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

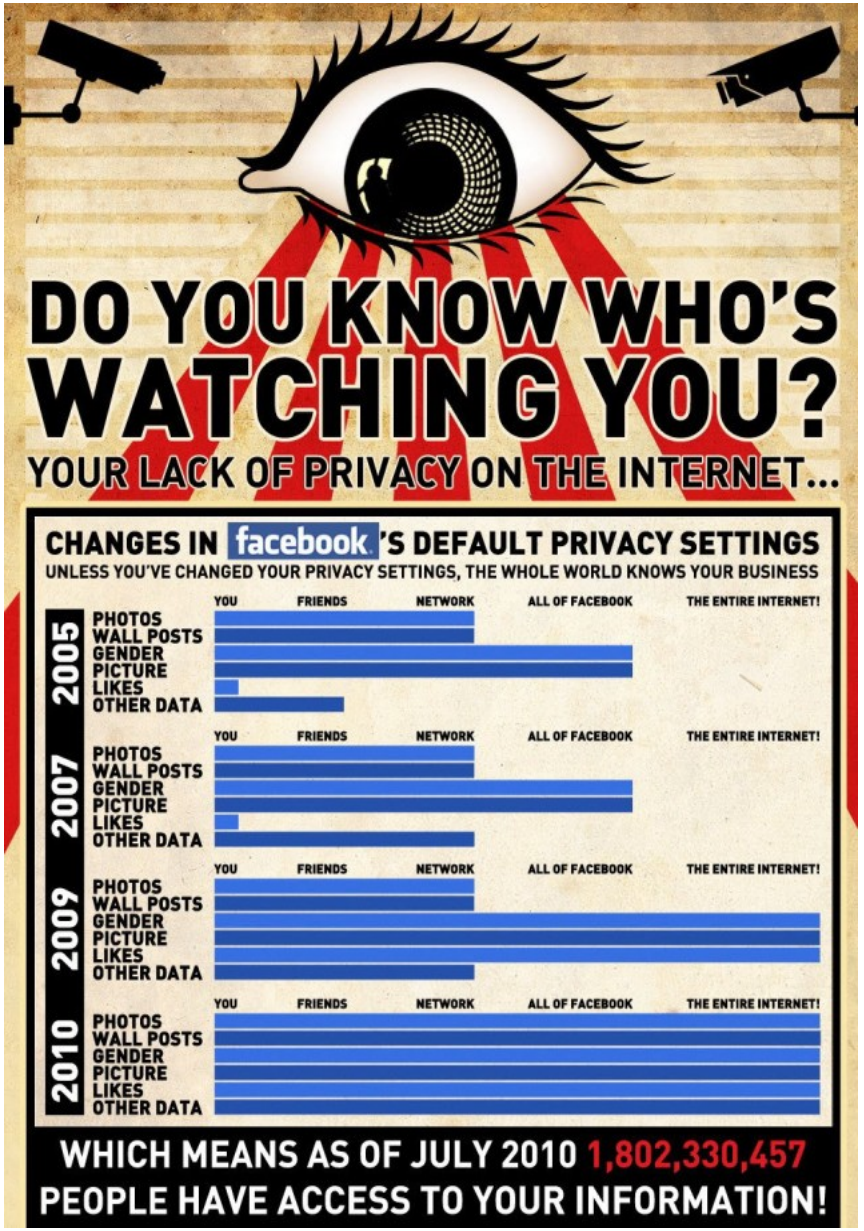
Ehealth outlook – EU policy

Quote Estonion 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.”

eHealth action plan 2012 – 2020, innovative healthcare for the 21st century, EC, Brussels, 6.12.2012.

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% patiënten avoids care in (early stages) of disease for fear of privacy breaches or stigma

- 2005 National Consumer Health Privacy Survey (Canada)

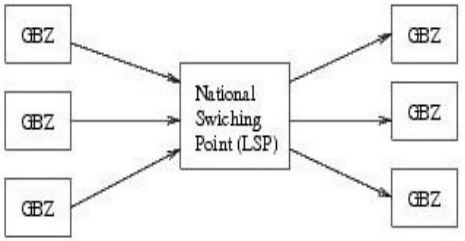
"*One out of eight* consumers has put their health at risk by engaging in such behaviors as: avoiding their regular doctor, asking their doctor to fudge a diagnosis, paying for a test because they didn't want to submit a claim, or avoiding a test altogether. Chronically ill, younger, and racial and ethnic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

Medical data – paths to disclosure

GP

HealthVault

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

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

[a] QID_A, see section 3.2.
[b] QID_B, see section 3.3.

PC4 + Date of birth + gender: 80,8% uniquely identifyable
Figuur: M. Koot et al., HotPETs, 2010 [Latanya Sweeney 2002, MASS. US]

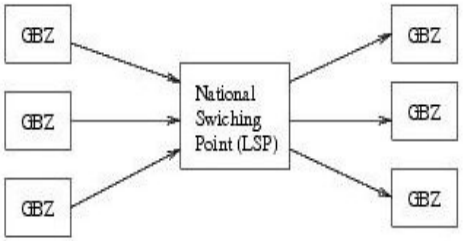
COMMIT/

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 succesful 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

GP

AUT

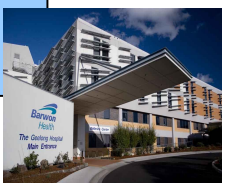
NSP

VWI

GP

Pharmacist

Hospital



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 wiith PIN code.

Security – some issues.

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

GP

AUT

vWI

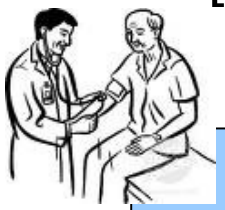
GP

Pharmacist

hospital

Security – some issues.

N = ?
[. . . . . .]

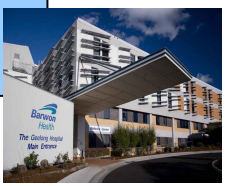


AUT
LSP
VWI

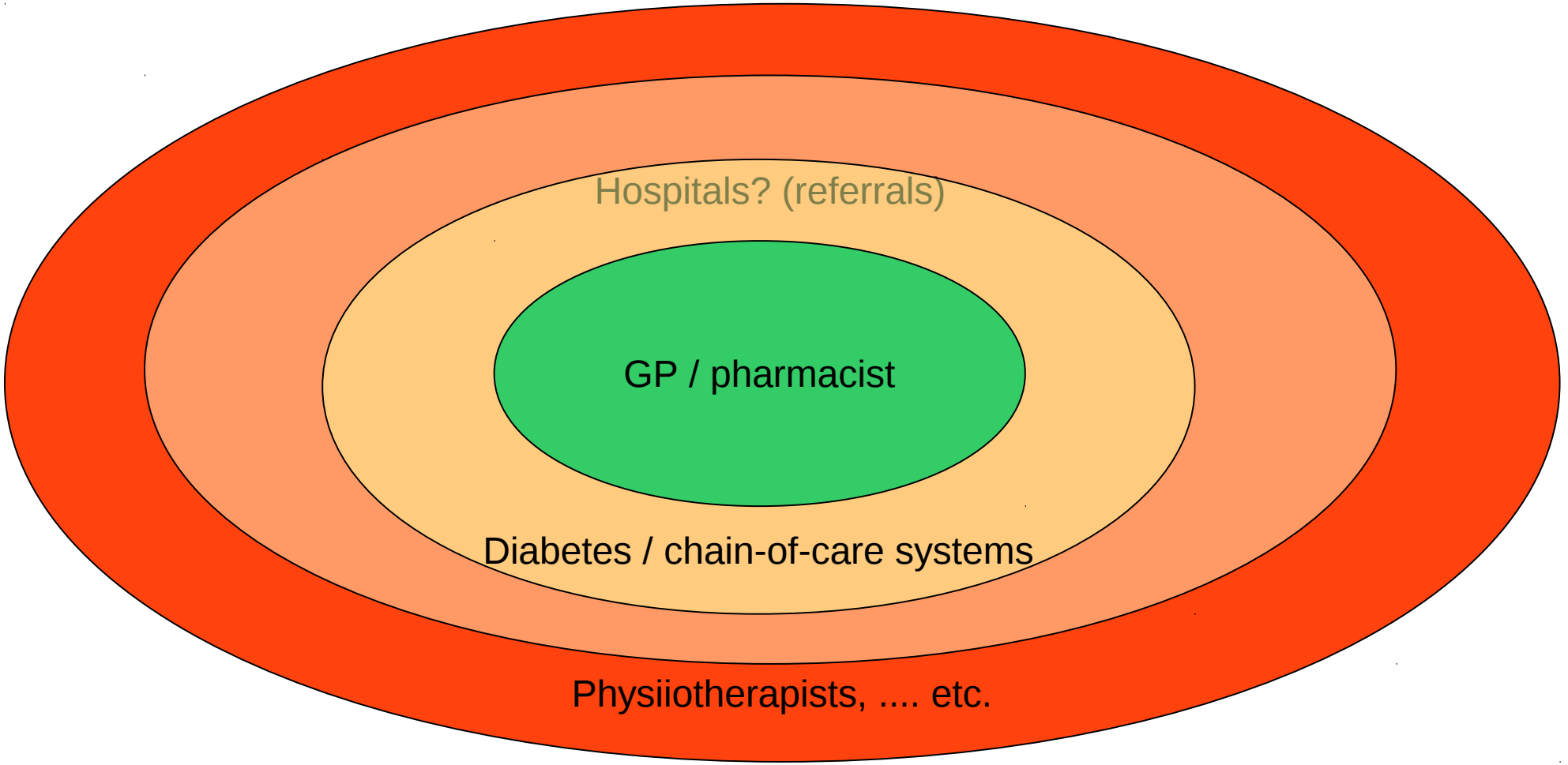
GP

Pharmacist

hospital



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



10.000 -> 400.000 smartcards ..... N = 1000 -> 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, collegues, ..

- 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.

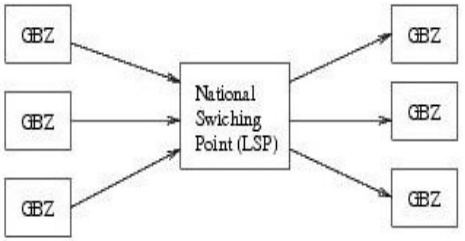
- 1, 2: (Open) standards for 1 and 2: very much OK.
- 3: Coupling a standard to an infrastructure? *NOT* OK
  - recipe for lock-in, huge scale, and mission creep – someone has to pay for the system! And typically wants something in return.

Medical data – paths to disclosure

GP

HealthVault

Personal health records



Professional Health information Exchange systems

“Anonymous” research data

Professional route: acceptance management

Give patient access to the system

GP

AUT

NSP

VWI

GP

Pharmacist

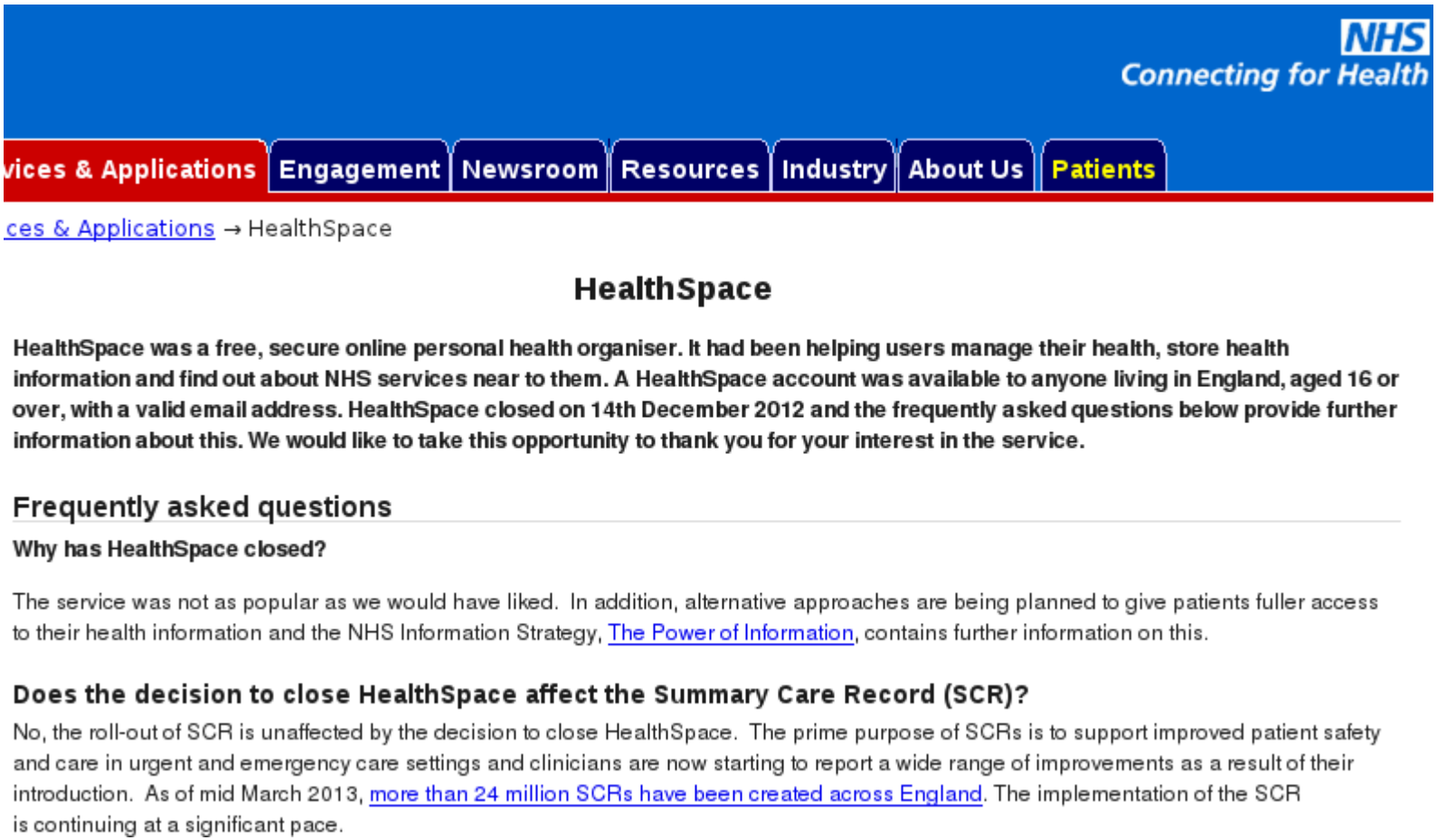
Portal

Hospital

. . . . . .

Makes patient organizations happy

Public (dis)interest?



NHS Connecting for Health

vices & Applications | Engagement | Newsroom | Resources | Industry | About Us | Patients

ces & Applications → HealthSpace

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

HealthVault

Google Health BETA

PHR

- 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!

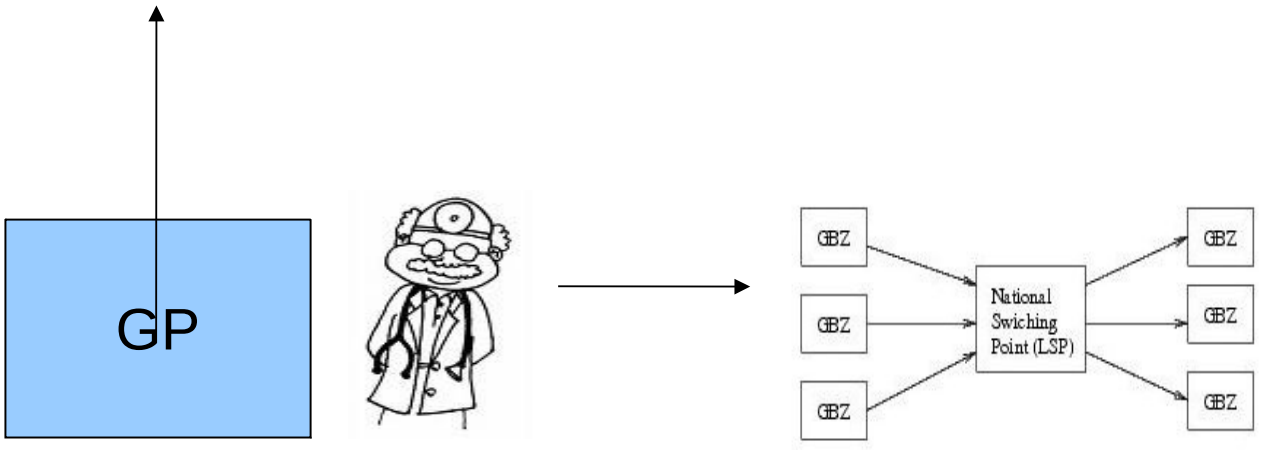
Where was data safe? *Yes, with the doctor.*

The patient route – a Good Thing?

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

HealthVault

[alternative: patient-mediated authorization]



But...

There's a problem.

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

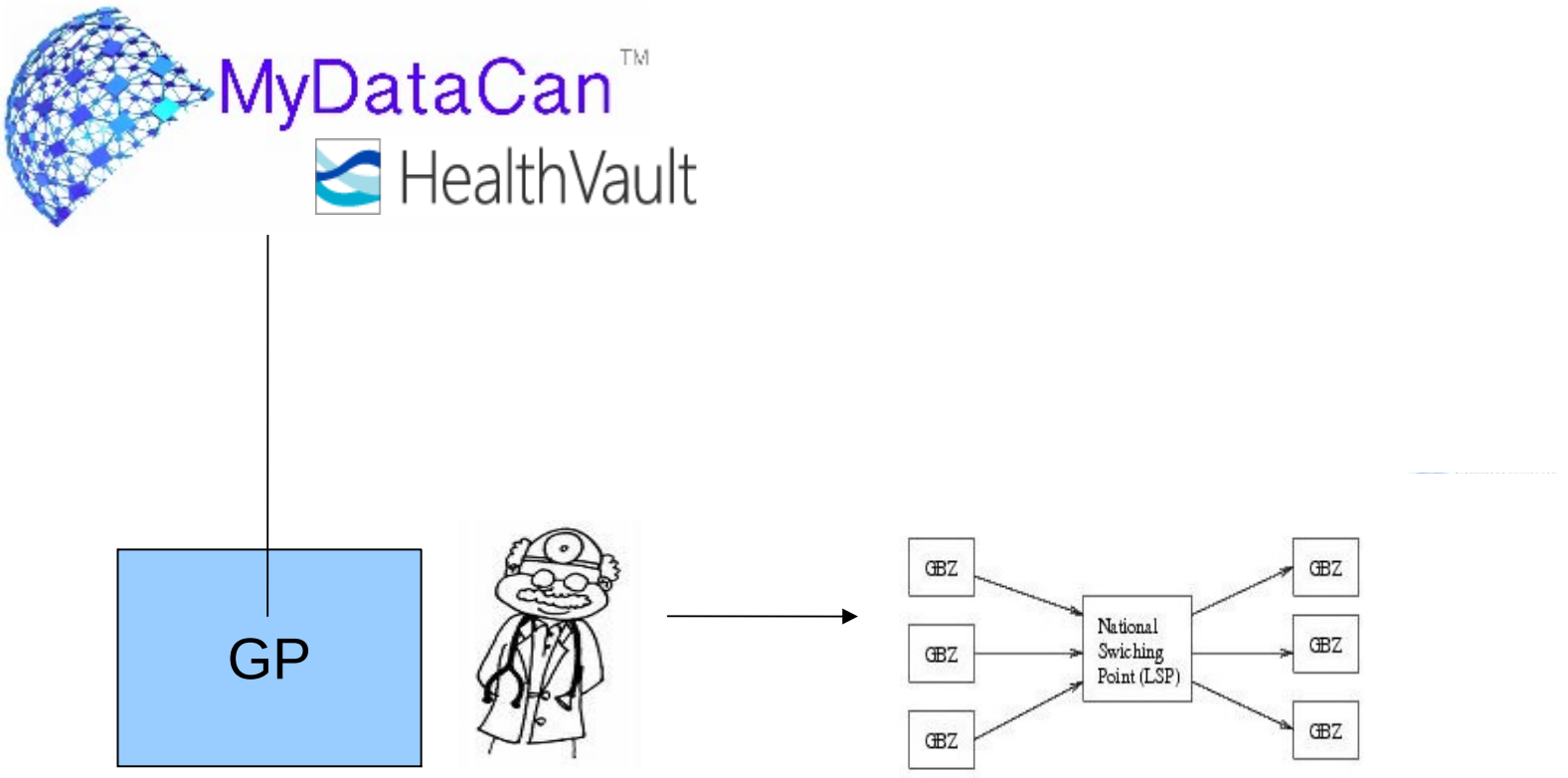
Coercion?

Example: insurers want access.

- ask a transcript of patient record from patient
- how to refuse?

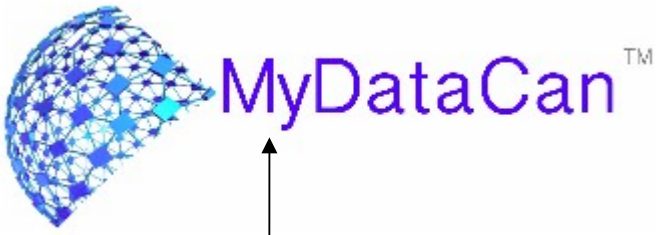
Related example

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

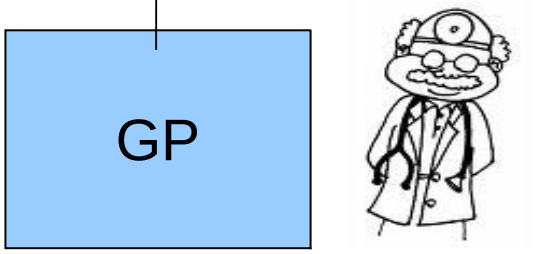


Examples

Patient-mediated access to research data



Exctract data to a patient-mediated access/consent/disclosure tool.
Great control, but..



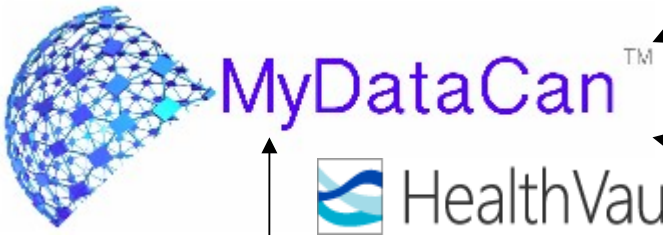
Give me my damn data?

Who wants what data?

Can I have your data for Research?

Can I see your record?

You have nothing To hide, do you?



GP

"How to avoid coercion?"

The future

Example: DNA

Can I have your DNA for Research?

GP

Do you know what you consent to?

Can you, will you say no?

Who do you consent for?

Informed consent – understand the consequences?

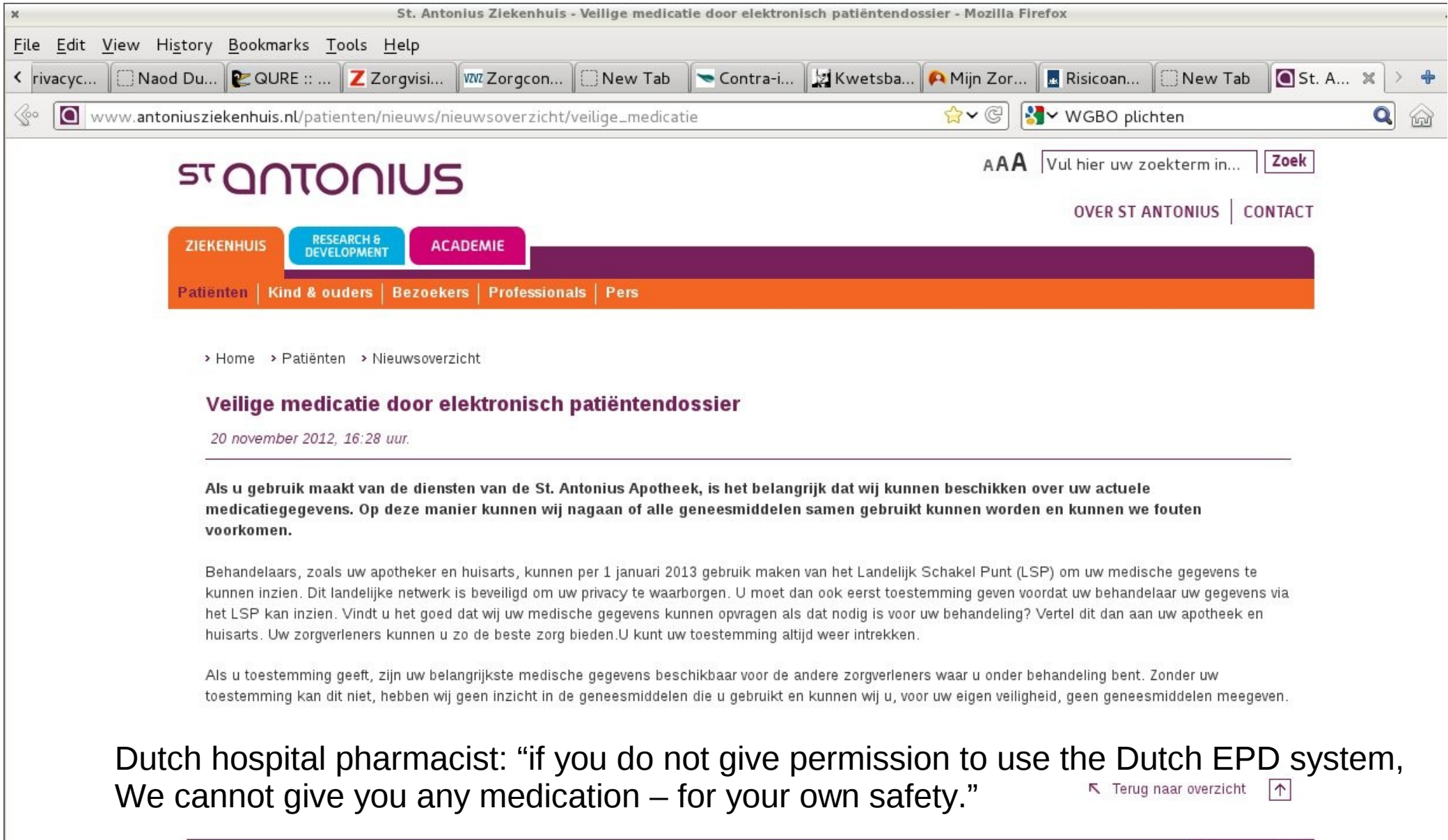
Consent Form

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.

Coerce into consent



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.

HealthVault

Google Health BETA

PHR

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

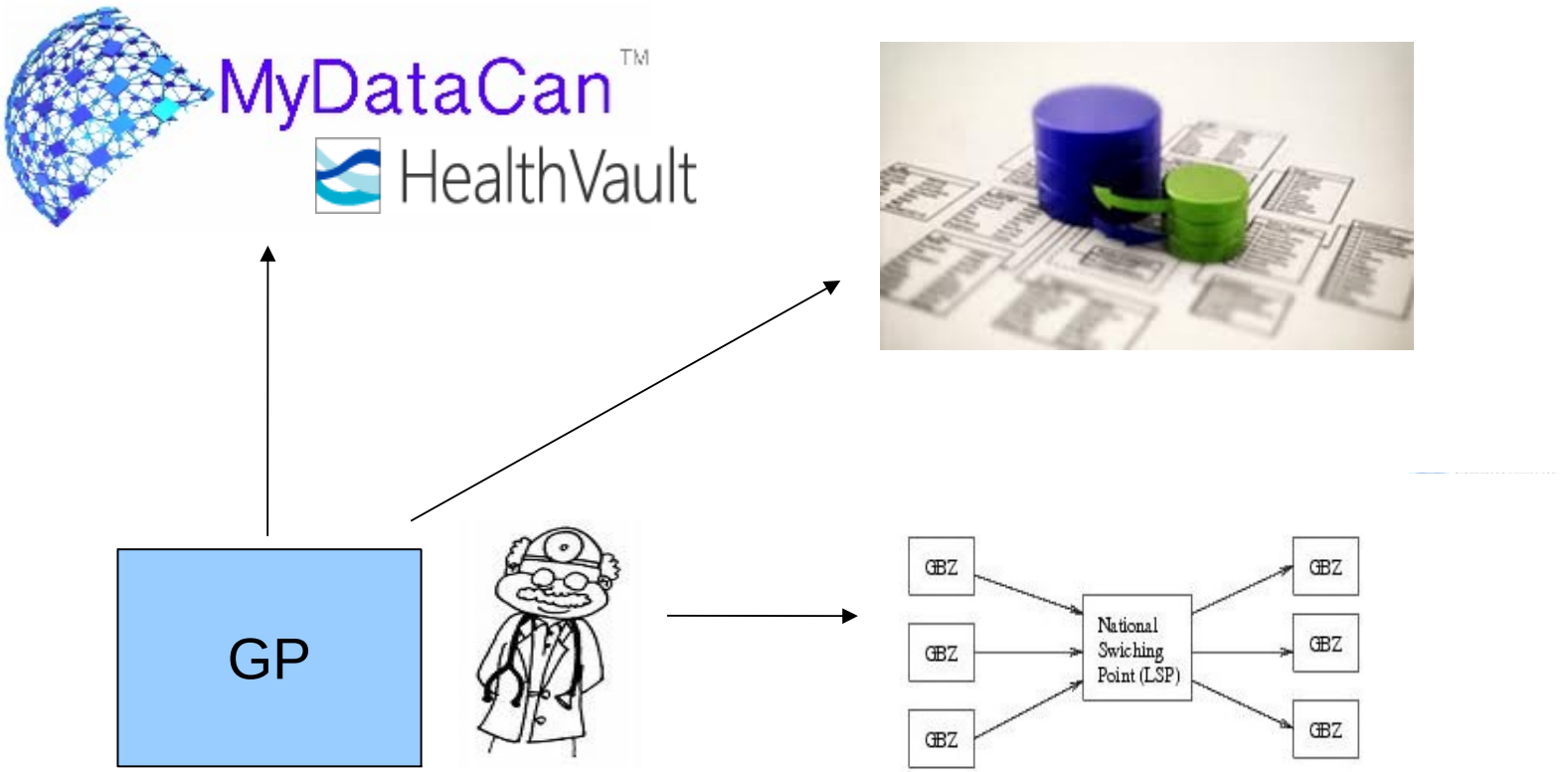
- Explicit consent before disclosing information: right to NOT disclose things, to keep stuff out of the record / transcript...
- Avoid the drive for *complete* records; will push privacy-sensitive people out of the care system, or may harm them.

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 “completenes” - 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 procecures 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

[noordende] G.J. van 't Noordende, "Security in the Dutch Electronic Patient Record System", 2nd ACM Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS), ACM Conf. Computer and Communications Systems (CCS),Chicago, Illinois, USA, October 8, 2010. pp. 21-31

[koot] M.R. Koot, G.J. van 't Noordende, C.T.A.M. de Laat, "A Study on the Re-Identifiability of Dutch Citizens", 3rd Hot Topics in Privacy Enhancing Technologies (HotPETs 2010), PETS workshop, Berlin, Germany, 2010

[sweeney] L. Sweeney. k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570.

[california] Forrester research, Inc.: National Consumer Health Privacy Survey 2005, URL: http://www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005

[hhs] U.S. Dept health and human services (HHS), Fed. Reg. Vol 65 nr. 250, Dec. 28, 2000 pp. 82761-82810, http://aspe.hhs.gov/admnsimp/final/PvcFR07.txt

[greenhalgh] T. Greenhalgh, “Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace, British Medical Journal (BMJ) 2010:341:c5814 online: http://www.bmj.com/content/341/bmj.c5814

[Brown] I. Brown, R. Anderson, T. Dowty P. Inglesant, W. Heath, A. Sasse, “Database state”, a report commissioned by the joseph rowntree reform trust ltd., 2009, available at http://www.jrrt.org.uk/publications/database-state-full-report

[mydatacan] Harvard University's MyDataCan project - http://mydatacan.org

[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/

[ec action plan] eHealth action plan 2012 – 2020, innovative healthcare for the 21st century, EC, Brussels, 6.12.2012