  - Proxy ReEncryption / Updatable encryption

Real Life Example – Smittestopp

Norwegian contact tracing App released (1st version) in April 2020.

- Built for contact tracing -> as expected
- Types of data collected/stored: GPS position (lat/long), time, altitude, speed, and all tied to personal identifier.
- GPS? -> possibly expected but not favored
- Public health research? –> not expected
- July 2020: Norwegian Data Protection Authority (NDPA) order all data collection and processing from Smittestopp to stop
- 21.12.2020: New version of Smittestopp is launched as a new app under the same name

-> Reasonable expectation, trasparency

Real Life Example – Trace Together

In early 2021, the Singapore Government admitted that data collected from its COVID19 contact-tracing App (Trace Together) could also be accessed “for the purpose of criminal investigation”, despite prior assurances that this would not be permitted.

-> Expectation can be … not ensured at all.

Real Life Example – Face mask

Privacy can be contextual and compliant to social norm, but social norm can be … changed!

- Year 2020 March (conversation of two my colleagues at NTNU campus in Gjøvik):
  - A: "why do you wear mask?"
  - B: "The virus can be air-born…"
  - A: "You make me not feeling well … you should go home!"
- Year 2021 fall: naked-face visitors to supermarket likely to receive stares from others…

-> social norm can change completely in one year

Real Life Example – Unvaccined

Privacy can be contextual and compliant to social norm, but social norm can be … changed!

- (fall 2021) One clinician from the inland hospital in Norway told journalist that those unvaccined should accept lower priority in treatment if hospitalised …
- now by the Green certificate, your COVID-related status (recovered, vaccined, test negative) will be known by many people than your GP and local clinicians

-> People are re-thinking of equality, privacy, autonomy, and dignity … those underlying values which before we thought so obvious.

Real Life Example – Health Digital Twin

- Omniscent dataset about a person's life and health

It can reduce the cost and human resource needs but increase the surveillance coverage of time and space about the patients.

https://www.iotforall.com/what-is-digital-twin-technology

Real Life Example – Home robot

Hole-and-corner applications (Pierce 2019, CHI2019; Lupton, 2020, The Inetrnet of Things: Social Dimensions)

Example: a home robot experienced by my colleague's parents:

- Camera and mic are good for the elderly to keep the social life …
- It also opens a channel for unnoticed surveillance …

Real Life Example – Health Monitoring System

(Anita Woll, 2017) "Use of Welfare Technology in Elderly Care«z

Digital privacy:

- One patient regularly turning off and unplugging the TV camera during a phase they are assumed to be working
- One patient thought the camera was always on and thus asked to replay some day's recording to find out where her money was placed
- One patient dressed well each time before she went to the kitchen thinking all activities there were video-taped

(Hargreaves et al 2018) "Learning to live in a smart home"

Users are afraid of advanced setting (privacy and security setting eg) ands want to stick to simple (but working) settings of technology

-> technology and privacy literacy

Real Life Example – Health Monitoring System

(Anita Woll, 2017) «Use of Welfare Technology in Elderly Care»

Physical privacy:

- Patients require the visitors show humility and respect when entering their private homes.
- Avoid the feeling of being monitored (e.g., hiding the sensor in flowers, installing a curtain before the camera lens)

-> need of life quality

Real Life Example – Trade off

(Anita Woll, 2017) «Use of Welfare Technology in Elderly Care»

- An old patient asked the care giver to let her door open so that she could hear people talking in the corridor – a feeling of safety.

(Luyi Sun, 2021) «Your Privacy Preference Matters: A Qualitative Study Envisioned for Homecare»

- a couple of old patients thought they don't care about the camera installed in their home but more care about their financial control and physical safety and caemra could bring more safety feeling

-> prvacy may be traded off with patients' actual need in a context

Thank You

Bian Yang, Assoc. Prof., Dr.
NTNU-IIK, CCIS-eHWS
Bian.Yang@ntnu.no