Zorg voor Privacy!

Grand Round, RadboudUMC

Bart Jacobs — Radboud University
bart@cs.ru.nl
18 sept. 2017

Outline

Where we are, so far

Own involvement in e-health

- Invited at expert meetings in Parliament (Senate) in 2009-2011 on Electronic Health Records "EPD"
  - rejected unanimously in April 2011, mainly for privacy concerns
- Since 2015 involved in **Parkinson op Maat** study, with Bas Bloem
  - joint project of RadboudUMC with Verily — life science branch of Alphabet/Google
  - our role: supplier of privacy-friendly "PEP" technology for managing research data — funded by Province of Gelderland
- Member of RadboudUMC's privacy advice board
- Active with non-profit foundation

  `https://privacybydesign.foundation`

  in **identity management**, also in the medical sector
  - the foundation issues BIG attributes — soon also AGB codes

EPD-security & privacy was/is hotly debated topic

(from: Kidsweek, feb. 2009)

Privacy is keeping information in context (Helen Nissenbaum)

- We naturally live in different contexts
  - home, work, sports club, in church, with friends ...
- We naturally want to keep information in context
  - what we tell to our doctor should not end up in a supermarket
- People get upset when contextual integrity is broken
  - recall anger: about selling customer financial data (ING), about speeding data ending up at the police (TomTom), about school children's performances in online tests ending up at publishers
- When explained like this, almost everybody cares about privacy
- The Google's and Facebook's of this world make us use the same identifier everywhere or track us via Like and cookies
  - they break-up contexts, and destroy our basic privacy intuitions
  - Mark Zuckerberg: "Having two identities for yourself is a lack of integrity" ☹☹☹

Where we are, so far

Specific law: WGBO

- WGBO = *wet op de geneeskundige behandelingsovereenkomst*
- It regulates interactions and obligations between patients and medical professionals, eg.
  - professionals must inform their patients (eg. about risks), and ask for informed consent before treatments
  - patients must provide correct and complete information
- Medical professionals must maintain a dossier about each patient
  - confidentiality and integrity of the dossier are required: medical information must remain in medical context!
  - patients have access rights to their dossier
- Nowadays, dossiers are no longer maintained personally
  - organised collectively in a hospital
  - outsourced to specific companies (Epic, HIS-providers, ...)
- What about medical apps? Who gets the data? In context? Legal?

Who owns medical data?

- Fundamental but difficult question!
- Situation in NL:
  - No-one !?!
  - medical professional is responsible
  - patient has rights

About medical professionals (based on own experience)

- **What they know well**
  - patient privacy one-on-one
  - that they should not talk about individual patients at parties etc.
- **Where they are ignorant and/or naive**
  - structural, analytical aspects of privacy and information security
  - strategic importance of data and data flows
  - sensitivity to this problem: "we are the good guys, so what?"
  - the wider picture — because of strong operational focus, a bit like with police officers

In teaching these matters receive no attention — as far as I know

- also, medical privacy & information security & the wider (societal) implications, are not academic topics within medical faculties

(REshape'rs are "believers" and uncritical technology-pushers)

Where we are, so far

Broad perspective

Follow the data!

- Traditionally, you should "follow the money" in order to understand power relations in society.

From: All president's men (1976)

- Nowadays you need to follow the data

There are many laws and rules to regulate and monitor financial flows.
Regulation of data flows is still in its infancy

Protecting people, possibly even against themselves

- In most civilised countries it is forbidden to sell your own organs
  - in legal terms, in Dutch: *organen zijn buiten de handel geplaatst*
- Why? This is so patronising!
  - In order to protect (poor) people against such definitive options
- Maybe it should also be forbidden to sell your own medical data

All big IT-firms are expanding into the medical world

Why?

- Profit margin are highest for medical devices/services
- Sick people don't wine about privacy and consent to any data transfer
- Medical data are extremely valuable
  - for commercial purposes, like targeted advertisements
  - for assessing (financial) risks — e.g. for mortgages
  - for own medical research and patents
  - for selling them (back) to hospitals, and to pharmaceuticals

Medical sector is often so naive about contextual integrity

- London's *Royal Free* hospital transferring medical data of 1.6M patients to Google's DeepMind for testing a kidney app
- Patients were unaware, no consent was asked
- "inappropriate legal basis" according to UK's national data guardian

"Googlisation of healthcare"

- Big-IT is compiling large health datasets, via apps and (free) services
  - they are the new proprietors, gatekeepers, mediators of the data
  - they can store and analyse health data in huge quantities
- Confusingly, they use public repertoire, fraiming their activities as only for the "public good"
  - they appeal to research participant's altruism and good will
- Which hospitals/universities will get access to these private datasets?
  - only the rich ones? Or the famous ones?
  - or the ones that promise to contribute with more data?
  - who is running the show, setting agenda's, with which goals?
- Fundamentally different relation than with pharmaceutical companies
  - pharmaceuticals are active only in one domain
  - big-IT is active in many: advertising, shopping, communication ...
  - they deliberately connect all these domains — breaking contexts

(See also: Tamar Sharon, 10.2217/pme-2016-0057)

People and their tools

Big question

To what extend should technology **help** and/or **force** medical professionals to keep data in context?

- Big-IT's tools aim at frictionless sharing — with big-IT!
  - E.g. **Whatsapp** is frequently used for medical communication
  - Where do pictures end up? In the iCloud / Google cloud / ...
  - Apps are for data collection, at odds with doctor's *dossierplicht*
- Alternatives are needed, but missing / cumbersome / expensive
  - Who uses secure mail systematically?
- Security technology slows you down, e.g. in authentication
  - lack of compartimentalisation of dossiers looks insane to me
- It's a shared responsability between management and professionals to introduce and use proper security technology; GDPR will require it

Medical IT-security & privacy must professionalise!

- **For external reasons**
  - Tough European data protection (GDPR) will be in force soon
  - e.g. more transparancy & explicit consent will be required (e.g. for PALGA and other such databanks, certainly commercially)
  - privacy impact assessments (PIA) needed for new technology
- **For internal reasons**
  (1) To keep patients' trust, for using their data in medical research
    - professionally pseudonymise and encrypt data
    - like with PEP technology, used for *Parkinson op Maat*
  (2) To keep healthcare under public control and counter big-IT
    - your professional independence is at stake!

Where we are, so far

iCIS | Digital Security
Radboud University

Main points

- The essence of privacy protection is keeping data in context
- Learn to think in terms of data and data flows
  - medical data is extremely valuable; don't give it away
  - stay in control of your data, e.g. via tough contracts
- Make medical security & privacy part of the curriculum and research agenda
  - it's a strategic matter; don't try to avoid/delegate it
  - you need to professionalise, to stay on top of developments
- Closer interdisciplinary cooperation with security/privacy specialists is needed — a non-trivial effort
  - but also a broader societal/political debate
- Consider making "data care" part of the hospital's public profile

Thanks for your attention!

iCIS | Digital Security
Radboud University