Data Liberation and eHealth: a double-edged sword

Guido van 't Noordende
Informatics Institute
University of Amsterdam
noordende <at> uva.nl

Document Freedom Day, European Parliament,
Brussels, March 27, 2013
Ehealth outlook – EU policy

Quote Estonian president T.H. Ilves, chair EU eHealth Task Force, May 2012:

“We know that in healthcare we lag at least 10 years behind virtually every other area in the implementation of IT solutions. We know from a wide range of other services that information technology applications can radically revolutionise and improve the way we do things.”

We should quickly catch up, then.
Think before you act

Privacy by design

Urgency?
Hippocratic Oath

Medical confidentiality.

“All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal”

~400 BC
Maybe, medical privacy is not so obsolete.

- HHS study, VS, 2001: 8% patient avoids care in (early stages) of disease for fear of privacy breaches or stigma

- 2005 National Consumer Health Privacy Survey (Canada)

“One out of eight consumers has put their health at risk by engaging in such behaviors as: avoiding their regular doctor, asking their doctor to fudge a diagnosis, paying for a test because they didn’t want to submit a claim, or avoiding a test altogether. Chronically ill, younger, and racial and ethnic minority respondents are more likely than average to practice one or more of these risky behaviors.”
Medical data – paths to disclosure

- Personal health records
- Professional Health information Exchange systems
- "Anonymous" research data
“Anonymized” (open) research data

Well, anonymous..
### Table 3. Number of Dutch citizens per anonymity set size, for various quasi-identifiers

<table>
<thead>
<tr>
<th>Quasi-identifier:</th>
<th>$k = 1$</th>
<th>$k \leq 5$</th>
<th>$k \leq 10$</th>
<th>$k \leq 50$</th>
<th>$k \leq 100$</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC4</td>
<td>0</td>
<td>9</td>
<td>19</td>
<td>345</td>
<td>996</td>
</tr>
<tr>
<td>PC6</td>
<td>429</td>
<td>6,109</td>
<td>25,103</td>
<td>1,459,939</td>
<td>2,354,255</td>
</tr>
<tr>
<td>PC4+DoB</td>
<td>1,861,081</td>
<td>2,754,465</td>
<td>2,765,932</td>
<td>2,774,476</td>
<td>-</td>
</tr>
<tr>
<td>PC6+DoB</td>
<td>2,744,653</td>
<td>2,774,476</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>PC4+gender</td>
<td>4</td>
<td>27</td>
<td>103</td>
<td>889</td>
<td>2,555</td>
</tr>
<tr>
<td>PC6+gender</td>
<td>1,854</td>
<td>31,262</td>
<td>184,803</td>
<td>2,342,242</td>
<td>2,629,017</td>
</tr>
<tr>
<td>gender+YoB</td>
<td>5</td>
<td>14</td>
<td>53</td>
<td>250</td>
<td>516</td>
</tr>
<tr>
<td>gender+YoB+MoB</td>
<td>55</td>
<td>356</td>
<td>712</td>
<td>4,478</td>
<td>9,674</td>
</tr>
<tr>
<td>gender+YoB+MoB+PC4</td>
<td>137,035</td>
<td>279,100</td>
<td>2,196,950</td>
<td>2,774,476</td>
<td>-</td>
</tr>
<tr>
<td>gender+YoB+MoB+muniparity</td>
<td>2,186</td>
<td>22,565</td>
<td>59,597</td>
<td>244,152</td>
<td>619,671</td>
</tr>
<tr>
<td>gender+DoB</td>
<td>2,014</td>
<td>14,506</td>
<td>40,322</td>
<td>1,392,622</td>
<td>2,725,472</td>
</tr>
<tr>
<td>gender+DoB+PC4</td>
<td>2,240,461</td>
<td>2,765,067</td>
<td>2,772,205</td>
<td>2,774,476</td>
<td>-</td>
</tr>
<tr>
<td>gender+DoB+PC6</td>
<td>2,758,578</td>
<td>2,774,476</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>town+gender</td>
<td>4</td>
<td>4</td>
<td>28</td>
<td>372</td>
<td>896</td>
</tr>
<tr>
<td>town+YoB</td>
<td>499</td>
<td>3,172</td>
<td>7,225</td>
<td>50,985</td>
<td>103,145</td>
</tr>
<tr>
<td>town+YoB+MoB</td>
<td>10,083</td>
<td>61,073</td>
<td>112,850</td>
<td>287,173</td>
<td>394,844</td>
</tr>
<tr>
<td>town+DoB</td>
<td>185,042</td>
<td>596,769</td>
<td>1,045,559</td>
<td>2,730,668</td>
<td>2,750,700</td>
</tr>
<tr>
<td>town+YoB+gender</td>
<td>1,153</td>
<td>7,195</td>
<td>16,333</td>
<td>102,018</td>
<td>150,135</td>
</tr>
<tr>
<td>town+YoB+MoB+gender</td>
<td>22,260</td>
<td>109,126</td>
<td>170,351</td>
<td>398,601</td>
<td>826,744</td>
</tr>
<tr>
<td>town+DoB+gender</td>
<td>288,409</td>
<td>1,029,601</td>
<td>1,813,559</td>
<td>2,750,669</td>
<td>2,764,050</td>
</tr>
</tbody>
</table>

---

$^a$ $QID_A$, see section 3.2.

$^b$ $QID_B$, see section 3.3.

---

PC4 + Date of birth + gender: 80,8% uniquely identifiable

Figuur: M. Koot et al., HotPETs, 2010 [Latanya Sweeney 2002, MASS. US]
Medical data – paths to disclosure

GP

HealthVault

Personal health records

Professional Health information Exchange systems

"Anonymous" research data
The traditional route: push

Physician (or pharmacist) act as a **dossier keeper**
- Physician keeps data under lock and key, and is responsible for quality of the record
- Discretionary decision to exchange information (e.g., “push” communication)
Professional Health Information Exchange - Pull

Plenty of attempts since '90/'00s, some successful some not.
- Usually some (closed source, single ownership) centralized system
- Scale tied to organizational boundaries (NL? EU?) and ownership
- Scale of disclosure / authorization not tied to patients
- Notable examples: U.K. NPfIT, Dutch EPD, ...
- Lock-in, government / policy push, monopolies,...
- Most pull-based Health Information Exchange systems scream security and privacy risks.
Pull example: Dutch electronic patient record system

National Switching Point: Central reference index (VWI) contains pointers to decentrally stored medical data. Centralized access control before forwarding requests. Access control based on physician-owned smartcards with PIN code.
Security – some issues.

Central access control. Implementation: CSC (US-based company)

- GP
- Pharmacist
- hospital

[Diagram showing relationships between GP, Pharmacist, hospital, and a central access control (CSC) system]
Security – some issues.

N = ?

[.........]
Scale, security and usability do not combine well. Add “ring of access”: ask permission (opt-in)!

10,000 -> 400,000 smartcards       .....       N = 1,000 -> 50,000 computers / PC's
A case for open standards?

**Yes:** simpler, open communication mechanisms
- Lock-in less likely
- Feature creep less likely
- Possibly less centralization: more open ownership / management of systems (if less costly)

Don't re-invent the wheel
- Learn from existing systems' *security* solutions; many standards exist, (e.g., PKIs etc.)
Example open standard – not tied to infrastructure!

*Push* data securely to HealthVault, colleagues, ..

- Content-type agnostic
- Simple **email** with attachments
- Security: standard S/MIME for encrypting mail messages (allows for using PKIs for authentication and encryption, if applicable)

Infrastructure independent! Just transport.

  - Cuts out the middleman (no lock-in); point-to-point, cheap, scalable.
  - Very controllable (doctor decides when to send information, and what)
  - Can be used instead of or besides “pull” systems in many cases
“Standardization” - what exactly?

Types of “standards” in (e)Health
1. content representation (e.g., HL7, ...)
2. data exchange / communication standards
3. infrastructure

Big difference.
- 1, 2: (Open) standards for 1 and 2: very much OK.
- 3: Coupling a standard to an infrastructure? NOT OK
  - recipe for lock-in, huge scale, and mission creep – someone has to pay for the system! And typically wants something in return.
Medical data – paths to disclosure

Personal health records

Professional Health information Exchange systems

“Anonymous” research data

Professional route: acceptance management
Give patient access to the system

Make patient organizations happy
Public (dis)interest?

HealthSpace

HealthSpace was a free, secure online personal health organiser. It had been helping users manage their health, store health information and find out about NHS services near to them. A HealthSpace account was available to anyone living in England, aged 16 or over, with a valid email address. HealthSpace closed on 14th December 2012 and the frequently asked questions below provide further information about this. We would like to take this opportunity to thank you for your interest in the service.

Frequently asked questions

Why has HealthSpace closed?

The service was not as popular as we would have liked. In addition, alternative approaches are being planned to give patients fuller access to their health information and the NHS Information Strategy, The Power of Information, contains further information on this.

Does the decision to close HealthSpace affect the Summary Care Record (SCR)?

No, the roll-out of SCR is unaffected by the decision to close HealthSpace. The prime purpose of SCRs is to support improved patient safety and care in urgent and emergency care settings and clinicians are now starting to report a wide range of improvements as a result of their introduction. As of mid March 2013, more than 24 million SCRs have been created across England. The implementation of the SCR is continuing at a significant pace.

Hardly any interest. See Prof. Greenhalgh (UCL)'s report.
ePatient Dave

“Gimme my damn data”
Personal health records / patient access / patient mediated transport

Patient in control
- Different route to disclose data

- Alternative route to professional health information exchange
- Room for innovation!
- Provides a choice, useful for some patients
- But not for all patients!

Some information is best kept under lock and key!
Where was data safe? Yes, with the doctor.
The patient route – a Good Thing?

- Patient route gives an alternative way to manage and disclose records
- That makes a right to (standardized, open) transcript of medical data a Good Thing.
But...

There's a problem.

It also provides an alternative route for illegitimate access, and coercion.
Coercion?

Example: insurers want access.
- ask a transcript of patient record from patient
- how to refuse?
Related example

Full patient control (patient mediated research, (experimental) consent mgt frameworks)
Examples

Patient-mediated access to research data

MyDataCan™

Extract data to a patient-mediated access/consent/disclosure tool. Great control, but..
Give me my damn data?

Who wants what data?

MyDataCan™
HealthVault

“How to avoid coercion?”

Can I have your data for Research?

Can I see your record?

You have nothing To hide, do you?
The future

Example: DNA

MyDataCan™

HealthVault

Can I have your DNA for Research?

Do you know what you consent to?

Can you, will you say no?

Who do you consent for?
Informed consent – understand the consequences?

Consent Form

Protocol Title: Personal Genome Project

Principal Investigator: George M. Church, Ph.D.

Site-Responsible Investigator’s Institution: Harvard Medical School

Co-Investigators & Study Staff: Joseph V. Thakuria, MD, MMSc

Description of Volunteer Population:
We are seeking a diverse range of volunteers from as varied a set of genetic, social and environmental backgrounds as possible. Volunteers must be willing to make their genetic and other human trait information publicly available and be knowledgeable about genetics, human subjects research and the benefits and risks of participation in a public genomics research study of this nature.

What is Informed Consent?
Informed consent means you understand the procedures, risks, possible benefits, and alternatives before you voluntarily agree to participate in a research study. Before you elect to participate, you need to understand if or how this study may affect you and your family. This form, along with other study documents available on the study website (http://www.personalgenomes.org/) (the “website”), is intended to help you make an informed decision about your participation in this study. The PGP website will be revised as needed, possibly on a frequent basis, and participants and prospective participants should check the website regularly to obtain the most current information about this study.
Dutch hospital pharmacist: “if you do not give permission to use the Dutch EPD system, We cannot give you any medication – for your own safety.”
Other examples of “patient centric” systems

E-Childcare dossier – whose record is it?

- A central repository payed by ... city of Amsterdam
- For the whole family (...)
- So, how about patient rights?
- Extra features?
- Who pays, decides
- Not open, will people be coerced to be into it in practice?

[ The e-child dossier proposal is now parked due to privacy considerations – but probably not dead. Many systems are sold as being “for/of the patient” but really are central systems containing patient data, primarily intended for professional care information exchange ]
Transparancy and patient-mediated access: a double-edged sword

Yes, patients gain control
But they can be coerced out of information, too.

Some information is best left under lock and key
Where was data safe? Yes – with the doctor!
Keep the doctor in the loop

Doctor has a stronger position to say “no” than the patient.
Patient may in practice be easily coerced
- Explicit consent before disclosing information: right to NOT disclose things, to keep stuff out of the record / transcript...
- Avoid the drive for complete records; will push privacy-sensitive people out of the care system, or may harm them.

Consent is needed for ALL routes to disclosure, including the patient route.
Summarizing: consent (opt-in) for all routes

Doctor should remain in charge over disclosure and guard data.

Patients must retain right to keep stuff out for any route.
Conclusions

Policy drive: “more (open) data, patient access, data must be complete!”
- Checks and balances are under threat. Doctor in the best position to guard the dossier.
- Beware of policy drive for “completeness” - don't forget oral, paper & direct doctor-to-doctor communication routes! ICT is no silver bullet – also not for medical care.

Ensure (open) alternative routes exist; cut out the middle man
- But.. do not consider the patient routes to be a privacy panacea

Some data should be left under lock and key.
- A general right to partial disclosure is needed! (right to leave stuff out)
- Ensure explicit opt-in procedures as a barrier to extract data through any route

Legally: ensure (severe) penalties for coercion - irrespective of the route!
- Disclosure must be the patient's FREE choice.
References


[pgp] Personal Genome Project, full consent form, available on http://www.personalgenomes.org/consent/

[directproject] The direct project – simple, secure standards-based push health information exchange – see http://directproject.org/