Problems with exchanging medical data.

Experiences in the Netherlands

A. Hasman

Two cases

- In this presentation I discuss two cases where privacy problems directly (in the case of benchmarking the quality of mental health institutions/providers) or indirecty (in the case of the national EPR) impeded the course of events
- These experiences may be useful to keep in mind by the MIRACUM project

Problems with the national EPR -1

- The national EPR was an initiative of the Dutch Ministry of Health. A project of designing, building and implementing a countrywide infrastructure to exchange data, called Aorta, started in 2002, financed by the ministry
- Since for several reasons a central healthcare database was not the solution an infrastructure was needed to exchange medical data between healthcare systems
- In addition information about which patients' data reside in which systems should be centrally available

Problems with the national EPR -2

- The rollout started in 2008
- In 2011 the EPR roll-out was discontinued because the Senate unanimously rejected a law that was earlier accepted by the House of Representatives. The ministry had to stop the roll-out of the EPR
- In 2012 the roll-out of the EPR was resumed by a private initiative by VZVZ, the Association of Healthcare providers for Care communication. Insurance companies financed an adapted EPR project

What went wrong and how was the problem solved?

- Patients' data were automatically exchanged unless the patient objected (opt-out)
  - This was changed in explicit permission, opt-in
- Physicians were obliged to exchange data via AORTA
  - This was changed to voluntary participation
- A national EPR was considered too costly (only of relatively few patients would there be data outside the region where they lived)
  - changed into a regional EPR via software means

What influenced the public opinion?

- In 2005 two hospitals agreed to let specialist hackers test their well trusted IT security systems. Hacking appeared to be easy
- Someone with a laptop visited a hospital and contacted physicians and nurses with the message that he as an engineer had to check the hospital information system. They gave him access not only to coffee and the copier but also passwords

Some examples of wrong information in media

- Physicians could look at patient data without having a treatment relation with that patient
  - All requests for information are logged and audited and heavy penalties given in case of unjustified requests
- If the physician's access card and pincode were stolen patient data could be acccessed by the thief anywhere
  - One first has to access the data network and that does not go automatically

Fear of physicians

- Fear that the exchanged patient data could contain errors. Who is responsible when these data are used and lead to harm to the patient?
  - At that time this responsibility was not settled by law but the general opinion was that the impact of erroneous data that are too difficult to be recognized by the receiver are the responsibility of the data provider

Some implementation areas of EPR

- Electronic Medication Record supports the process of prescribing and supplying medication, and the querying of a medication registry for medication that has been prescribed and supplied to a patient. There are an estimated 90,000 cases of hospitalization a year in the Netherlands as a result of avoidable medication errors, so this application is needed.
- Electronic Locum Record allows a locum GP (mostly when out of hours services are being provided) to get hold of a summary from the patient's GP, and supports the transmission of performed locum GP services to the patient's GP.

What are the components of a regional EPR?

- AORTA: supporting the transport of patient data between healthcare providers within a region via its infrastructure
- A national switchpoint with:
  - A repository (Act Reference Registry) containing metadata about which patient data can be found in the systems related with which healthcare providers
  - Information to determine if the requesting physician is allowed to see the data based on his role
  - An audit log with information about data exchanges
- The information systems of GPs, hospitals, etc.

Identification of healthcare provider

- UZI (Unique healthcare provider ID) Registry: A registry of all persons authorized to perform healthcare services in the Netherlands, managed by CIBG, an agency of the Ministry of Health
- The UZI registry delivers
  - a UZI card and a pincode to the healthcare provider with which they authenticate themselves and
  - a UZI server certificate for the QHIS (to authenticate the system)

Additional functions UZI card

- The card also facilitates authentication, encryption and the use of a digital signature (for each of these functions it uses a separate certificate)
- For using the functions of the UZI card, the UZI Registry makes use of certificates issued by the Public Key Infrastructure of the government (PKIO)

Patient identification

- BSN (Citizen Service Number) Registry: a registry of unique registration numbers of all persons living in the Netherlands, managed by the Ministry for the Interior
- The healthcare provider has to determine the identity of the patient during the first patient encounter on the basis of a legal identification document and to check the correctness of the BSN
- The healthcare provider has to record in his information system that the patient (dis)agreed with exchange of his/her data

Authorisation -1

- The authorisation of healthcare providers to request patient data takes into account:
  - Active acceptance by the patient that data can be viewed by other healthcare providers (opt-in)
  - The existence of a treatment relationship between the healthcare provider and the patient
  - That the healthcare provider is recorded in the ‘Professions in individual health care’ register

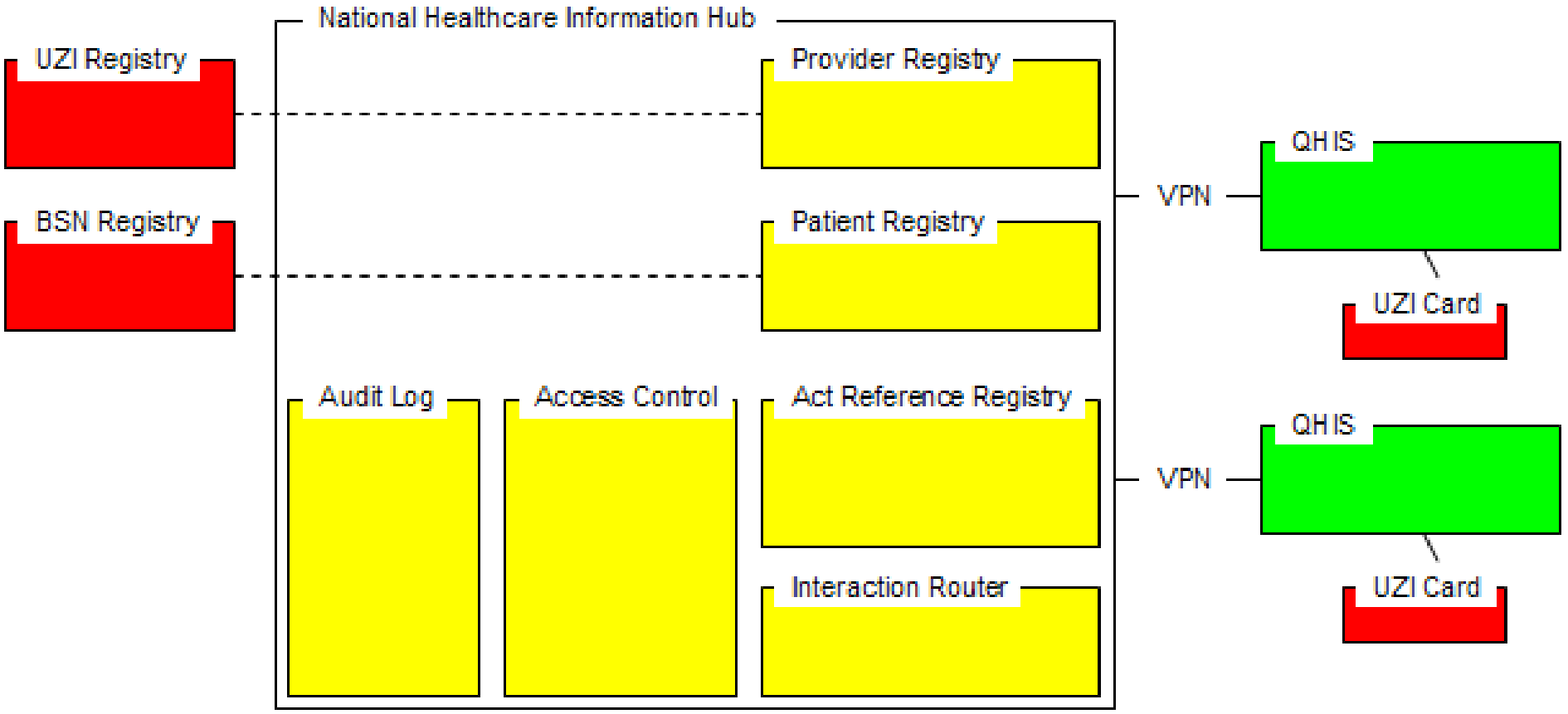
Authorisation -2

- For each healthcare profession and specialization (for each role) it is recorded which data he is allowed to view
- This information is centrally stored in a table (in the national switchboard)
- The data in the table for a specific role are compared with the contents of the HL7 message

National switchpoint

- The National switchpoint manages an Act Reference Registry; healthcare professionals provide the registry with new patient data
- The Natiional switchpoint contains an information broker that is responsible for the exchange of messages between requesting systems and source systems

National switchpoint



The architecture

- The information broker and the information systems of the providers are connected via data communication networks. The network is a private or virtual private TCP/IP network
- Both the communication network and the systems of the healthcare providers have to meet organizational and technical requirements to become a Qualified Care Network (QCN) respectively a Qualified Healthcare Information System (QHIS) in order to be accepted

Transport and security protocols

- For the transport of HL7v3 messages/documents between a QHIS and the information broker use is made of current internet protocols:
  - HTTP with TLS (HTTPS) over TCP/IP
  - To create a secure connection between QHIS and the information broker according to the TLS protocol (token identification) the QHIS possesses a UZI server certificate and the information broker a PKIO (Public key infrastructure government) certificate
  - Use is made of SOAP and of WS-security, XML-signature and XML encryption standards

Next case

- Quality assurance is increasingly important
- Apart from the use of performance indicators to determine the quality of care, healthcare providers also have to work according to a quality statute

Example -1

- Routine outcome measurements (ROMs) are used for monitoring the quality of mental healthcare: a professional therapist discusses periodically with his patients the measured progress of the treatment (as recorded in the ROMs) in order to determine, together with the patient, whether the treatment has to be adapted
- This approach is described in a quality statute and should be followed.

Example -2

- The personal data contained in the ROMs can also be used to determine the quality of the provided care to make practice variation visible.
- To that end the data are processed via a number of privacy steps by the SBG, the Foundation Benchmark GGZ (mental health care) and then analyzed
- At an aggregated level the information is fedback to the institutions/providers (benchmarking).

Privacy law

- The privacy law is applicable for the partly or wholly computerized processing of personal data
- Automatic processing concerns any act with respect to personal data, among others collection, storage, updating, changing, retrieval or the transmission of data
- Processing of personal data is only acceptable in certain situations or in case the data are anonymized

Anonymization

- Anonymizing is the process of rendering data into a form which does not identify individuals and where identification is not likely to take place

When is exchange of personal data accepted?

- There are six exceptions, among others
  - informed consent of the persons involved
  - legal obligation (it is not possible to carry out the commitment without exchange of personal data)
  - vital interest of person (an urgent medical need for example)
- For sensitive personal data there are more requirements in addition to the six

Change in interpretation

- The collection and use of ROM data is part of direct patient care. The doubly pseudomized data are used to enhance the quality of care
- The Dutch privacy watchdog, Autoriteit Persoonsgegevens, recently stated that pseudonimisation is not an anonymization technique but a measure to reduce privacy riscs
- Therefore the SBG is not allowed to process these doubly pseudonimized data
- Now the ministry of health is searching for a legal foundation for quality assurance projects

Conclusion

- It seems that the choice is: consent or anonymize, which can provide large practical problems
- Why not use another criterion: are the data secure? Data are secure when they cannot be processed outside the context of the data collection. In this case the context is benchmarking and the creatio nof anonymous (at the patient level) statistical overviews about the performance of GGZ institutions
- We should talk of privacy by design