


Andreas Holzinger  
VO 709.049 Medical Informatics  
13.01.2016 11:15-12:45

# Lecture 11

## Biomedical Data: Privacy, Safety, Security, Data Protection

a.holzinger@tugraz.at  
Tutor: markus.plass@student.tugraz.at  
<http://hci-kdd.org/biomedical-informatics-big-data>



A. Holzinger 709.049 1/76 Med Informatics L11

Status as of 12.01.2015 18:30

Dear Students, welcome to the 11th lecture of our course on issues of privacy, safety, security and data protection.

Please remember from the last lecture the key challenges: lack of integrated systems, clinical workplace efficiency and all aspects around cloud computing and service oriented computing (SaaS).

Please always be aware of the definition of biomedical informatics (Medizinische Informatik):

Biomedical Informatics is the inter-disciplinary field that studies and pursues the effective use of biomedical data, information, and knowledge for scientific inquiry, problem solving, and decision making, motivated by efforts to improve human health (and well-being).

## Schedule



- 1. Intro: Computer Science meets Life Sciences, challenges, future directions
- 2. Back to the future: Fundamentals of Data, Information and Knowledge
- 3. Structured Data: Coding, Classification (ICD, SNOMED, MeSH, UMLS)
- 4. Biomedical Databases: Acquisition, Storage, Information Retrieval and Use
- 5. Semi structured and weakly structured data (structural homologues)
- 6. Multimedia Data Mining and Knowledge Discovery
- 7. Knowledge and Decision: Cognitive Science & Human-Computer Interaction
- 8. Biomedical Decision Making: Reasoning and Decision Support
- 9. Intelligent Information Visualization and Visual Analytics
- 10. Biomedical Information Systems and Medical Knowledge Management
- **11. Biomedical Data: Privacy, Safety and Security**
- 12. Methodology for Info Systems: System Design, Usability & Evaluation

**Learning Goals: At the end of this 11th lecture you ...**

- are able to determine between privacy, safety and security;
- know the famous IOM report “Why do accidents happen” and its influence on safety engineering;
- have a basic understanding of human error and are able to determine types of adverse events in medicine and health care;
- have seen some examples on how ubiquitous computing might contribute to enhancing patient safety;
- got an idea of the principles of context-aware patient safety;
- saw a recent approach about pseudonymization for privacy in e-health;
- are aware of the security characteristics of the popular personal health records;

**Keywords of the 11<sup>th</sup> Lecture**

- Adverse events
- Anonymization
- Context aware patient safety
- Faults and Human error
- Medical errors
- Privacy
- Pseudonymization
- Privacy aware machine learning
- Safety and Security
- Swiss-Cheese Model of human error
- Technical dependability



**Advance Organizer (1/3)**

- **Acceptable Risk** = the residual risk remaining after identification/reporting of hazards and the acceptance of those risks;
- **Adverse event** = harmful, undesired effect resulting from a medication or other intervention such as surgery;
- **Anonymization** = important method of de-identification to protect the privacy of health information (antonym: re-identification);
- **Authentication** = to verify the identity of a user (or other entity, could also be another device), as a prerequisite to allow access to the system; also: to verify the integrity of the stored data to possible unauthorized modification;
- **Confidentiality** = The rule dates back to at least the Hippocratic Oath: “Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of man, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret”;
- **Data protection** = ensuring that personal data is not processed without the knowledge and the consent of the data owner (e.g. patient);
- **Data security** = includes confidentiality, integrity, and availability of data, and helps to ensure privacy;
- **Hazard** = the potential for adverse effects, but not the effect (accident) itself; hazards are just contributory events that might lead to a final adverse outcome;
- **Human fallibility** = addresses the fundamental sensory, cognitive, and motor limitations of humans that predispose them to error;

**Advance Organizer (2/3)**

- **k-Anonymity** = an approach to counter linking attacks using quasi-identifiers, where a table satisfies k-anonymity if every record in the table is indistinguishable from at least  $k - 1$  other records with respect to every set of quasi-identifier attributes; hence, for every combination of values of the quasi-identifiers in the k-anonymous table, there are at least k records that share those values, which ensures that individuals cannot be uniquely identified by linking attacks;
- **Medical error** = any kind of adverse effect of care, whether or not harmful to the patient; including inaccuracy, incompleteness of a diagnosis, treatment etc.;
- **Nomen nescio (N.N)** = used to signify an anonymous non-specific person;
- **Patient safety** = in healthcare this is the equivalent of systems safety in industry;
- **Personally-identifying information** = can be used to connect a medical record back to an identified person;
- **Prevention** = any action directed to preventing illness and promoting health to reduce the need for secondary or tertiary health care; including the assessment of disease risk and raising public health awareness;
- **Privacy** = (US pron. "prai ..."; UK pron. "pri ..."; from Latin: privatus "separated from the rest", is the individual rights of people to protect their personal life and matters from the outside world;
- **Privacy policy** = organizational access rules and obligations on privacy, use and disclosure of data;

### Advance Organizer (3/3)



- **Protected health information (PHI)** = any info on e.g. health status, treatments or even payment details for health care which may be linked back to a particular person;
- **Pseudonymisation** = procedure where (some) identifying fields within a data record are replaced by artificial identifiers (pseudonyms) in order to render the patient record less identifying;
- **Quasi-Identifiers** = sets of attributes (e.g. gender, date of birth, and zip code) that can be linked with external data so that it is possible to identify individuals out of the population;
- **Safety** = any protection from any harm, injury, or damage;
- **Safety engineering** = is an applied science strongly related to systems engineering / industrial engineering and the subset System Safety Engineering. Safety engineering assures that a life-critical system behaves as needed even when components fail.
- **Safety risk management** = follows the process defined in the ISO 14971 standard (see Lecture 12)
- **Safety-critical systems research** = interdisciplinary field of systems research, software engineering and cognitive psychology to improve safety in high-risk environments; such technologies cannot be studied in isolation from human factors and the contexts and environments in which they are used;
- **Security** = (in terms of computer, data, information security) means protecting from unauthorized access, use, modification, disruption or destruction etc.;
- **Sensitive data** = According to EC definition it encompasses *all* data concerning health of a person;
- **Swiss-Cheese Model** = used to analyze the causes of systematic failures or accidents in aviation, engineering and healthcare; it describes accident causation as a series of events which must occur in a specific order and manner for an accident to occur;

**Slide 11-1 Key Challenges**



- Sensitive, Personal Health Data
- Mobile solutions, Cloud solutions
- Primary use of Data
- Secondary use of Data for Research
- In the medical area ALL aspects require strict

# ▪ Privacy, Safety, Security and Data Protection!

Horvitz, E. & Mulligan, D. 2015. Data, privacy, and the greater good. Science, 349, (6245), 253-255.

A. Holzinger 709.049

8/76

Med Informatics L11

## Slide 11-1: Key Challenges

- Data in the Cloud,
  - mobile solutions, the trend towards software-as-a-service, and
  - the massive increase in the amount of data ...
- ... in the medical area require a lot of future effort in Privacy, Data Protection, Security and Safety.

The challenges of data integration, data fusion and the increased use of data for secondary use put these issues from a “nice-to-have” into the key interest. Example: In January 2013, the US Department of Health and Human Services released the Omnibus Final Rule, which significantly modified the privacy and security standards under the Health Insurance Portability and Accountability Act (HIPAA). These new regulations were driven by a need to ensure the confidentiality, integrity, and security of patients’ protected health information (PHI) in electronic health records (EHRs) and addresses these concerns by expanding the scope of regulations and increasing penalties for PHI violations (Wang & Huang, 2013).

# Safety first ...

Let us start with a look at safety first

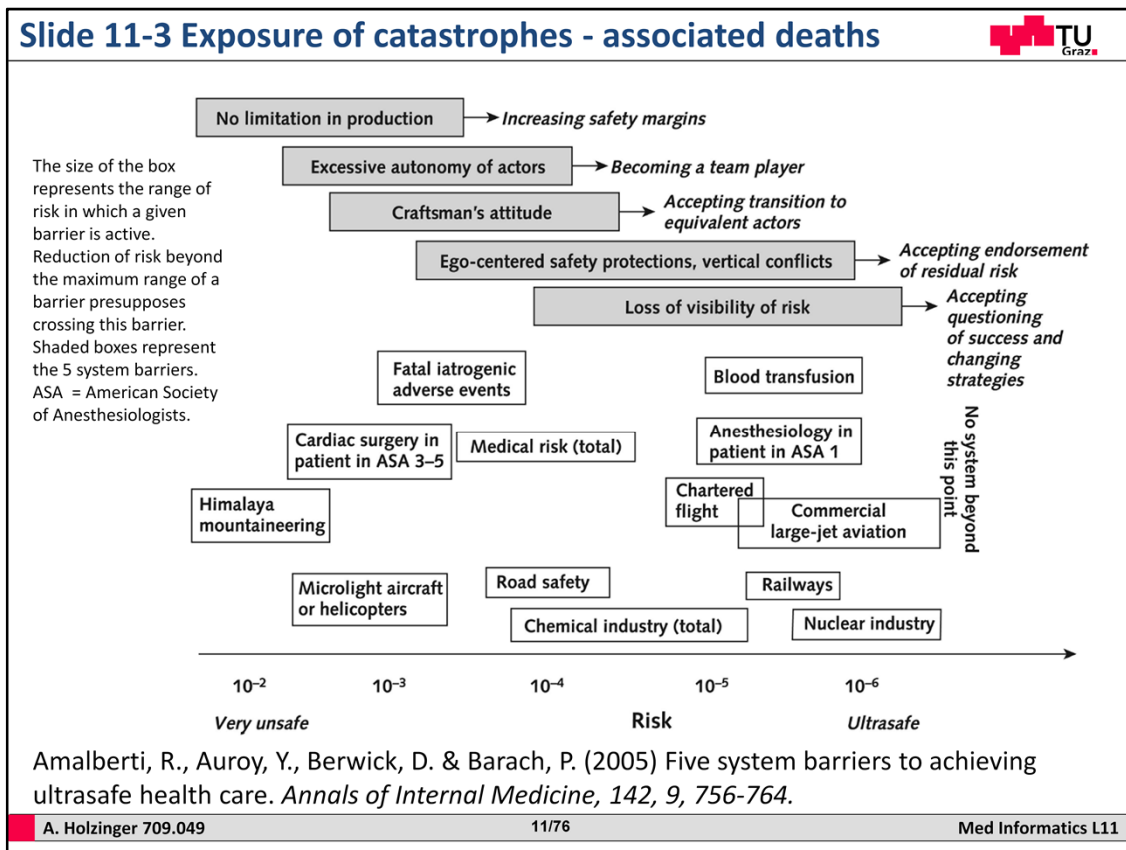
**Slide 11-2 We start with thinking about safety first ...**



<http://ngadventure.typepad.com/blog/news-k2-death-trap-is-sec.html>

A. Holzinger 709.049 10/76 Med Informatics L11

According to a classic survey by Amalberti et al. (2005) we can determine between very risky enterprises, typically Himalaya mountaineering and relatively save enterprises with low risk, typically commercial large-jet aviation. The medical area is in between, with a tendency to the Himalaya depending on the health area.



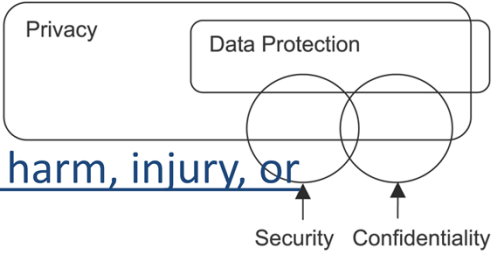
These are the study results presented by Amalberti (2005), ranging from very unsafe to ultrasafe.

In many clinical domains, such as trauma surgery, the rate of serious complications is relatively high, but not all complications are related to medical errors. In contrast, some health care sectors, e.g. gastroenterologic endoscopy, are very safe.

The size of the box represents the range of risk in which a given barrier is active. Reduction of risk beyond the maximum range of a barrier presupposes crossing this barrier. Shaded boxes represent the 5 system barriers. ASA American Society of Anesthesiologists.



**Slide 11-4a Definitions (1/2) ...**



- **Safety** = any protection from harm, injury, or damage;
- **Data Protection** = all measures to ensure availability and integrity of data
- **Privacy** = (US pron. “prai ...”; UK pron. “pri ...”; from Latin: privatus "separated from the rest", are the individual rights of people to protect their personal life and matters Confidentiality = secrecy (“ärztliche Schweigepflicht”)

Mills, K. S., Yao, R. S. & Chan, Y. E. (2003) Privacy in Canadian Health Networks: challenges and opportunities. *Leadership in Health Services*, 16, 1, 1-10.

A. Holzinger 709.049 12/76 Med Informatics L11

#### Slide 11-4 Definitions: Privacy, Security - Safety

Privacy = include the individual rights of people to protect their personal life and matters from the outside world;

Safety = any protection from harm, injury, or damage; a weighting process reflects how comfortable an organization deals with its risk exposure. Accident rates in health care currently range from 10<sup>-1</sup> to 10<sup>-7</sup> events per exposure (Amalberti, Auroy, Berwick & Barach, 2005).

Security = (in terms of computer, data, information security) means protecting from unauthorized access, use, modification, disruption or destruction etc.;

A good example for these issues is the electronic health record in →Slide 11-26:

The patient data must be confidential, secure and safe, whilst at the same time it must be usable, useful, accurate, up-to-date and accessible.



**Slide 11-4b Definitions (2/2)...**

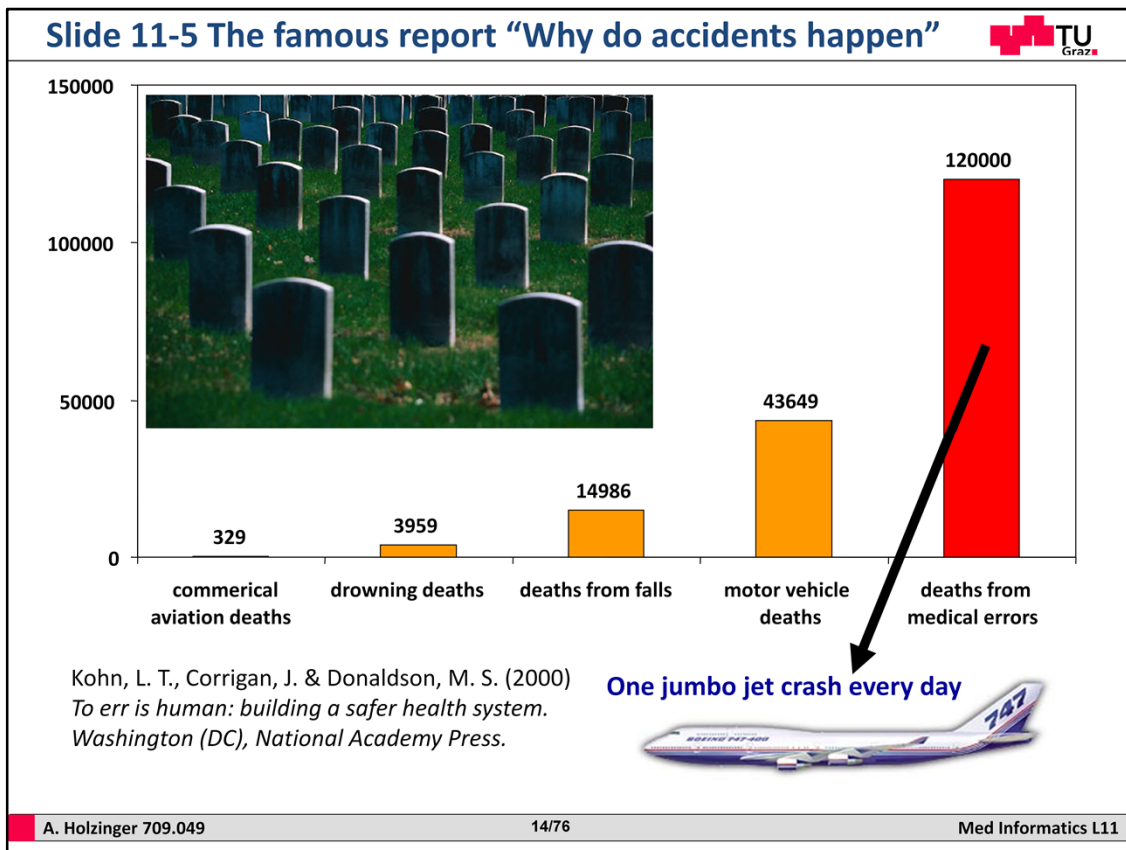
- **Availability** =  $p(x)$  that a system is operational at a given time, i.e. the amount of time a device is actually operating as the percentage of total time it should be operating;
- **Reliability** = the probability that a system will produce correct outputs up to some given time;
- **Security** = (in terms of computer, data, information security) means protecting from unauthorized access, use, modification, disruption or destruction etc.;
- **Dependability** = the system property that integrates such attributes as reliability, availability, safety, security, survivability, maintainability (see slide 11-22);



**ARES Conference**  
*International Conference on Availability, Reliability and Security*

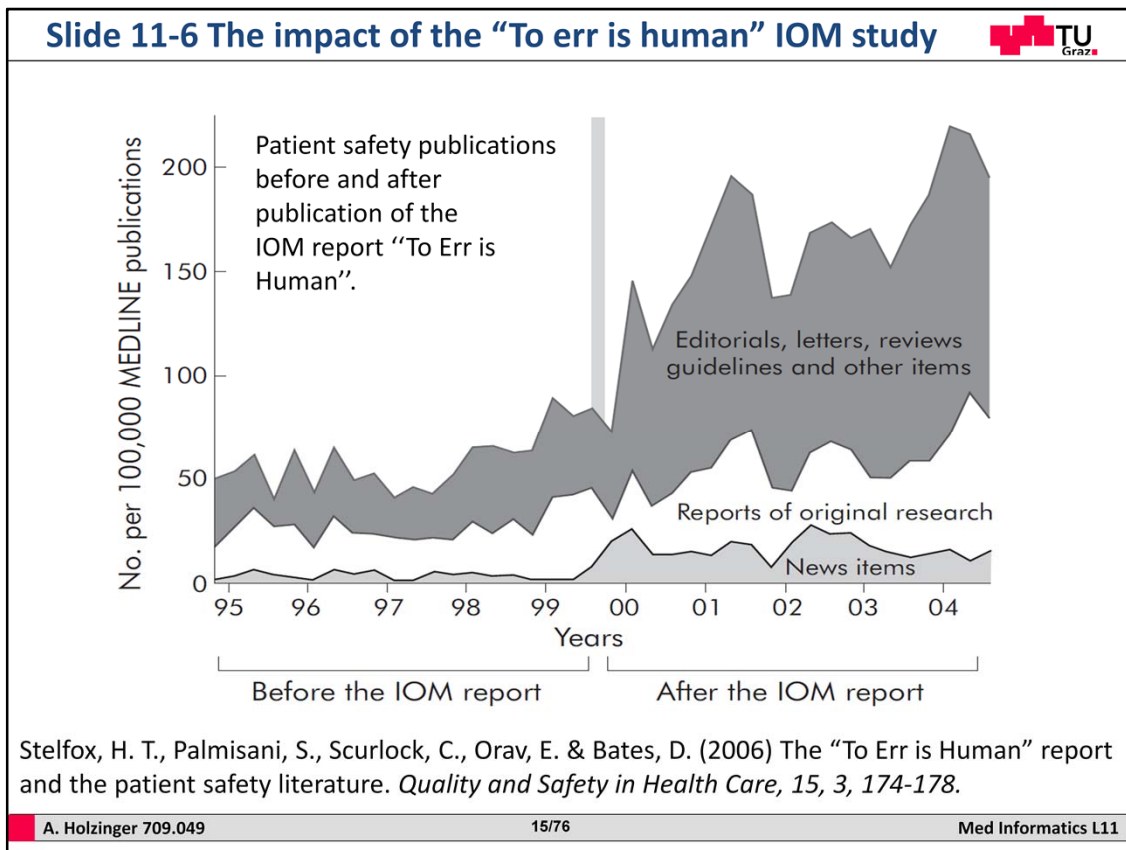
<http://www.ares-conference.eu>

security as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security in the different fields of applications.



As we have already heard in lecture 7, the Institute of Medicine (IOM) released a report in 1999 entitled “To Err is Human: Building a Safer Health System”. The IOM report called for a 50% reduction in medical errors over 5 years. Its goal was to break the cycle of inaction regarding medical errors by advocating a comprehensive approach to improve patient safety. The healthcare industry responded with a wide range of patient safety efforts and safety was a topic for researchers (Figure 11-3). Hospital information systems vendors adopted safer practices and emphasized that safety was also now a priority for them (Stelfox et al., 2006). However, so far no comprehensive nationwide monitoring system exists for patient safety, and a recent effort by the Agency for Healthcare Research and Quality (AHRQ) to get a national estimate by using existing measures showed little improvement (Leape & Berwick, 2005).

Kohn L.T., Corrigan, J.M., Donaldson, M.S. (1999): *To Err is Human: Building a Safer Health System*, National Academy Press, Washington (DC)



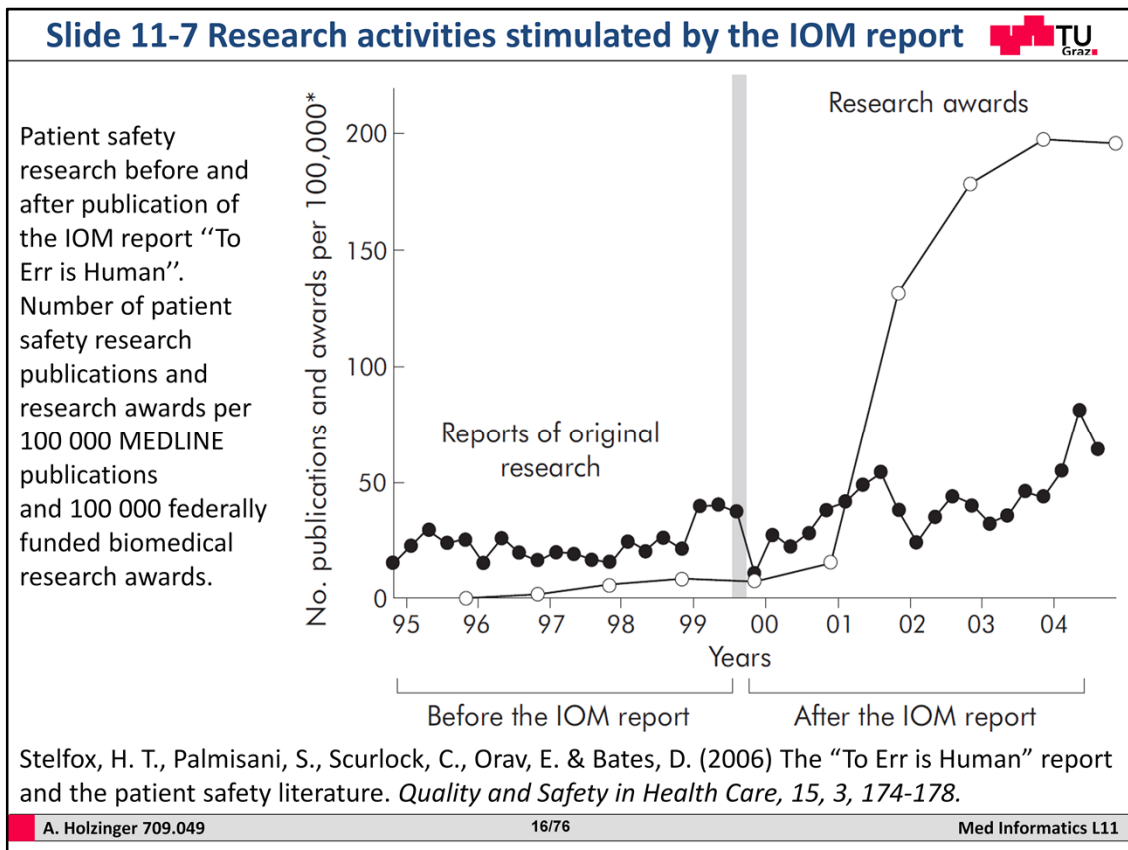
### Five years after the IOM report

#### Changes in patient safety publications

A large shift in the number of patient safety publications followed the release of the IOM report (fig 1). An average of 59 patient safety articles were published per 100 000

MEDLINE publications in the 5 years before the IOM report; this increased to 164 articles per 100 000 MEDLINE publications in the 5 years after publication of the report (p,0.001).

Even after controlling for an existing 3% per quarter upward trend (p,0.001), the rate of patient safety publications increased immediately after the release of the IOM report by 64% (p,0.001). Significantly increased rates of publication were observed for all types of patient safety articles (table 1). Rates of patient safety publications in the top general medical journals mirrored those in MEDLINE indexed journals, averaging four articles per 100 000 MEDLINE publications before the IOM report and 13 articles per 100 000 MEDLINE publications after the IOM report (p,0.001).



Here we see that the report stimulated research to a certain extent.

**Slide 11-8 Deaths from medical error (2009) ...**



**SCIENTIFIC AMERICAN™**  
Winner of the 2011 National Magazine Award for General Excellence  
Search: ScientificAmerican.com

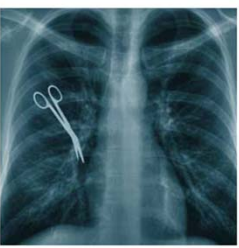
Subscribe News & Features Blogs Multimedia Education Citizen Science Topics

Home » Blogs » News Blog »

 **News Blog**  
More Blogs »

**Deaths from avoidable medical error more than double in past decade, investigation shows**  
By Katherine Harmon | Aug 10, 2009 06:45 PM | 28

Share Email Print

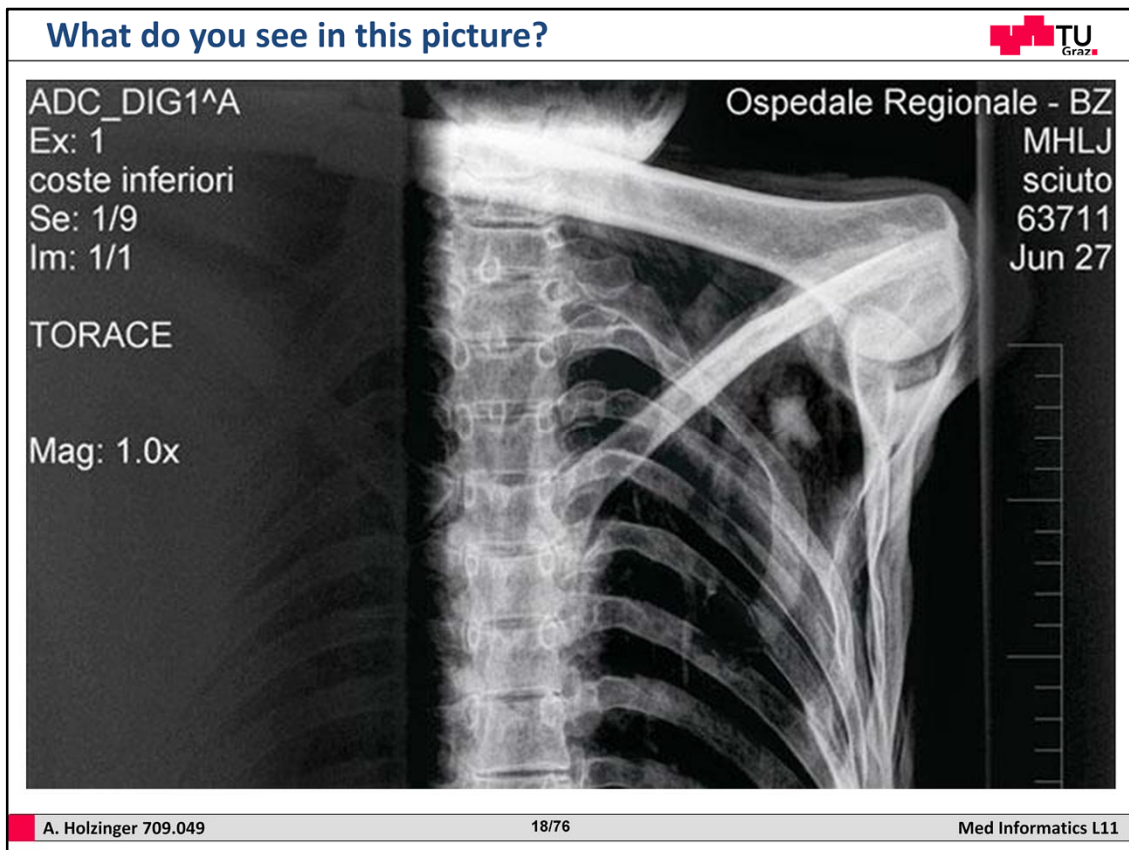


Preventable medical mistakes and infections are responsible for about 200,000 deaths in the U.S. each year, according to an investigation by the Hearst media corporation. The report comes 10 years after the Institute of Medicine's "To Err Is Human" analysis, which found that 44,000 to 98,000 people were dying annually due to these errors and called for the medical community and government to cut that number in half by 2004.

The precise number of these deaths is still unknown because many states lack a standard or mandatory reporting system for injuries due to medical mistakes. The investigative team gathered disparate medical records, legal documents, personnel files and reports and analyzed databases to arrive at its estimate.

A. Holzinger 709.049 17/76 Med Informatics L11


<http://www.scientificamerican.com/blog/post.cfm?id=deaths-from-avoidable-medical-error-2009-08-10>




Ötzi the Iceman (Similaun Man) is the oldest preserved natural mummy of a man who lived around 3300 BC




## Slide 11-9 Medical Error Example: Wrong-Site Surgery





Manjunath, P. S., Palte, H. & Gayer, S. (2010) Wrong site surgery—a clear and constant fear. *British Medical Journal (BMJ)*, 341.

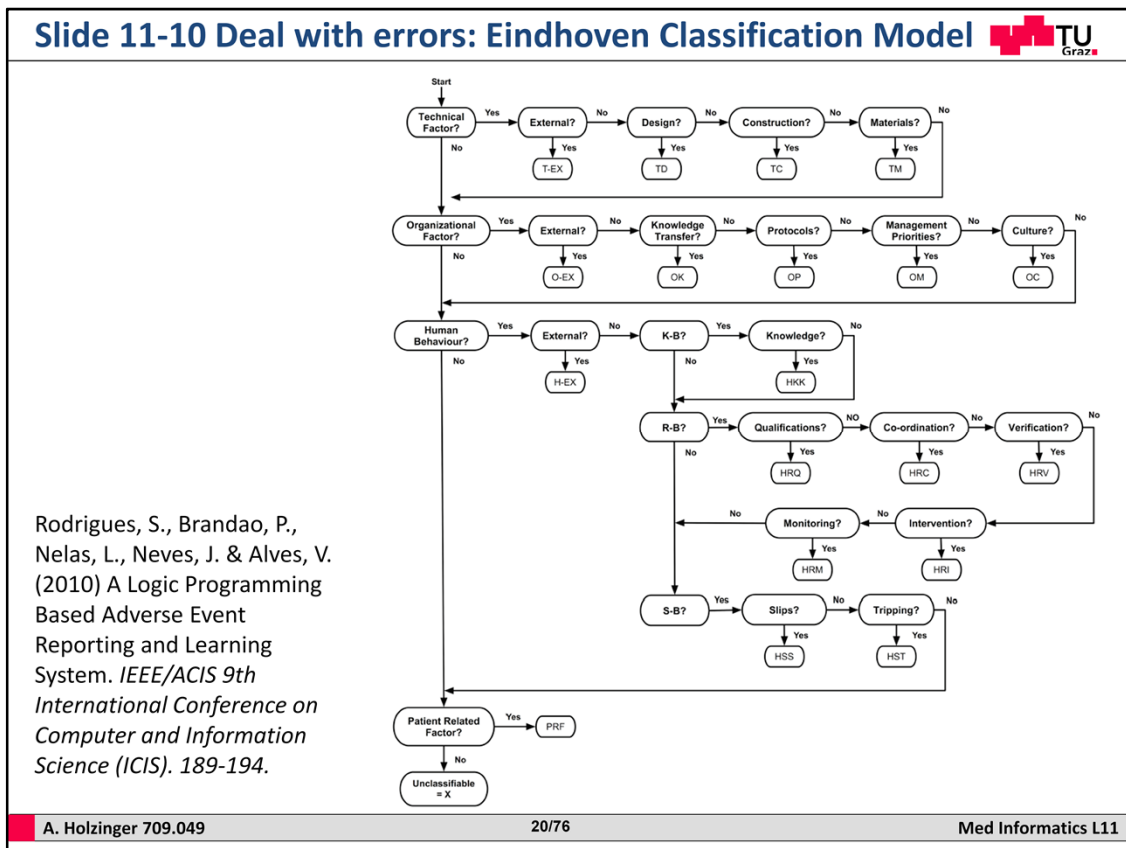


Starling, J. & Coldiron, B. M. (2011) Outcome of 6 years of protocol use for preventing wrong site office surgery. *Journal of the American Academy of Dermatology*, 65, 4, 807-810.

Integration of a correct surgery site protocol into a daily patient care model is a useful step in preventing occurrences of wrong site dermatologic surgery.

A. Holzinger 709.049
19/76
Med Informatics L11

As you can still read in the newspapers wrong-site surgery is still a big issue , or as {Manjunath, 2010 #4665} put it forward it is a clear and constant fear.

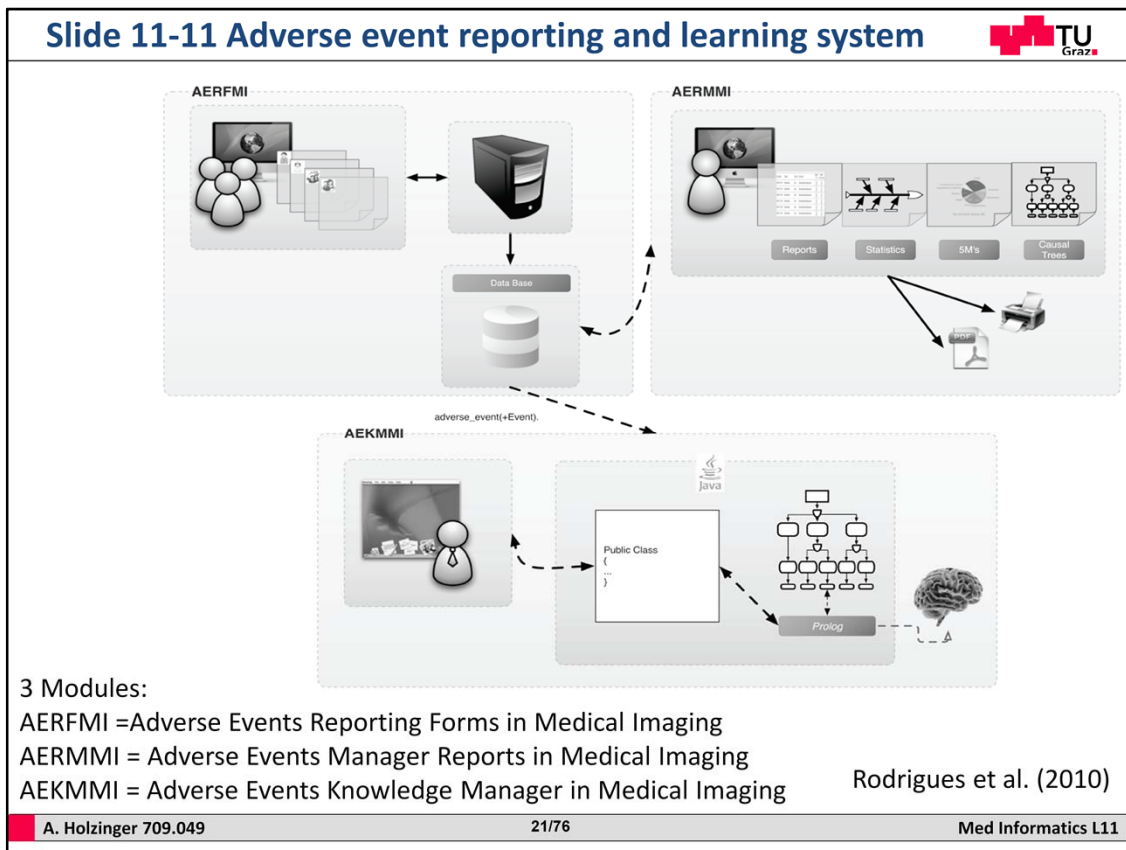


The ECM medical version consists of 20 codes, divided into four categories seen in this slide, frequently used in a medical environment to classify the underlying causes of the adverse events: 1) technical factors, 2) organizational factors, 3) human factors and 4) Patient related factors – if it is none of the above – it is unclassifiable.

## II. EXTENDED EINDHOVEN CLASSIFICATION MODEL

A large number of different systems have been used to classify events regarding to patient safety [10]. Many of the methods used to analyze patient safety were adapted from risk-management techniques in industries, especially in high-risk industries such as the chemical, nuclear power and aviation industry [5]. The Eindhoven Classification Model (ECM) was originally developed to manage human error in the chemical process industry and was then applied to various other industries, such as steel industry, energy production and in healthcare. The ECM medical version consists of 20 codes, divided into four categories (Fig. 1), frequently used in a medical environment to classify the underlying causes of the adverse events [11].



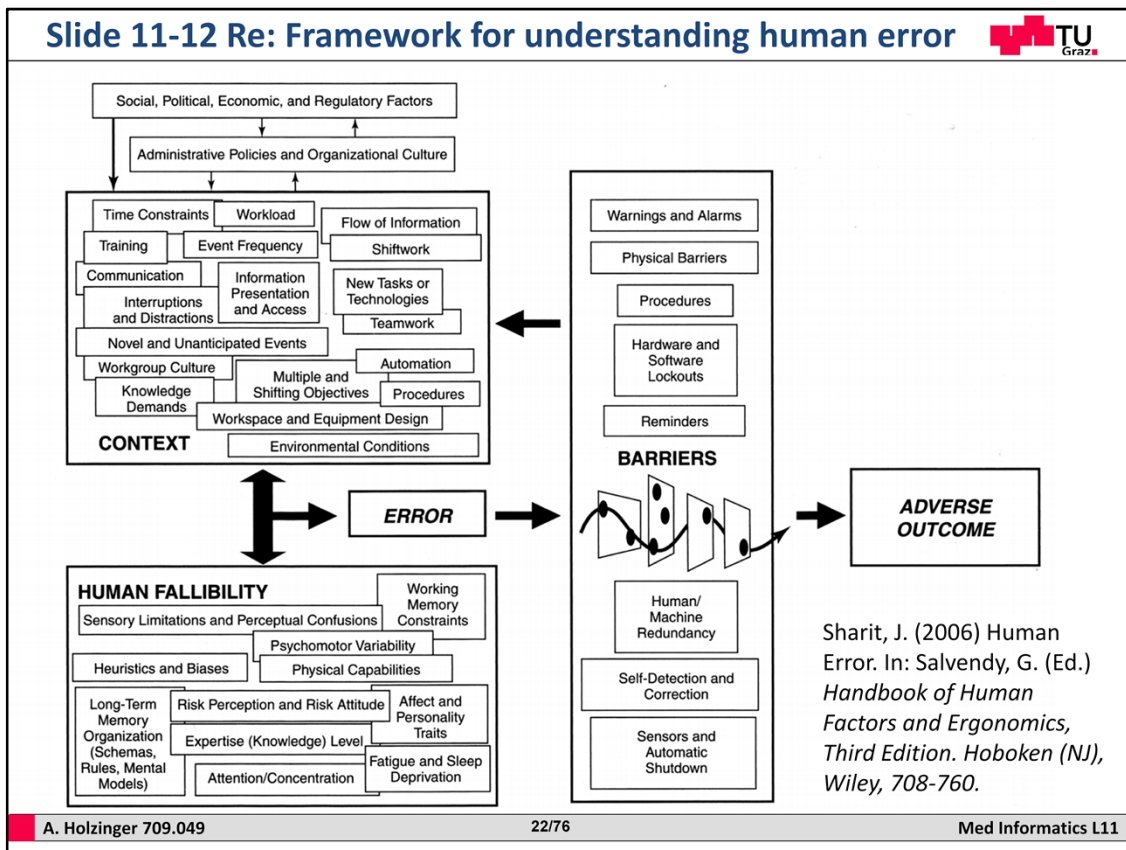


### Slide 11-11 Adverse event reporting and learning system

Here we see the AEMI (Adverse Events in Medical Imaging) system developed by (Rodrigues et al., 2010), which intends to reduce the amount of time and manual labor required for analysis. The AEMI architecture includes three modules:

- 1) Adverse Events Reporting Forms in Medical Imaging (AERFMI),
- 2) Adverse Events Manager Reports in Medical Imaging (AERMMI) and
- 3) Knowledge Manager Adverse Events in Medical Imaging (AEKMMI).

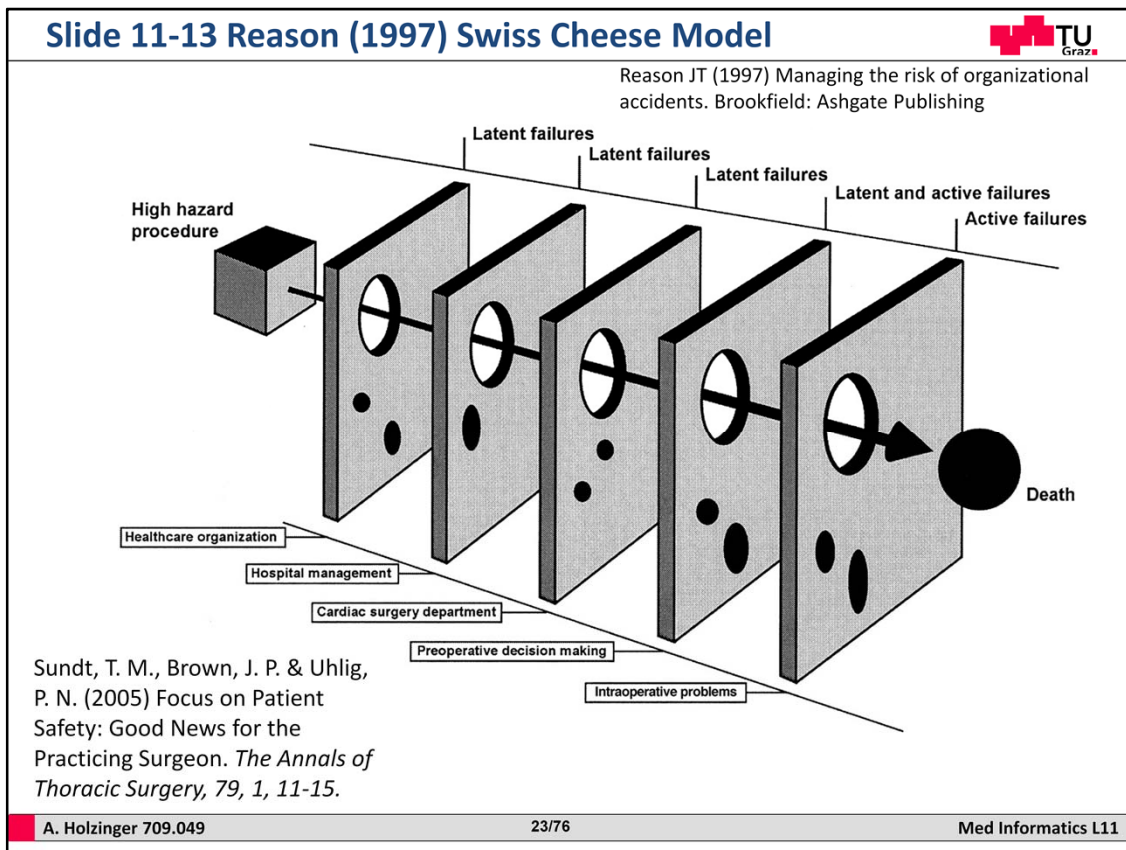
AERFMI provides the Web interface for adverse events registration. The effort on this interface was focused in its usability. AERMMI is also Web based and aims to enable the individual analysis of each adverse event recorded by AERFMI and provides some relevant statistics related to the various events registered. AEKMMI is a Java application. This module uses the data from the system database to create a Knowledge Base (KB) based on the EECM using the logic programming language Prolog (Rodrigues et al., 2010).



### Slide 11-12 Review: Framework for understanding human error

In lecture 7 we discussed a framework for demonstrating how human error – resulting in adverse events – arise. Remember, the framework consists of three components:


- 1) Human fallibility addresses the fundamental sensory, cognitive, and motor limitations of humans that predispose them to error;
  - 2) Context refers to situational variables that can affect the way in which human fallibility becomes manifest; and
  - 3) Barriers concerning the various ways in which human errors can be contained;
- We will now focus on one particular issue in the third component: The next slide shows the famous “Swiss cheese” model of accident causation.



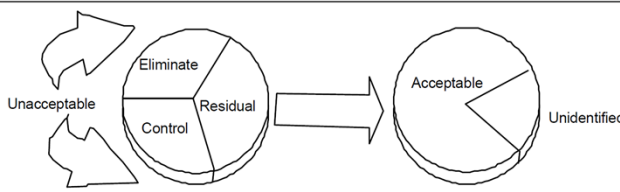
### Slide 11-13 Reason (1997) Swiss Cheese Model

The “Swiss cheese” model of accident causation emphasizes that adverse events occur when active failures align with gaps or weaknesses in the systems permitting an error to go untrapped and uncompensated (Sundt, Brown & Uhlig, 2005). The model was originally developed by (Reason, 1997), and a good reading is (Reason, 2000).

## Slide 11-14 Risk management - FAA System Safety



Note: Now just definitions, refer to risk management in Lecture 12



Total Risk
Residual Risk

- **Total risk** = identified + unidentified risks.
- **Identified risk** = determined through various analysis techniques. The first task of system safety is to identify, within practical limitations, all possible risks. This step precedes determine the significance of the risk (severity) and the likelihood of its occurrence (hazard probability). The time and costs of analysis efforts, the quality of the safety program, and the state of technology impact the number of risks identified.
- **Unidentified risk** is the risk not yet identified. Some unidentified risks are subsequently identified when a mishap occurs. Some risk is never known.
- **Unacceptable risk** is that risk which cannot be tolerated by the managing activity. It is a subset of identified risk that must be eliminated or controlled.
- **Acceptable risk** is the part of identified risk that is allowed to persist without further engineering or management action. Making this decision is a difficult yet necessary responsibility of the managing activity. This decision is made with full knowledge that it is the user who is exposed to this risk.
- **Residual risk** is the risk left over after system safety efforts have been fully employed. It is not necessarily the same as acceptable risk. Residual risk is the sum of acceptable risk and unidentified risk. This is the total risk passed on to the user.

A. Holzinger 709.049
24/76
Med Informatics L11

### Slide 11-14 Risk management - FAA System Safety

We will talk about risk management also in the last lecture, but we need the definitions now for a common understanding, and look at the image top right in the slide:

Total risk = identified + unidentified risks.

Identified risk = determined through various analysis techniques. The first task of system safety is to identify, within practical limitations, all possible risks. This step precedes determine the significance of the risk (severity) and the likelihood of its occurrence (hazard probability). The time and costs of analysis efforts, the quality of the safety program, and the state of technology impact the number of risks identified.


Unidentified risk is the risk not yet identified. Some unidentified risks are subsequently identified when a mishap occurs. Some risk is never known.


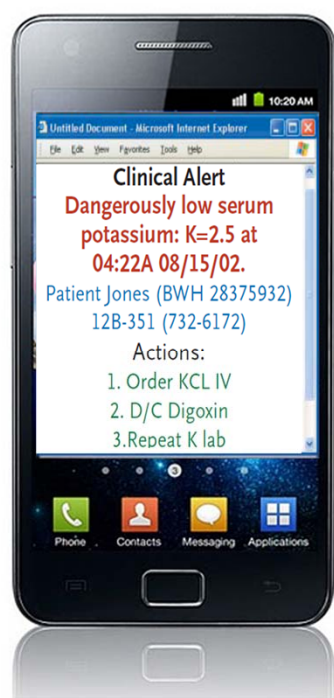
Unacceptable risk is that risk which cannot be tolerated by the managing activity. It is a subset of identified risk that must be eliminated or controlled.

Acceptable risk is the part of identified risk that is allowed to persist without further engineering or management action. Making this decision is a difficult yet necessary responsibility of the managing activity. This decision is made with full knowledge that it is the user who is exposed to this risk.

Residual risk is the risk left over after system safety efforts have been fully employed. It is not necessarily the same as acceptable risk. Residual risk is the sum of acceptable risk and unidentified risk. This is the total risk passed on to the user.

## Slide 11-15 Improving Safety with IT – Example Mobile



Bates, D. W. & Gawande, A. A. (2003)  
Improving Safety with Information Technology.  
*New England Journal of Medicine*, 348, 25,  
2526-2534.

A. Holzinger 709.049
25/76
Med Informatics L11

Slide 11-15 Improving Safety with IT – here a meanwhile historical example Mobile


Patient safety in healthcare is the equivalent of systems safety in industry, which is usually built in four steps:

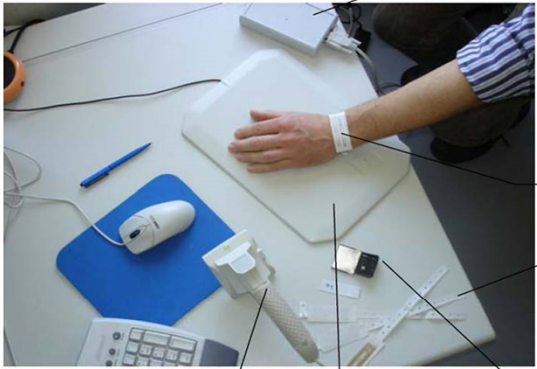
- (1) measuring risk and planning the ideal defense model,
- (2) assessing the model against the real behavior of professionals, and modifying the model or inducing a change in behavior when there are gaps,
- (3) adopting a better micro- and macro-organization,
- (4) gradually re-introducing within the rather rigid, prescriptive system built in steps 1–3 some level of resilience enabling it to adapt to crises and exceptional situations .

In this slide we see an example of a mobile system screening for laboratory abnormalities, for example, hypokalemia and a decreasing haematocrit, would require urgent action but occur relatively infrequently, often when a clinician is not at hand, and such results can be buried amid less critical data.

Such mobile systems can identify and rapidly communicate these problems to clinicians automatically (Bates & Gawande, 2003).



**Slide 11-16: Enhancing Patient Safety with ubiquitous devices** 



Midrange Reader Feig MR100

Wristband including RFID Transponder Infineon my-d (15693)

Compact Flash Slot Module for Tablet PC or Mobile Devices Microsensys

Mid Range Reader PRH100 Serial COM Interface

Pad Antenna Feig 300/300

Holzinger, A., Schwabberger, K. & Weitlaner, M. (2005). *Ubiquitous Computing for Hospital Applications: RFID-Applications to enable research in Real-Life environments* 29th Annual International Conference on Computer Software & Applications (IEEE COMPSAC), Edinburgh (UK), IEEE, 19-20.

A. Holzinger 709.049 26/76 Med Informatics L11

### Slide 11-16: Enhancing Patient Safety with ubiquitous devices

This is another example on how, for example wrong site surgery can be avoided: Patients check in at the Hospital – in addition to an ordinary wristband an RFID transponder is supplied. Patient data is entered via our application at the check-in-point, any previous patient data can be retrieved from the HIS. From this information, uncritical but important data (such as name, blood type, allergies, vital medication etc.) is transferred to the wristband's RFID transponder. The Electronic Patient Record (EPR) is created and stored at the central server. From this time the patient is easily and unmistakably identifiable. All information can be read from the wristband's transponder or can be easily retrieved from the EPR by identifying the patient with a reader. In contrast to manual identification, automatic processes are less error-prone. Unlike barcodes, RFID transponders can be read without line of sight, through the human body and most other materials. This enables physicians and nurses to retrieve, verify and modify information in the Hospital accurately and instantly. In addition, this system provides patient identification and patient data – even when the network is crashed (Holzinger, Schwabberger & Weitlaner, 2005)

## Slide 11-17: Security Problems of ubiquitous computing



### 1) Protection precautions:

- 1) vulnerability to eavesdropping,
- 2) traffic analysis,
- 3) spoofing and denial of service.
- 4) Security objectives, such as confidentiality, integrity, availability, authentication, authorization, nonrepudiation and anonymity are *not* achieved unless special security mechanisms are integrated into the system.

**2) Confidentiality:** the communication between reader and tag is unprotected, except of high-end systems (ISO 14443). Consequently, eavesdroppers can listen in if they are in immediate vicinity.

**3) Integrity:** With the exception of high-end systems which use message authentication codes (MACs), the integrity of transmitted information cannot be assured. Checksums (cyclic redundancy checks, CRCs) are used, but protect only against random failures. The writable tag memory can be manipulated if access control is not implemented.

Weippl, E., Holzinger, A. & Tjoa, A. M. (2006) Security aspects of ubiquitous computing in health care. *Springer Elektrotechnik & Informationstechnik, e&i, 123, 4, 156-162.*

A. Holzinger 709.049

27/76

Med Informatics L11

### Slide 11-17: Security Problems of ubiquitous computing

Security requires confidentiality (aka secrecy), integrity and availability. All other requirements such as non-repudiation can be traced back to one of these three requirements. Non-repudiation, for instance, can be seen as a special case of integrity, i.e. the integrity of log data recording.

The most well-known security requirement is confidentiality. It means that users may obtain access only to those objects for which they have received authorization, and will not get access to information they must not see.


The integrity of the data and programs is just as important as confidentiality but in daily life it is frequently neglected.

Integrity means that only authorized people are permitted to modify data (or programs). Secrecy of data is closely connected to the integrity of programs of operating systems. If the integrity of the operating system is compromised, then the integrity of the data can no longer be guaranteed. The reason is that a part of the operating system (i.e. the reference monitor) checks for each access to a resource whether the subject is authorized to perform the requested operation. Since the operating system is compromised the reference monitor is no longer trustworthy. It is then obvious that secrecy of information cannot be guaranteed any longer if this mechanism is not working. For this reason it is important to protect the integrity of operating systems just as properly as the secrecy of information.

It is through the Internet that many users have become aware that availability is one of the major security requirements for computer systems. Availability is defined as the readiness of a system for correct service.

With growing ubiquitous computing in health care security problems are increasing (Weippl, Holzinger & Tjoa, 2006):

- 1) Protection precautions: vulnerability to eavesdropping, traffic analysis, spoofing and denial of service. Security objectives, such as confidentiality, integrity, availability, authentication, authorization, nonrepudiation and anonymity are not achieved unless special security mechanisms are integrated into the system.
- 2) Confidentiality: the communication between reader and tag is unprotected, except of high-end systems (ISO 14443). Consequently, eavesdroppers can listen in if they are in immediate vicinity.
- 3) Integrity: With the exception of high-end systems which use message authentication codes (MACs), the integrity of transmitted information cannot be assured. Checksums (cyclic redundancy checks, CRCs) are used, but protect only against random failures. The writable tag memory can be manipulated if access control is not implemented.

**Slide 11-18 Clinical Example: Context-aware patient safety 1/2** 




Bardram & Norskov (2008)


A. Holzinger 709.049 28/76 Med Informatics L11

### Slide 11-18 Clinical Example: Context-aware patient safety 1/2

(Bardram & Norskov, 2008) developed a context aware patient safety and information system (CAPSIS) designed for use during surgery, designed to monitor what is going on in the operating room (OR). This information is used to display medical data to the clinicians at the appropriate time, and to issue warnings if any safety issues are detected. CAPSIS was implemented using the Java Context-Awareness Framework (JCAF) and monitors such information as the status of the operation; the status and location of the patient; the location of the clinicians in the operating team; and equipment, medication, and blood bags used in the operating room. This information is acquired and handled by the JCAF context awareness infrastructure, and a special safety service, implemented by means of the Java Expert System Shell (Jess), is used for overall reasoning on what actions should be taken or what warnings should be issued. CAPSIS differs from other patient safety systems in being designed to monitor everything (or as many things as possible) in the OR, and therefore to be capable of reasoning across the entire gamut of facts pertaining to the situation in the OR. It thus supplements human vigilance on safety by providing a machine counterpart that is capable of drawing inferences (Bardram & Norskov, 2008).



**Slide 11-19 Clinical Example: Context aware patient safety 2/2** 



The screenshot displays the CAPSIS system interface, which is divided into several panels. Panel A (top left) shows patient information: 070160-1114, Anna Hansen, female, 48 years old. It includes a photo, a 'CAVE' (Critical Alert Value Error) list, and a 'STOP' button. Panel B (top middle) shows the patient's medical record, including a list of diagnoses and medications. Panel C (top right) shows the patient's medical images, including X-rays and ultrasound scans. Panel D (bottom right) shows a checklist for the surgical procedure. Panel E (bottom left) shows a surgeon in an operating room interacting with the system. Panel F (bottom middle) shows a surgeon in an operating room interacting with the system.

Bardram, J. E. & Nørskov, N. (2008) A context-aware patient safety system for the operating room. *Proceedings of the 10th international conference on Ubiquitous computing. Seoul, Korea, ACM, 272-281.*

A. Holzinger 709.049 29/76 Med Informatics L11

### Slide 11-19 Clinical Example: Context aware patient safety 2/2

This slide shows the user interface of the CAPSIS system, which consists of 4 windows: (A) is the main patient safety window, which provides an overview of the patient's safety status for the operation in question;

(B) shows the patient's medical record;

(C) shows the patient's medical images; and

(D) shows the relevant checklist for the given surgical procedure.

The patient safety window (A) is composed of three panels: the patient panel, the staff panel and the patient safety panel. The patient panel aggregates important information about the current patient and surgery, including the patient's name, social security number (SSN), allergies (CAVE), picture, scheduled surgery, and current status and location. The main purpose of this frame is to help the surgical staff avoid the three big wrongs: wrong patient, wrong procedure and wrong surgical site, as well as presenting vital information on the safety of the patient such as the CAVE list and patient status (Bardram & Nørskov, 2008).


**Slide 11-20 Patient Safety**

- (1) measuring risk and planning the ideal defense model,
- (2) assessing the model against the real behavior of professionals, and modifying the model or inducing a change in behavior when there are gaps,
- (3) adopting a better micro- and macro-organization,
- (4) gradually re-introducing within the rather rigid, prescriptive system built in steps 1–3 some level of resilience enabling it to adapt to crises and exceptional situations

Amalberti, R., Benhamou, D., Auroy, Y. & Degos, L. (2011) Adverse events in medicine: Easy to count, complicated to understand, and complex to prevent. *Journal of Biomedical Informatics*, 44, 3, 390-394.


**Slide 11-20 Patient Safety**

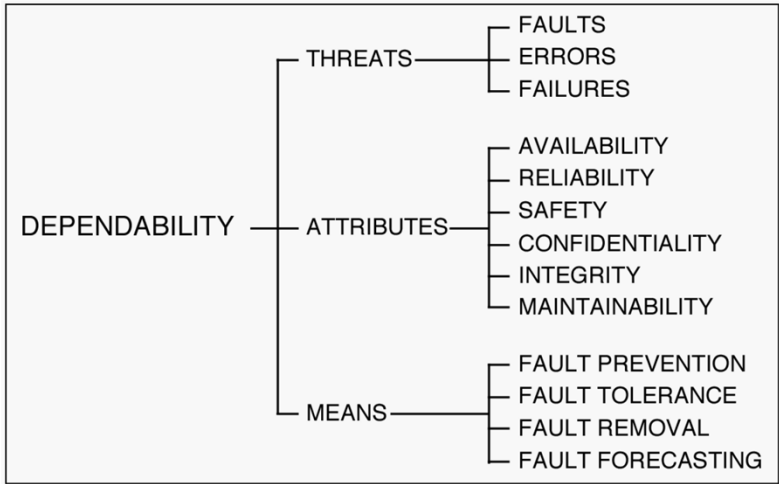
Patient safety in healthcare is the equivalent of systems safety in industry, which is usually built in four steps: (1) measuring risk and planning the ideal defense model, (2) assessing the model against the real behavior of professionals, and modifying the model or inducing a change in behavior when there are gaps, (3) adopting a better micro- and macro-organization, (4) gradually re-introducing within the rather rigid, prescriptive system built in steps 1–3 some level of resilience enabling it to adapt to crises and exceptional situations. The development of patient safety has nowhere near reached step 4 except in specific areas such as blood transfusion or laboratory testing. Even step 1 has not been completed (Amalberti et al., 2011).

Slide 11-21 Types of adverse events in medicine and care					
					
Number	Events	Description			
1	Sentinel event	The case is not anticipative death, lose any abilities in normal processing, or such that the patient kills himself, the thief takes baby, blood transfusion or blood type incompatible cause hemolysis, or person or operation position identify wrong et al..	7	Medical adverse event	The event causes harm on body of patient, extends hospital day, loses any abilities, or death. But causing the event not come from original disease.
		The person is not intentionally, indiscriminately, or unsuitable behavior that forms un-expect or unfortunate events.	8	No harm event	The event had happen on patient, but has not caused anything or a bit harm
			9	Preventable - avoidable adverse event	The related employee had done use specify processing that can avoid harm for patients, but related employee still mistake to cause adverse event.
2	Accident	Manual error or equipment shutdown causes fault of processing sporadically. No matter what, operation of the system was broken.	10	High-alert drugs	The event maybe cause critical harm to patient result from un-normal use or manage drugs.
3	Incident		11	Adverse drug reaction, ADR	Patients usually not expect serious reaction for using drugs or one of list below entry (notice: about ADR announce ,that was when patient takes medicine cause expect response, were the ability of encouraged) : <ul style="list-style-type: none"> <li>● Do not using any drugs ( drugs were either therapy nor diagnosis )</li> <li>● To change medicine therapy</li> <li>● To adjust dosage ( to adjust a bit dosage )</li> <li>● Go to hospital over night</li> <li>● Extension in hospital day</li> <li>● Assisted therapy</li> <li>● Causing diagnosis complicated</li> <li>● Producing negative effect</li> </ul> Result in temporary or permanent harm(disabled or death )
4	Critical incident	If the event, that was manual error or equipment shutdown, does not timely discovery or correction. The event maybe causes serious result such as extension			
5	Incident reporting	To record all un-normal processing and treatment different with normal processing in hospital.			
6	Near miss	Due to un-expect or immediately action makes who has not happen accident, harm, or disease about the patient.	12	Adverse drug event ,ADE	Because the patient take medicine or medical employee has not get medicine result in the event.
Chen, R. C., Tsan, P. C., Lee, I. Y. & Hsu, J. C. (2009). <i>Medical Adverse Events Classification for Domain Knowledge Extraction. 2009 Ninth International Conference on Hybrid Intelligent Systems, Shenyang (China), IEEE, 298-303.</i>					
A. Holzinger 709.049			31/76		Med Informatics L11

### Slide 11-21 Types of adverse events in medicine and care

An error may or may not cause an adverse event. Adverse events are injuries that result from a medical intervention and are responsible for harm to the patient (death, life-threatening illness, disability at the time of discharge, prolongation of the hospital stay, etc.). For example, a near miss (Number 6 in this slide) is an adverse event that either resolves spontaneously or is neutralized by voluntary action before the consequences have time to develop. Adverse events may be due to medical errors, in which case they are preventable, or to factors that are not preventable; so, the occurrence is always a combination of human factors and system factors (Garrouste-Orgeas et al., 2012).

**Slide 11-22 Safety, Security -> Technical Dependability**




```

graph LR
    D[DEPENDABILITY] --- T[THREATS]
    D --- A[ATTRIBUTES]
    D --- M[MEANS]
    T --- F1[FAULTS]
    T --- E[ERRORS]
    T --- FA[FAILURES]
    A --- AV[AVAILABILITY]
    A --- R[RELIABILITY]
    A --- S[SAFETY]
    A --- C[CONFIDENTIALITY]
    A --- I[INTEGRITY]
    A --- MA[MAINTAINABILITY]
    M --- FP[FAULT PREVENTION]
    M --- FT[FAULT TOLERANCE]
    M --- FR[FAULT REMOVAL]
    M --- FF[FAULT FORECASTING]
        
```

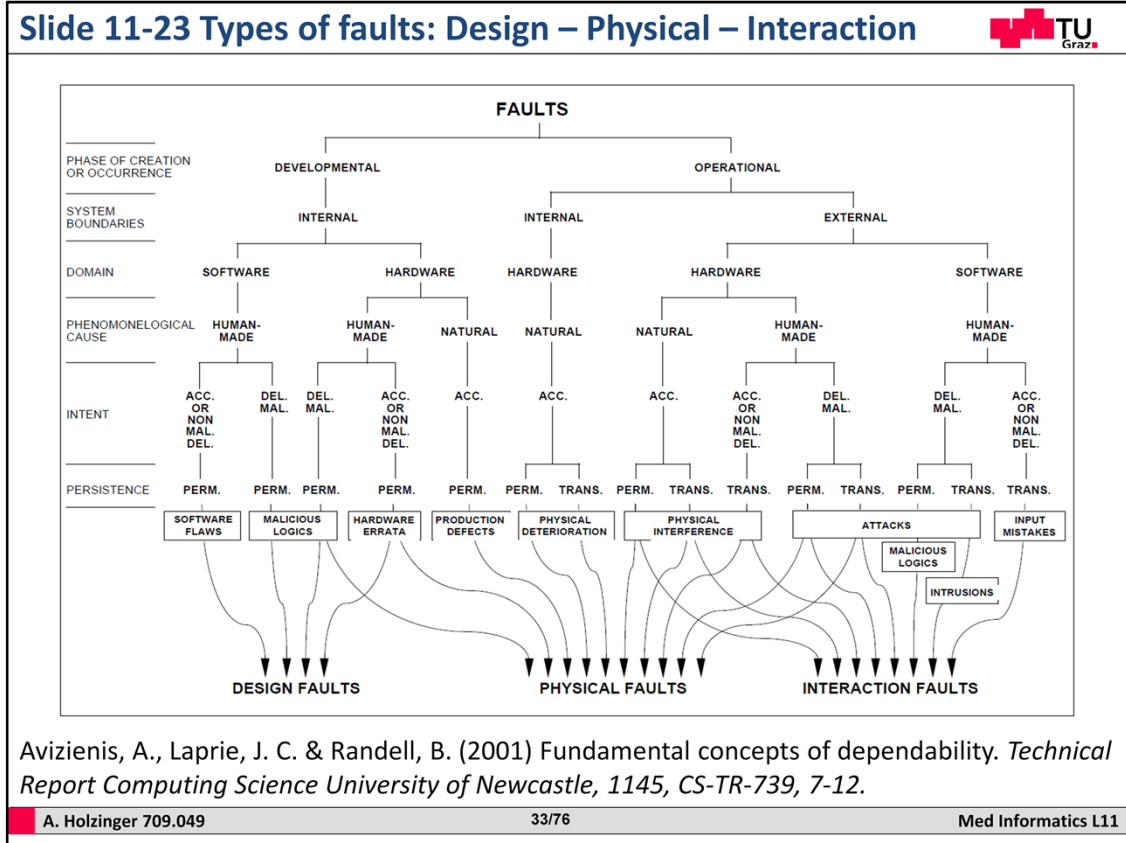
Avizienis, A., Laprie, J. C. & Randell, B. (2001) Fundamental concepts of dependability. *Technical Report Computing Science University of Newcastle, 1145, CS-TR-739, 7-12.*

A. Holzinger 709.049
32/76
Med Informatics L11

### Slide 11-22 Safety, Security -> Technical Dependability



Dependability consists of three parts: the threats to, the attributes of, and the means by which dependability is attained, as shown in this slide.

Computing systems are characterized by five fundamental properties: functionality, usability, performance, cost, and dependability. Dependability of a computing system is the ability to deliver service that can justifiably be trusted. The trust-factor is perceived by the users (remember the Previous Exposure to Technology, PET-Factor (Holzinger, Searle & Wernbacher, 2011)), and a user is another system (human) that interacts with the former at the service interface. The function of a system is what the system is intended to do, and is described by the functional specification. Correct service is delivered when the service implements the system function. A system failure is an event that occurs when the delivered service deviates from correct service. A failure is thus a transition from correct service to incorrect service, i.e., to not implementing the system function. The delivery of incorrect service is a system outage. A transition from incorrect service to correct service is service restoration. Based on the definition of failure, an alternate definition of dependability, which complements the initial definition in providing a criterion for adjudicating whether the delivered service can be trusted or not: the ability of a system to avoid failures that are more frequent or more severe, and outage durations that are longer, than is acceptable to the user(s). In the opposite case, the system is no longer dependable: it suffers from a dependability failure, that is a meta-failure (Avizienis, Laprie & Randell, 2001).



### Slide 11-23 Types of faults: Design – Physical – Interaction

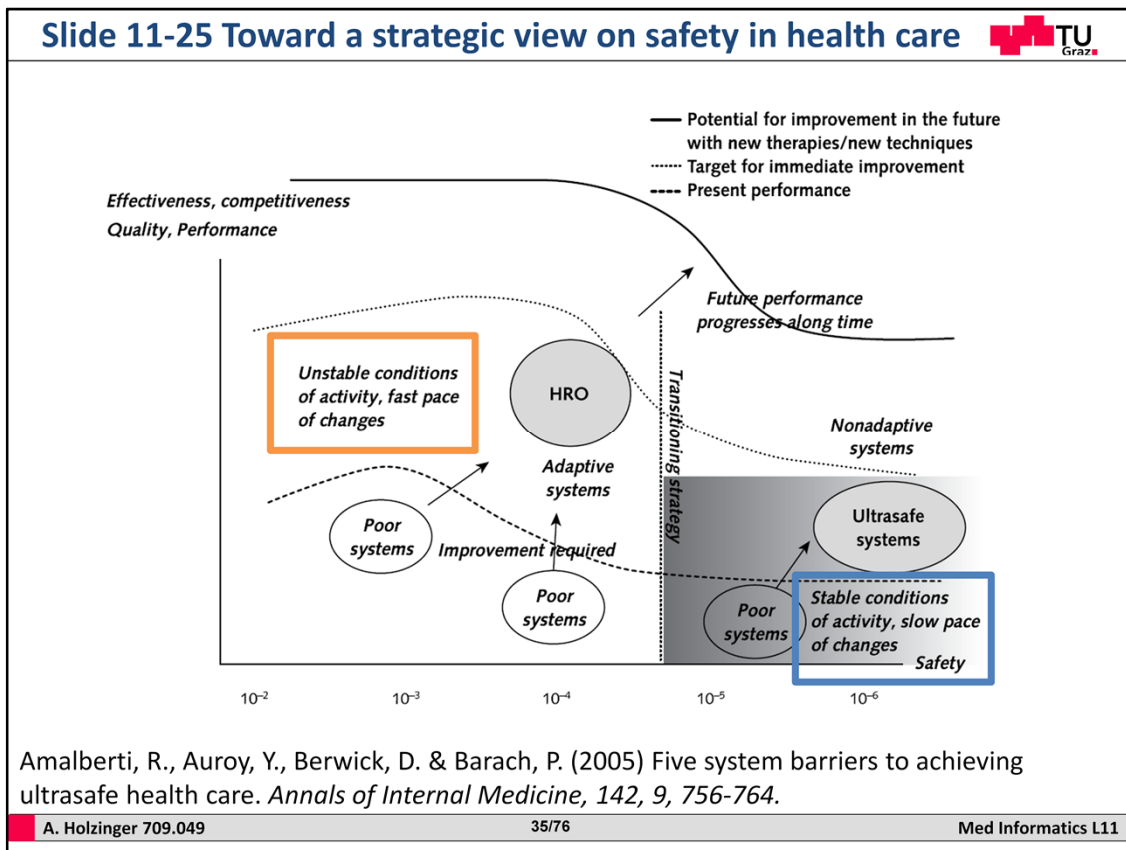
Combining the elementary fault classes leads to the tree in this slide: The leaves of the tree lead into three major fault classes for which defenses need to be devised: design faults, physical faults, interaction faults. The boxes in this slide point at generic illustrative fault classes. Non-malicious deliberate faults can arise during either development or operation. During development, they result generally from tradeoffs, either a) aimed at preserving acceptable performance and facilitating system utilization, or b) induced by economic considerations; such faults can be sources of security breaches, in the form of covert channels. Non-malicious deliberate interaction faults may result from the action of an operator either aimed at overcoming an unforeseen situation, or deliberately violating an operating procedure without having realized the possibly damaging consequences of his or her action. Non-malicious deliberate faults share the property that often it is recognized that they were faults only after an unacceptable system behavior, thus a failure, has ensued; the specifier(s), designer(s), implementer(s) or operator(s) did not realize that the consequence of some decision of theirs was a fault (Avizienis, Laprie & Randell, 2001).

Slide 11-24 A Two-Tiered System of Medicine			TU Graz
Category	Type of System		Amalberti et al. (2005)
	Ultrasafe System	High-Reliability Organization	
Example of industry	Nuclear power Commercial aviation Blood transfusion Anesthesiology* Radiotherapy	Military systems Chemical production Intensive care unit Surgical ward	 
Safety goals	Safety first Quality of work preserved against unacceptable pressure	Production first (imposed) Degree of safety as high as possible for the imposed level of performance	
Safety level (in terms of risk per exposure)	Better than $1 \times 10^{-5}$ , possibly $1 \times 10^{-6}$	Better than $1 \times 10^{-4}$	
Stability of the process	Well-codified and delineated area of expertise Ultradominant, rule-based behavior Consistent recruitment of patients (flow and quality)	Broad area of expertise Frequent knowledge-based behavior Unstable recruitment of patients (flow and quality)	
Complexity of expertise required	Limited complexity  Actors are requested to follow procedure Equivalent actors	Potential complexity; severe and abnormal cases are challenging  Reluctance to simplify Deference to expertise of individual experts	
Situational awareness	Good at the managerial level	Good among all actors, whatever their role and status	
Supervision	Inside (team) and outside supervision and control (black boxes)	Inside supervision and mutual control (team supervision)	
Teamwork	Effective teamwork and communication, resulting in good task sharing, controls, and collective routines	Effective teamwork and communication, with special attention to safe adaptation to the range of individual experts	
distinction between a limited number of clinical domains that can achieve ultrasafety and sectors in which a certain level of risk is inherent – and cannot be reduced!			
A. Holzinger 709.049		34/76	Med Informatics L11

### Slide 11-24 A Two-Tiered System of Medicine

This table by (Amalberti, Auroy, Berwick & Barach, 2005) show a detailed comparison of these 2 possible tiers of health care. Physician training would have to accommodate this 2-tiered approach, and patients would have to understand that aggressive treatment of high-risk disease may require acceptance of greater risk and number of medical errors during clinical treatment.






### Slide 11-25 Toward a strategic view on safety in health care

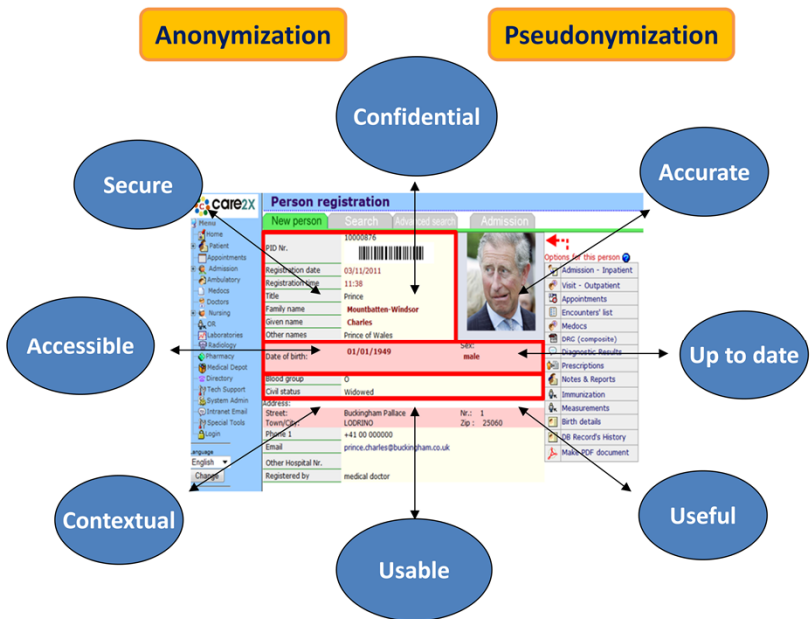
An improved vision by leadership of the safety and dangers of health care is needed to optimize the risk–benefit ratio. Stratification could lead to 2 tiers or “speeds” of medical care, each with its own type and level of safety goals. This 2-tier system could distinguish between medical domains that are stable enough to reach criteria for ultrasafety and those that will always deal with unstable conditions and are therefore inevitably less safe. For medicine, high-reliability organizations may offer a sound safety model and High-reliability organizations are those that have consistently reduced the number of expected or “normal” accidents (according to the normal accident theory) through such means as change to culture and technologic advances, despite an inherently high-stress, fast-paced environment (Amalberti, Auroy, Berwick & Barach, 2005).

# Data ...

Ok, now lets focus on data issues



**Slide 11-26 Requirements of an electronic patient record** 



**Anonymization** **Pseudonymization**

**Confidential** **Accurate** **Up to date** **Useful** **Usable** **Contextual** **Accessible** **Secure**

**Person registration**

care2X

New person Search Advanced search Admission

ID Nr. 10000816

Registration date 03/11/2011

Registration time 11:38

Title Prince

Family name Mountbatten Windsor

Given name Charles

Other names Prince of Wales

Date of birth 01/01/1949

Sex male

SSC group 0

Civil status Widowed

Address Buckingham Palace, London, W1 00 000000

Nr. 1

Zip 25000

Street Buckingham Palace

Town/City London

Phone 1

Email prince.charles@buckingham.co.uk

Other Hospital Nr.

Registered by medical doctor

Options for the person

Admission - Inpatient

Visit - Outpatient

Appointments

Encounters' list

Medics

Diagnosis Results

Prescriptions

Notes & Reports

Immunization

Measurements

Birth details

MR Record's History

Download PDF document

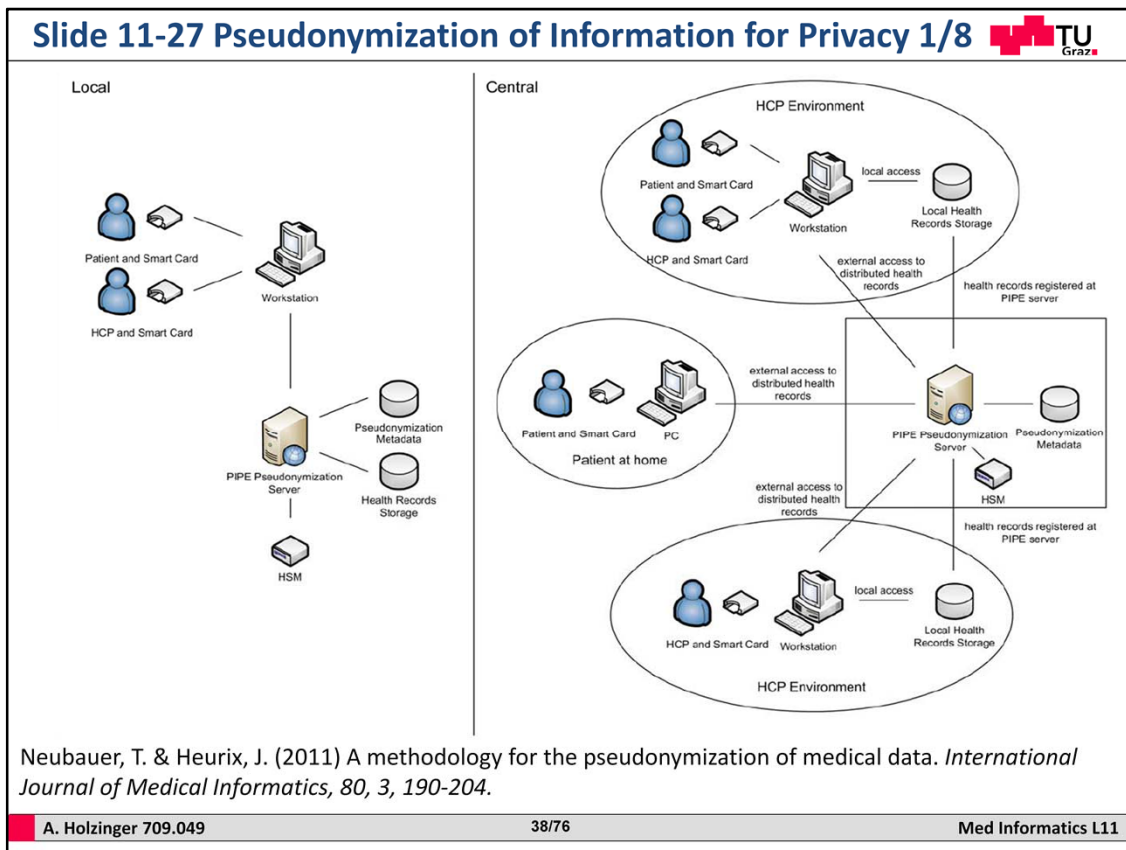
Anonymization: Personal data cannot be re-identified (e.g. k-Anonymization)  
Pseudonymization: The personal data is replaced by a "pseudonym", which allows later tracking back to the source data (re-identification)

A. Holzinger 709.049 37/76 Med Informatics L11

## Requirements of an electronic patient record

Remember the requirements to a patient record from the viewpoint of ensuring privacy: The patient data must be confidential, secure and safe, while at the same time must be usable, useful, accurate, up-to-date and accessible.

Security issues are crucial in a number of machine learning applications, especially in scenarios dealing with human activity rather than natural phenomena (e.g., information ranking, spam detection, malware detection, etc.). In such cases, learning algorithms may have to cope with manipulated data aimed at hampering decision making. Although some previous work addressed the issue of handling malicious data in the context of supervised learning, very little is known about the behavior of anomaly detection methods in such scenarios.



An excellent paper by (Neubauer & Heurix, 2011) shall provide a good teaching example, in the following consisting of 8 slides.

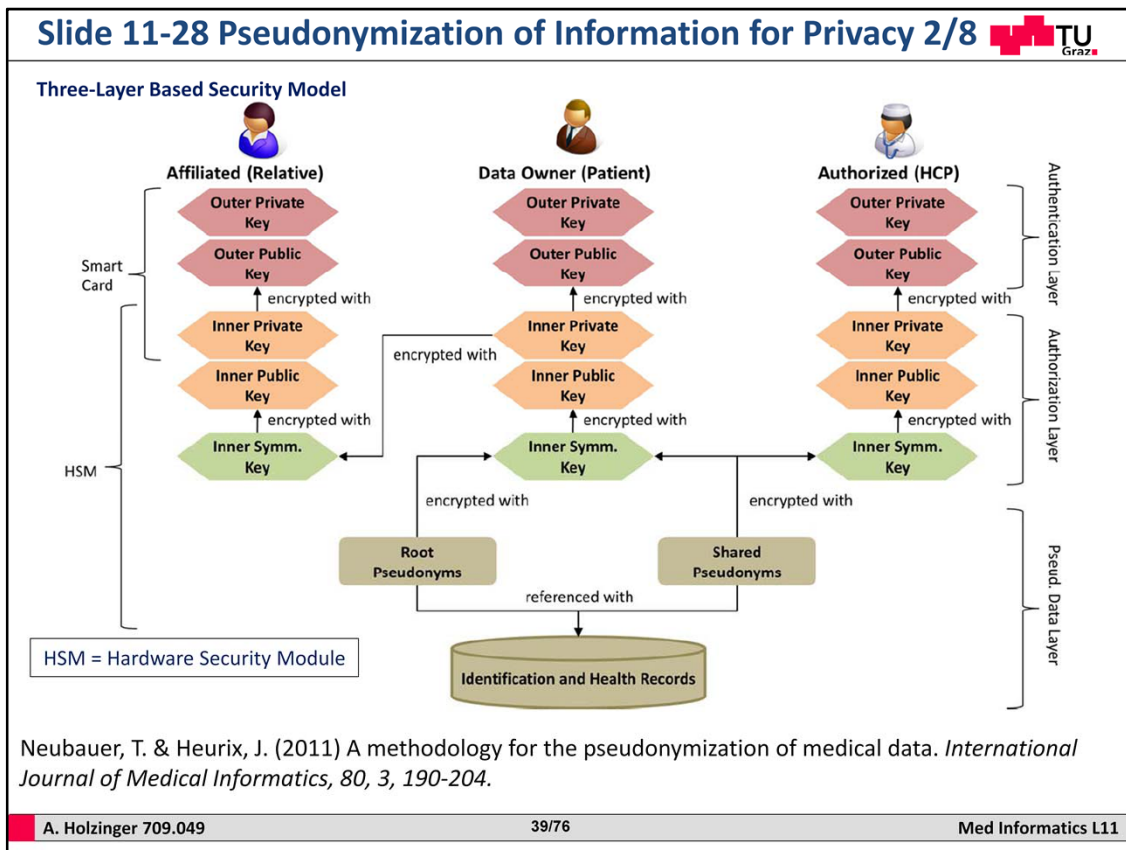
Protection of the patients' data privacy can be achieved with two different techniques, anonymization and encryption, which unfortunately both suffer from major drawbacks: While anonymization – the removal of the identifier from the medical data – cannot be reversed and therefore prevents primary use of the records by health care providers who obviously need to know the corresponding patient (as a minor point, patients cannot benefit from the results gained in clinical studies because they cannot be informed about new findings etc.), encryption of the medical records prevents them from being used for clinical research (secondary use of clinical data).

In this slide we see two separate health care provider environments where the individual workstations have direct access to their local data repositories. Via the pseudonymization service, the health care providers are able to access records of other domains if they are explicitly authorized to do so. In this scenario, the patient also has the opportunity to retrieve the records at home.

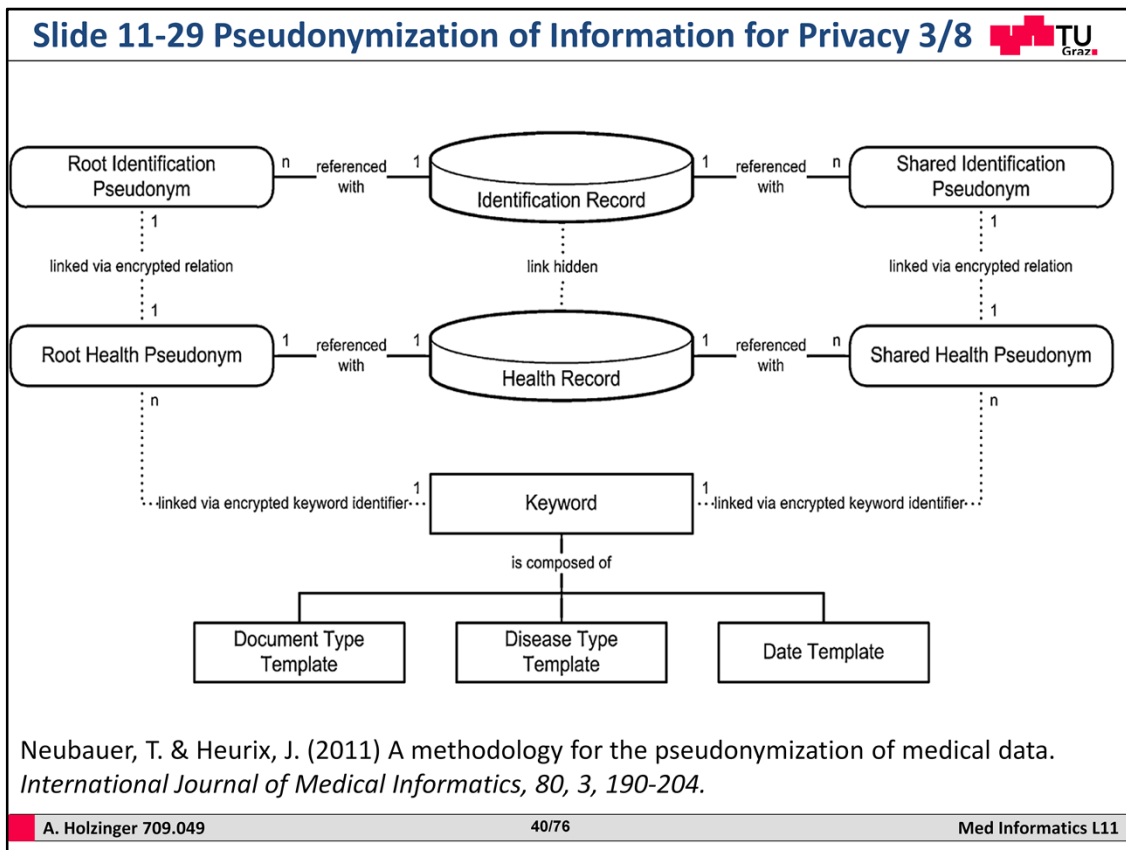
*At least without the explicit permission of the patient, who has to decrypt the data and, in doing so, reveals her identity. Considering that some medical records can be very large, encryption can also be seen as a time-consuming operation. A method that resolves these issues is pseudonymization, where identification data is transformed and then replaced by a specifier that cannot be associated with the identification data without knowing a certain secret. Pseudonymization allows the data to be associated with a patient only under specified and controlled circumstances.*

Aimed to provide a pseudonymization service, PIPE (Pseudonymization of Information for Privacy in e-Health) can be applied to different scenarios: In the local scenario, the PIPE server pseudonymizes only records stored in the local (health) data repository and makes them available to a local (health care provider's) workstation where both patient and health care provider interact with the pseudonymization server as part of a health care provider environment (e.g., with a hospital information system). In an alternative central scenario, the PIPE pseudonymization server is responsible for providing linking information to different health records stored at distributed

locations. In the slide two separate health care provider environments exist where the individual workstations have direct access to their local data repositories. Via the pseudonymization service, the health care providers are able to access records of other domains if they are explicitly authorized to do so. In this scenario, the patient also has the opportunity to retrieve the records at home.

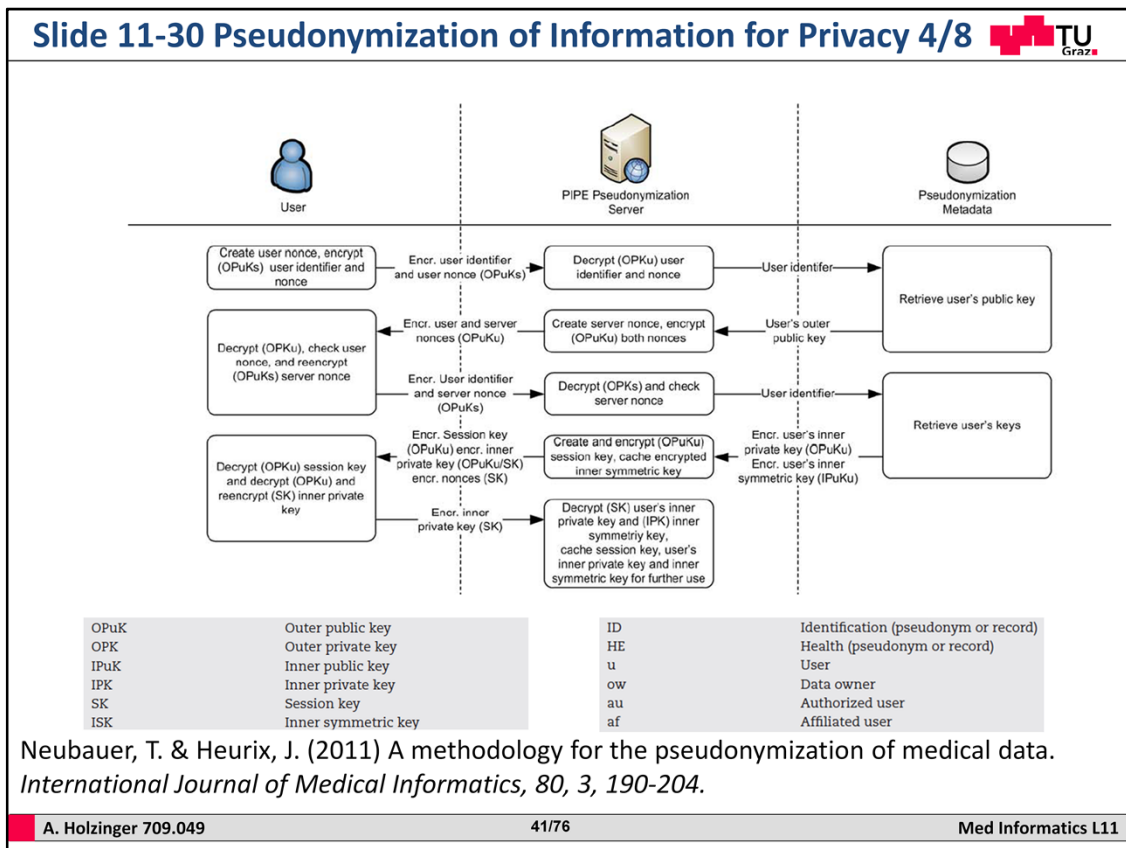


The PIPE protocol uses a combination of symmetric and asymmetric cryptographic keys to realize a logical multi-tier hull model with three different layers – which we can see in this slide, where each layer is responsible for one step in the data access process. The user has to pass all layers in order to retrieve the actual health data records. The outer public and outer private keys form the outer layer, the authentication layer, which is responsible for unambiguously identifying the corresponding user. Together with the user's identifier, the outer private key represents the authentication credentials, which are stored along with the server's public key on the user's smart card. In combination with the correct PIN, the smart card provides two-factor authentication, where the authentication procedure involves both the user's and the PIPE server's outer keypair; the user's identifier, and two randomly selected challenges. The middle layer, the authorization layer, consists of the user's inner asymmetric keypair and the inner symmetric key. While the user's outer private key is created on the smart card when the card is issued to the user and never actually leaves the card, the other keys are stored in the pseudonymization database where the secret keys are stored encrypted: the inner symmetric key is encrypted with the inner public key, while the inner private key is encrypted with the outer public key (Neubauer & Heurix, 2011).



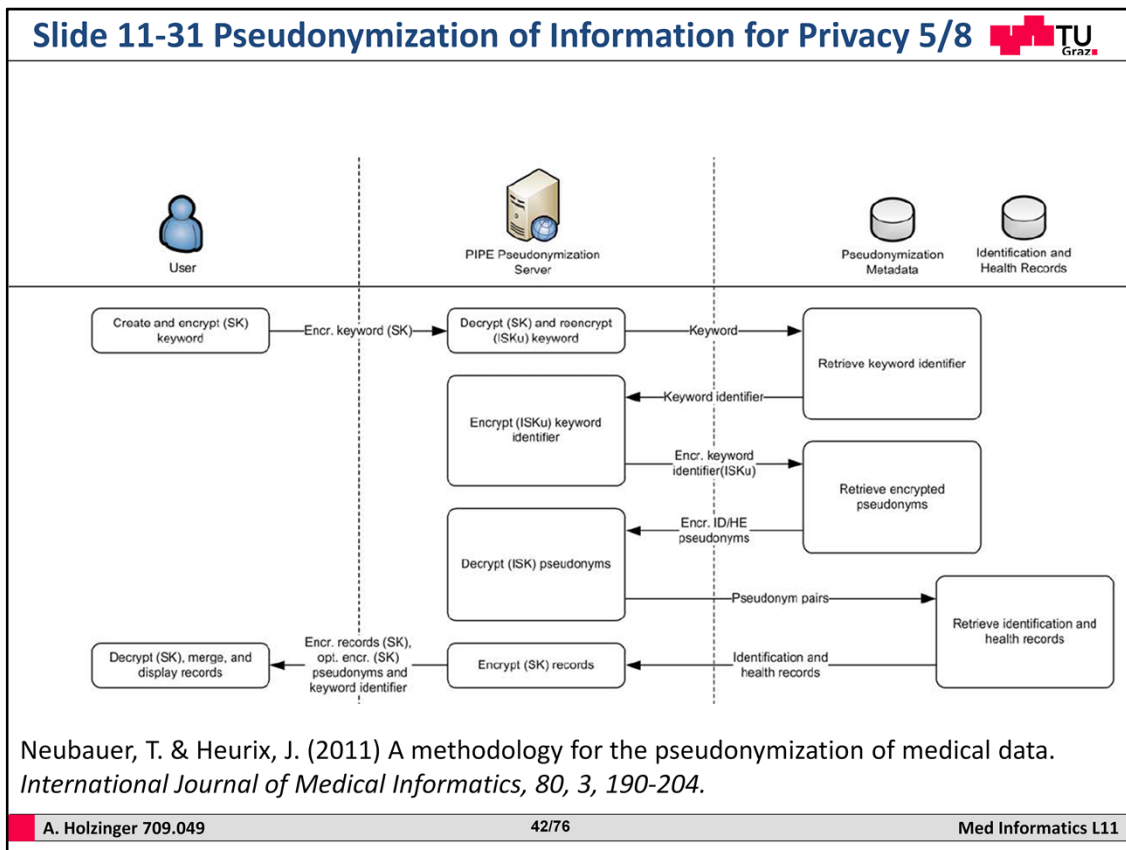
Here in this slide we see the data model.

The identification and health pseudonyms always form a 1:1 relationship and are referenced with their corresponding document type where this reference is stored in cleartext (record/pseudonym mapping). The link between the identification and health pseudonyms is stored encrypted with the user's inner symmetric key (pseudonym/pseudonym mapping): while the root pseudonyms are encrypted with the data owner's (patient's) inner symmetric key only, the shared pseudonyms are encrypted with both the data owner's and the authorized user's (health professional's) inner symmetric key so that both users are able to decrypt them using their corresponding ciphertexts. The link between the identification and health record is hidden and represented by the link between identification and health pseudonyms. Each health record is assigned exactly one root health pseudonym while each identification record has multiple root pseudonyms, depending on the number of health records, due to the 1:1 relationship. The health record is assigned a number of shared health pseudonyms according to the number of individual authorizations for that particular health record.

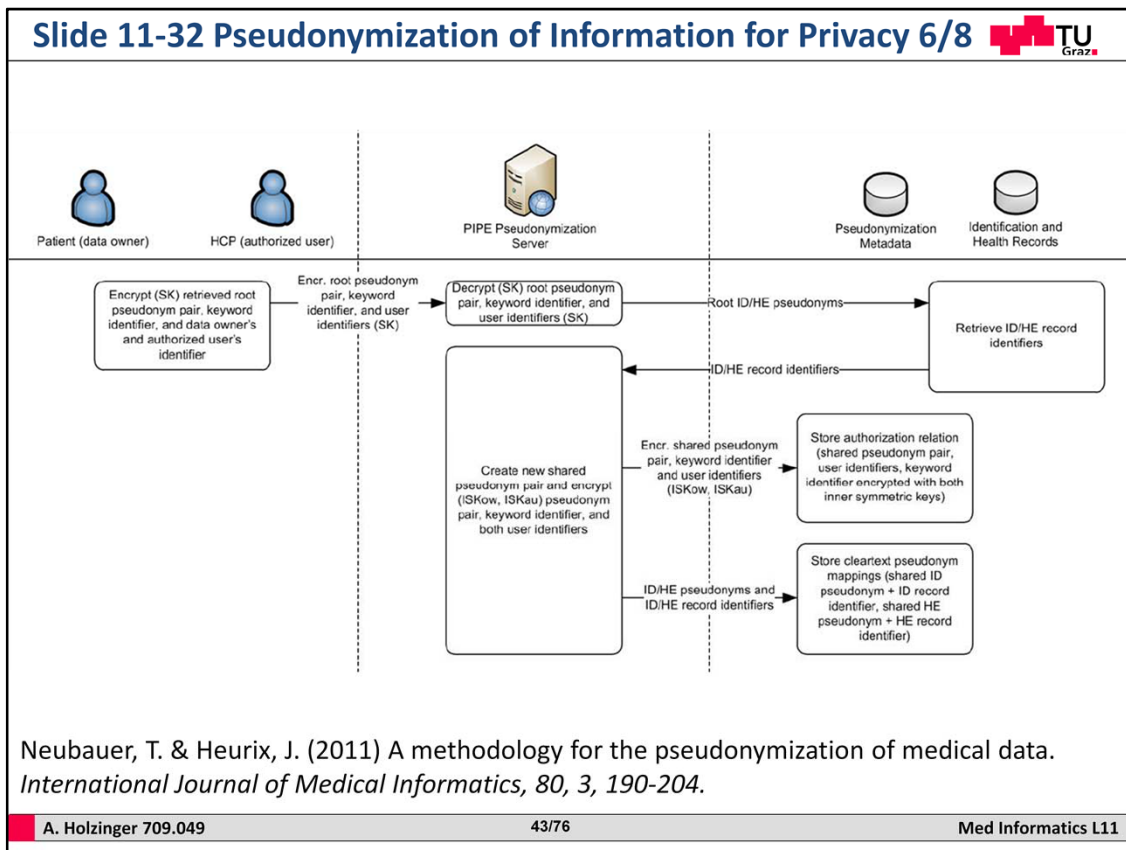


This slide shows the User authentication, which involves the mutual authentication of the user using the smart card and the server, involving their outer keypair and two nonces (randomly selected numbers used once) as user/server challenges. Once both identities are confirmed, the user's inner private key is retrieved from the pseudonymization database and transferred to the user's smart card to be decrypted with the user's outer private 3 Transport Layer Security. key. With the decrypted inner private key, the user's inner symmetric key can be decrypted within the HSM at the pseudonymization server and be cached for further operations along with the user's inner private key. In addition, a session key is generated at the HSM and securely (via encryption) transported to the user's smart card so that the key appears in cleartext only on the smart card and HSM (Neubauer & Heurix, 2011).

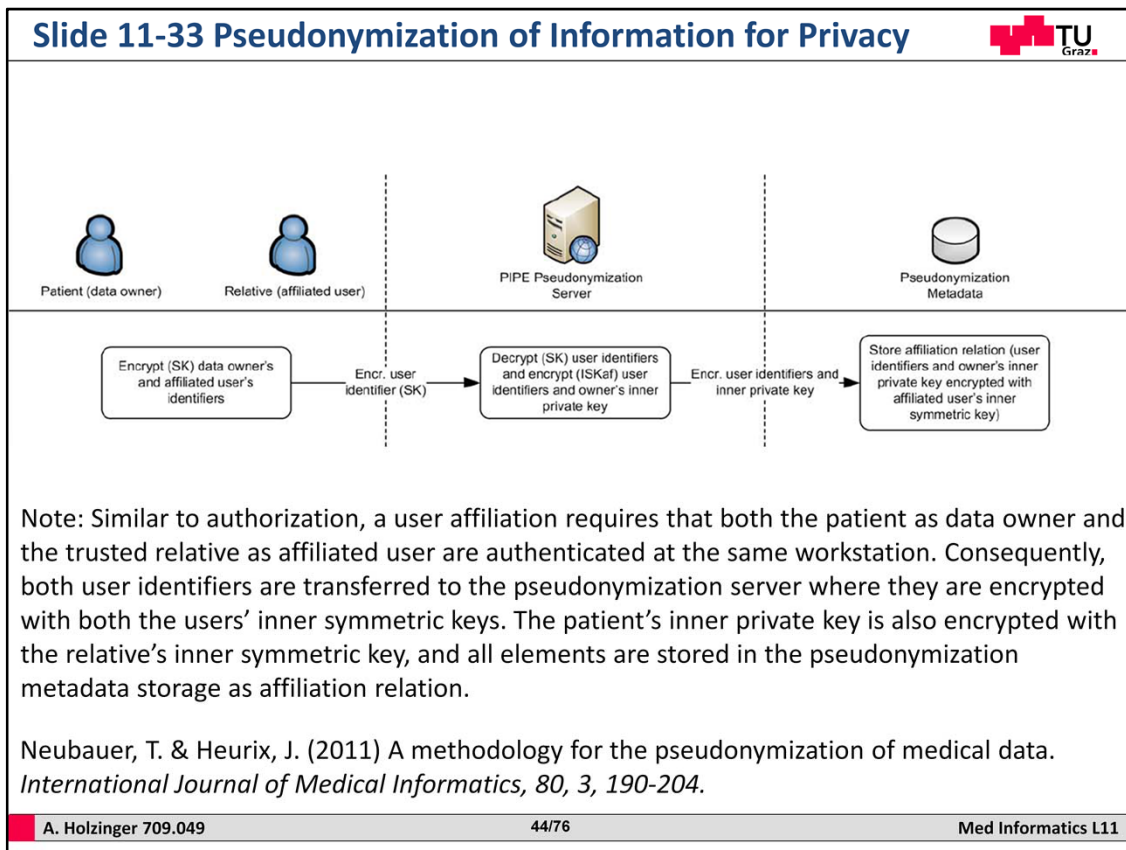




To retrieve a particular health record, the user first needs to query for the particular encrypted pseudonyms by creating a keyword using the keyword templates, retrieving the corresponding keyword identifier, and querying for the encrypted identifier to find matching encrypted pseudonyms, i.e., the encrypted pseudonym mappings associated with the encrypted keyword identifier. The pseudonym pairs are then decrypted with the user's inner symmetric key and the plaintext pseudonyms then used to retrieve the corresponding identification and health records, which are transferred to the user to be displayed (possibly merged). Optionally, the pseudonyms and keyword identifier are also transferred to the user (root pseudonyms for authorizations). The record retrieval procedure is the same for the patient as data owner, health care provider as authorized user, and relative as affiliated user, with the difference that the patient and relative both query for the patient's root pseudonyms, while the health care provider relies on the shared pseudonyms (Neubauer & Heurix, 2011).

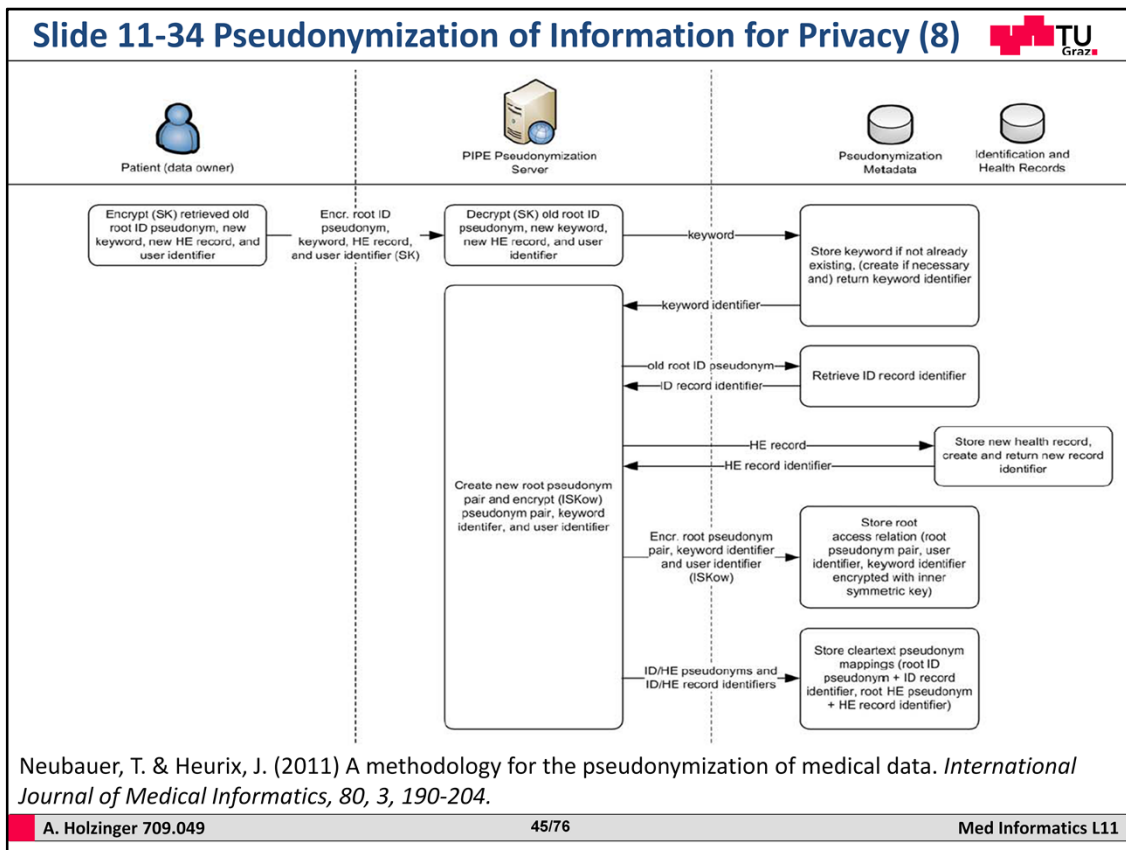


To provide a trusted health care provider with the knowledge of the link between the patient's identification record and a particular health record, a new shared pseudonym pair is created as authorization relation. The patient first has to retrieve the root pseudonym pair and keyword identifier corresponding to the health record he or she intends to share with the health care provider. Furthermore, both the patient as data owner and the health care provider as authorized user have to be authenticated at the same workstation so that both user identifiers are available at the client side, while both inner symmetric keys are cached at the HSM of the pseudonymization server. The root pseudonym pair is then transferred to the pseudonymization server along with both user identifiers and the keyword identifier, and the corresponding record identifiers retrieved using the cleartext record/pseudonym mappings. The server then randomly selects a new shared pseudonym pair, which is first encrypted with both users' inner symmetric keys (along with both identifiers and the keyword identifier) and then stores them in the database as authorization relation. Finally, the cleartext pseudonyms are then referenced with the retrieved record identifiers to create two new record/pseudonym mappings (Neubauer & Heurix, 2011).



### Slide 11-33 Pseudonymization of Information for Privacy 7/8

As with authorizations, a user affiliation requires that both the patient as data owner and the trusted relative as affiliated user are authenticated at the same workstation. Then both user identifiers are transferred to the pseudonymization server where they are encrypted with both users' inner symmetric keys. In addition, the patient's inner private key is also encrypted with the relative's inner symmetric key, and all elements are stored in the pseudonymization metadata storage as affiliation relation (Neubauer & Heurix, 2011).



Finally, from the viewpoint of the patient as data owner, health data storage first requires that an 'old' root identification pseudonym is retrieved as reference to the identification record. Furthermore, the patient creates a new keyword and enters the new health record into the workstation. Then the pseudonym, new keyword, new health record, and user identifier are transferred to the pseudonymization server, where the keyword is stored (and its identifier determined by the database engine) and the identification record identifier retrieved. The new record is stored in the health records database and its record identifier returned to the server. Then, the server creates a new root pseudonym pair and stores it encrypted with the keyword identifier and user identifier as root access, as well as the cleartext record/pseudonym mappings (Neubauer & Heurix, 2011).

**Slide 11-35 Example: private personal health record**

<http://healthbutler.com/>

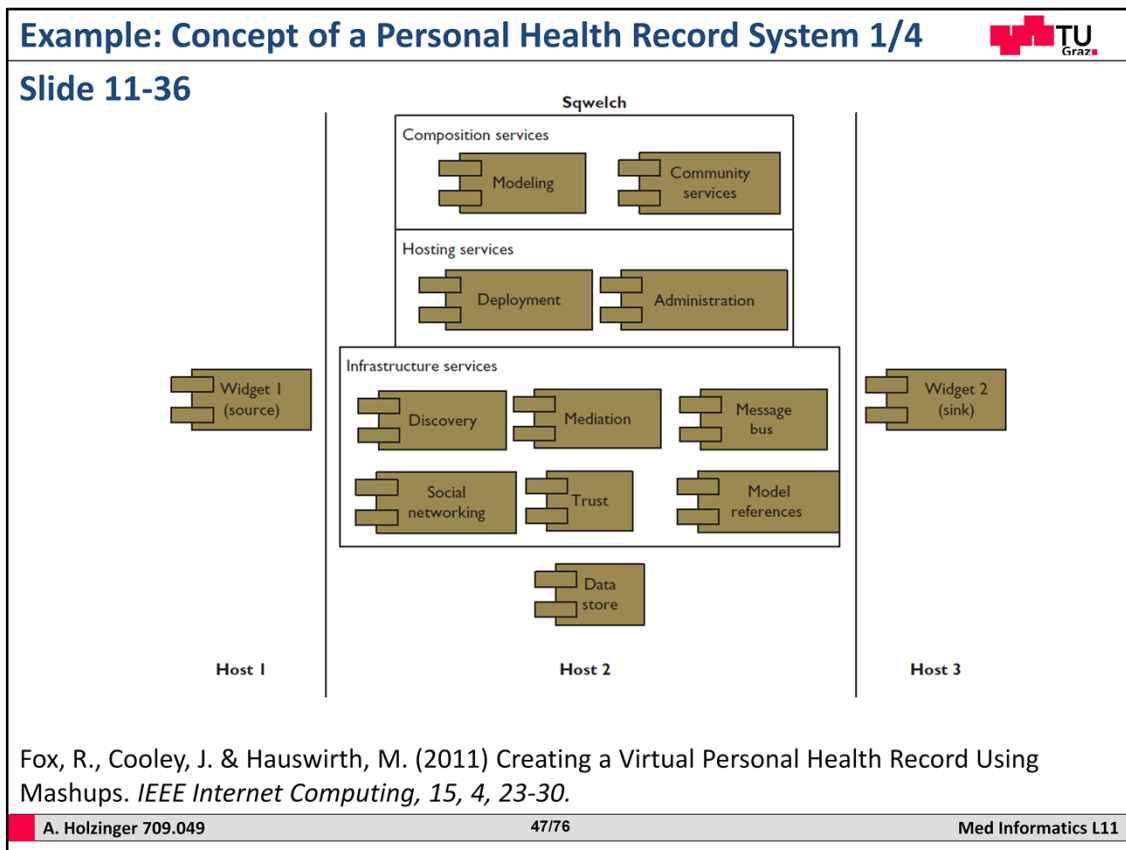
<https://www.healthcompanion.com>

A. Holzinger 709.049 46/76 Med Informatics L11

### Slide 11-35 Example: private personal health record

As the awareness of patients for their medical data increases, there is a trend of private personal health records, sometimes called health vaults. An example can be seen in <http://healthbutler.com>

In the following four slides we look at the technological concept of such a personal health record system. In this concept we will get to know a very interesting concept: Mashups.



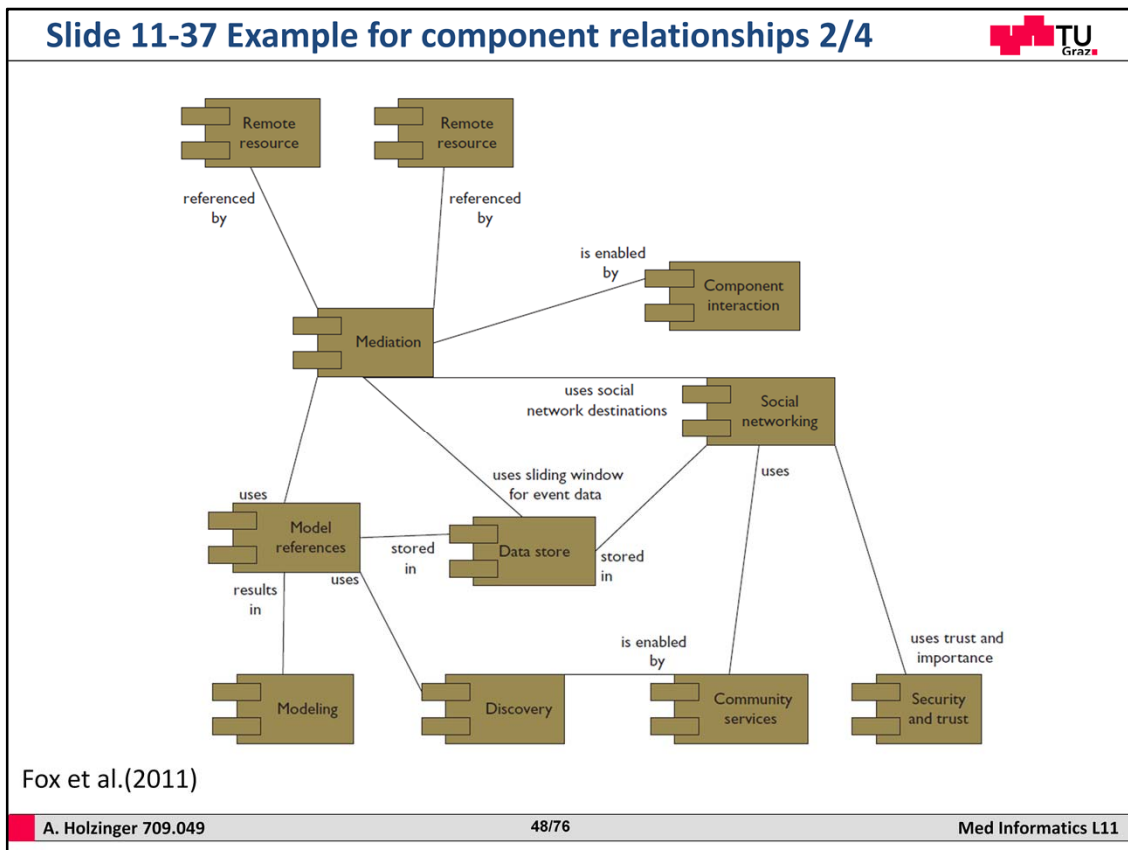
### Slide 11-36 Example: Concept of a Personal Health Record System 1/4

PHRs that use centralized data stores do not offer stakeholders a choice in services, data storage, or user requirements. However, various stakeholders have varying skills, requirements, and responsibilities, which a single application can not satisfy. Consequently, personalization is required where such a heterogeneous mix of stakeholders exists. The concept of Mashups (Auinger et al., 2009) let users create applications to suit their individual requirements. End users can use mashup makers to integrate various resources. Mashup makers let users create personalized applications with lower costs than traditional integration projects, in which a single application must incorporate many users' needs. As the explosion of Web mashups available on the Programmable Web ([www.programmableweb.com](http://www.programmableweb.com)) show, many users are finding new and diverse ways to satisfy individual requirements.

This slide shows the conceptual architecture of a system called Sqwelch (Fox, Cooley & Hauswirth, 2011): Within the architecture, there are three components:

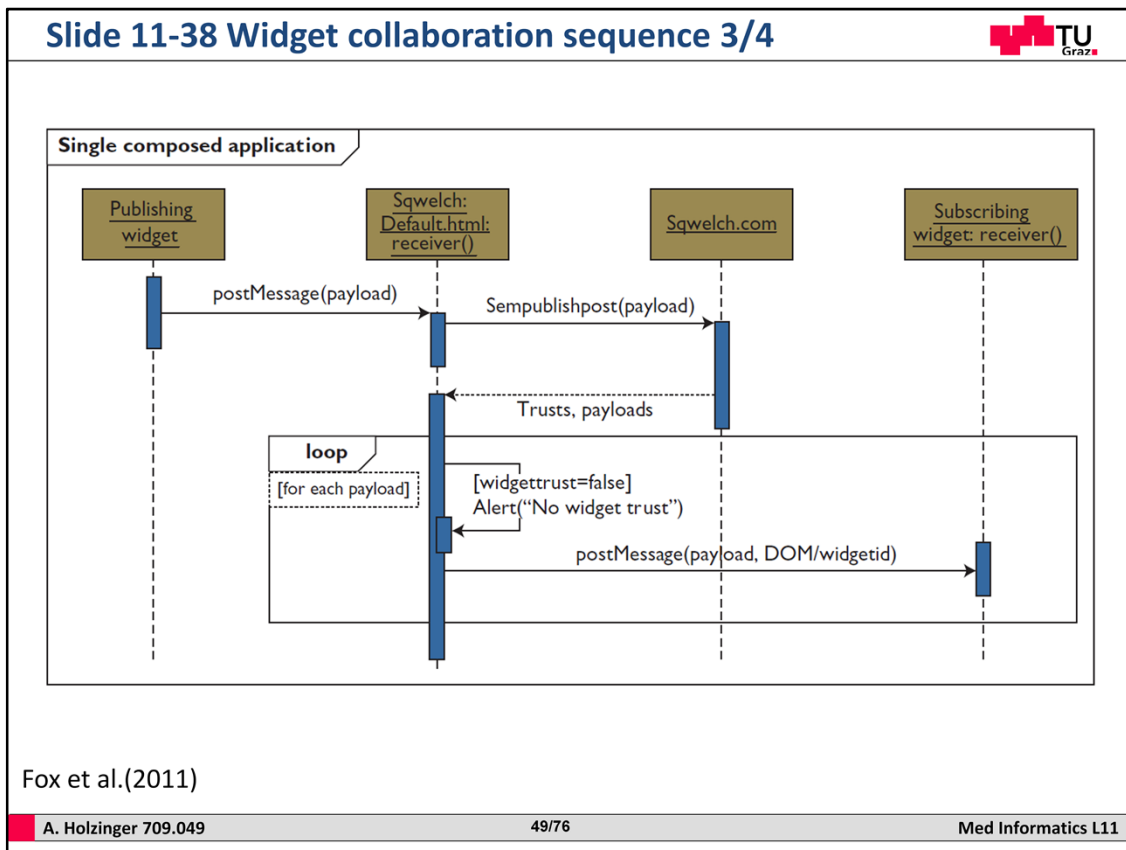
- 1) Composition services provide mechanisms for modeling widgets and engaging with the stakeholder community in developing mashups.
- 2) Hosting services provide mechanisms for managing the environment, customizing mashup containers, and deploying mashups.
- 3) Infrastructure services form the basis of the mashup maker, including discovery services, social networking capabilities, security and trust, widget interaction, and management.





### Slide 11-37 Example for component relationships 2/4

Here we see the Sqwelch component relationships: The components work in cooperation and fulfill specific roles to enable heterogeneous widgets and users to collaborate in a trusted way: When registering widgets, developers create model references that are stored for future use in the discovery and mediation components. During a mashup's execution, the social networking component determines the destinations for data if users are collaborating, which in turn uses trust and importance as a means of controlling data access. Model references are used to transform data, and component interaction is provided as publish-subscribe to loosely couple the remote resources (Web widgets) (Fox, Cooley & Hauswirth, 2011).



### Slide 11-38 Widget collaboration sequence 3/4

Here we see the Widget collaboration sequence. Widgets communicate with the Sqwelch server using HTML 5 standards. Sqwelch alerts users if widgets aren't trusted.

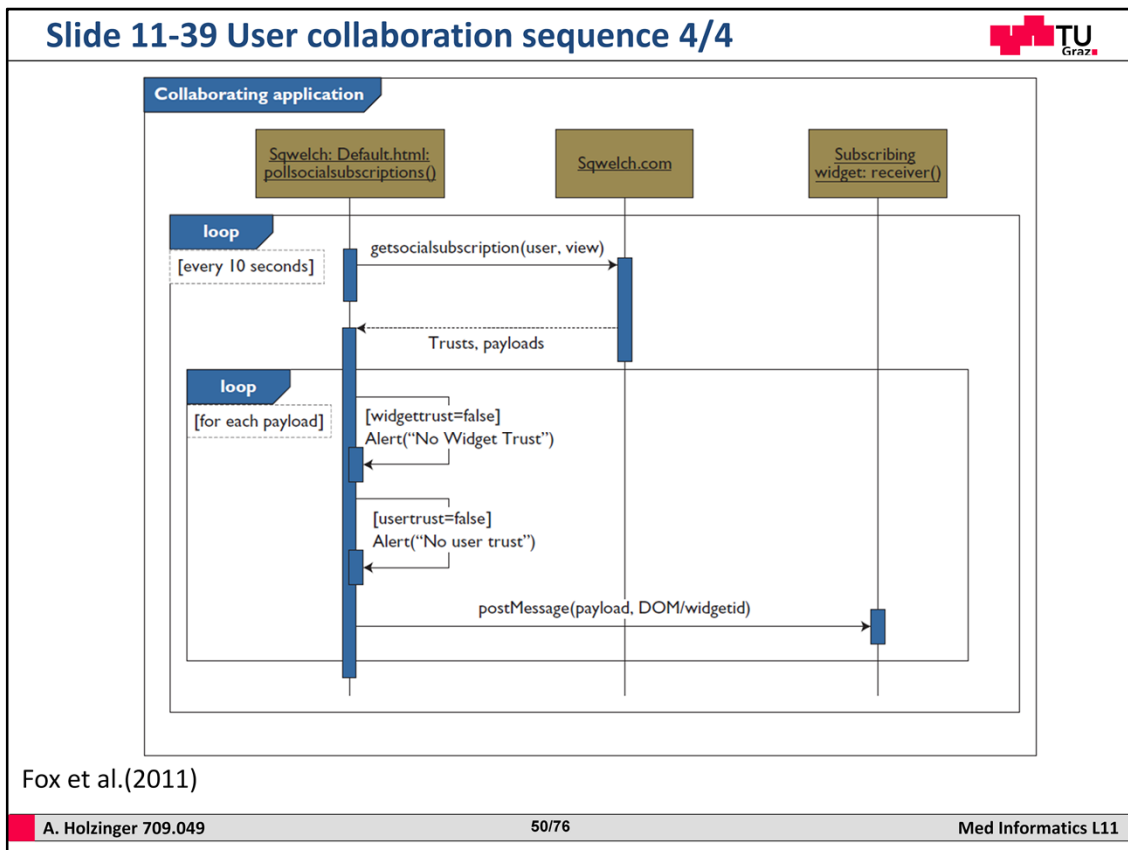
The diagram shows the calls to be made by widgets, the execution host (Sqwelch default.html), and the server (Sqwelch. com) in enabling trusted publish-subscribe between heterogeneous widgets. In our example, the publishing widget could be the sensor viewer widget and the subscribing widget could be the sensor filter widget. We must consider some important points (Fox, Cooley & Hauswirth, 2011):

1) The HTML 5 `postMessage` syntax is used to publish data payloads from widgets and from the Sqwelch main page. HTML 5 event listener functions are required in subscribing widgets to listen for incoming payloads.

2) The payloads `sempublishpost` returns are those expected by the subscribing widgets (payload), based on the original published payload.

3) Payload as received by the subscribing widget will be a combination of default values the user specifies and real values, depending on the importance associated with the real data and the trust specified for the subscribing widget.

4) If the widget isn't trusted, Sqwelch alerts the user and provides a view of the data elements the subscribing widget has requested. This will happen only once for each widget in the current session.



### Slide 11-39 User collaboration sequence 4/4

Finally, here the User collaboration sequence is depicted: Polling is used by subscribing mashups deployed by caregivers to retrieve data published by the patient. Sqwelch alerts the caregiver if the patient doesn't trust him or her. The sequences include (Fox, Cooley & Hauswirth, 2011):

- 1) The polling code is run on the hosting mashup webpage, retrieving data for all social widgets in the current page using getsocialsubscriptions.
- 2) The hosting mashup webpage returns with the latest heart rate readings for Mary.
- 3) If Mary doesn't trust either the widget or John, the payload will contain static, user-defined information, and Mary will be alerted.



# Machine Learning and Data Privacy ...

Ok, now lets now focus on data privacy issues – spy fridges

Trust plays an increasingly important role


We are surrounded by zillions of computing devices, sensors etc.

RFID tags, smart dust, sensor networks, cameras, etc.

Embedded in devices for everyday use, or even human bodies



Privacy has become a growing concern, due to the massive increase in personal information stored in electronic databases, such as medical records, financial records, web search histories, and social network data. Machine learning can be employed to discover novel population-wide patterns, however the results of such algorithms may reveal certain individuals' sensitive information, thereby violating their privacy. Thus, an emerging challenge for machine learning is how to learn from data sets that contain sensitive personal information.

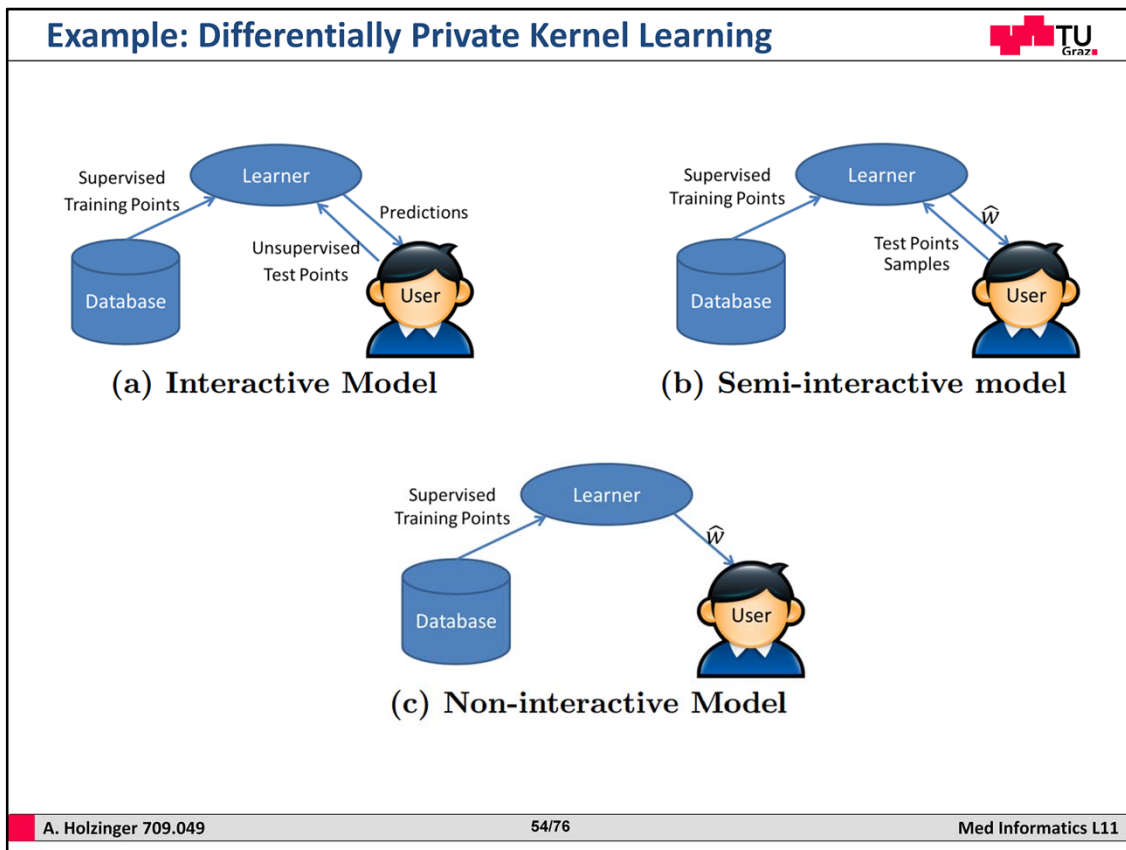
Privacy Principles		
<ul style="list-style-type: none"><li>▪ Lawfulness and fairness</li><li>▪ Necessity of data collection and processing</li><li>▪ Purpose specification and purpose binding</li><li>▪ There are no "non-sensitive" data</li><li>▪ Transparency</li><li>▪ Data subject's right to information correction, erasure or blocking of incorrect/ illegally stored data</li><li>▪ Supervision (= control by independent data protection authority) &amp; sanctions</li><li>▪ Adequate organizational and technical safeguards</li> <li>▪ <b>Privacy protection can be undertaken by:</b></li><li>▪ Privacy and data protection laws promoted by government</li><li>▪ Self-regulation for fair information practices by codes of conducts promoted by businesses</li><li>▪ Privacy-enhancing technologies (PETs) adopted by individuals</li><li>▪ Privacy education of consumers and IT professionals</li></ul>		
<p>Fischer-Hübner, S. 2001. IT-security and privacy: design and use of privacy-enhancing security mechanisms, Springer.</p>		
A. Holzinger 709.049	53/76	Med Informatics L11

Of course there are many threats to break privacy

Pseudonyms

- i) Self-generated pseudonyms
- ii) Reference pseudonyms
- iii) Cryptographic pseudonyms
- iv) One-way pseudonyms





Differential privacy = aims to provide means to maximize the accuracy of queries from statistical databases while minimizing the chances of identifying its records. Here we have three parties: 1) user, 2) data, 3) trusted ML; ml learns from the dataset, user goal is to obtain labels for the test set, and the ML goal is to provide predictions – now it is important not to violate privacy! In (a) the user sends the test data to the learner and gets back predictions (human-in-the-loop); (b) the user sends a small subset of the test set and the learner sends a Private Vector  $\hat{w}$  – guaranteed with similar predictions as on the test set; c learner sends the user a private Vector  $w$  which contains similar predictions on all the points in the input space.

We consider the problem of differentially private kernelized learning and study it under three practical models. Our algorithms for the first two models are computationally efficient but for the third model they can have exponential time complexity for some kernel functions. Interactive: Our interactive model is useful for several learning tasks faced by online systems like ad-systems, recommendation systems. We provide an efficient algorithm that can accurately predict for exponentially many test points, in terms of error bound and training points. Semi-interactive: Our semi-interactive model is useful when public test sets are available. Here, we provide an efficient differentially private algorithm with additional generalization error that is independent of the dimensionality of the data. Non-interactive: Finally, we provide a privacy preserving algorithm with generalization error bound for the standard learning model but where kernel function is restricted to a function of low-dimensional vector spaces. Although our

algorithm for this setting might not be computationally efficient in general, but for the case of linear kernels we can prove it to be efficient.


Models for kernelized privacy preserving learning using kernel ERM. We have three parties: a dataset, a trusted learner and a user. Learner learns optimum ( $w$

) of the ERM using the training data from the dataset. User's goal is to obtain labels for its test set while learner's goal is to provide user with accurate predictions/model parameters without violating dataset's privacy. (a) Interactive Model: In this model, the user sends its test data to the learner for which it returns back accurate predictions without violating dataset's privacy. (b) Semi-interactive model: In this model, the user sends a small subset of its test set, and then learner sends a differentially private  $b w$  that is guaranteed to obtain similar predictions to  $w$

on user's test set. (c) Non-interactive Model: In this model, learner sends the user a differentially private  $b w$  that is expected to provide similar predictions to  $w$

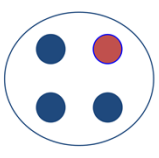
on all the points in the input space

## Simplest Privacy Metric

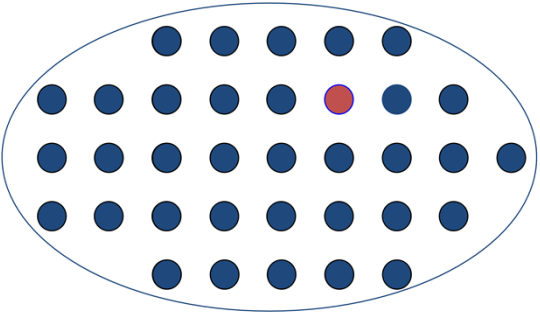


- The larger the set of indistinguishable entities, the lower probability of identifying any one of them

“Hiding in a crowd”



Less anonymous ( $1/4$ )



More anonymous ( $1/n$ )

Anonymity set A

$$A = \{(s_1, p_1), (s_2, p_2), \dots, (s_n, p_n)\}$$

$s_i$ : subject  $i$  who might access private data  
or:  $i$ -th possible value for a private data attribute

$p_i$ : probability that  $s_i$  accessed private data  
or: probability that the attribute assumes the  $i$ -th possible value

More details see: Bharat K. Bharava (2003), Purdue University

A. Holzinger 709.049
55/76
Med Informatics L11

Can be used to “anonymize” a selected private attribute value within the domain of all possible values

## Effective Anonymity Set Size



- Effective anonymity set size is calculated by

$$L = |A| \sum_{i=1}^{|A|} \min p_i \frac{1}{|A|}$$

Maximum value of L is |A| iff all  $p_i = 1/|A|$

L below maximum when distribution is skewed  
skewed when  $p_i$  have different values

Deficiency:

L does not consider violator's *learning* behavior

**Example: Entropy**

- Remember: Entropy measures the randomness (uncertainty) – here private data
- Violator gains more information -> entropy decreases!
- Metric: Compare the current entropy value with its maximum value and the difference shows how much information has been leaked
- Privacy loss  $D(A,t)$  at time  $t$ , when a subset of attribute values  $A$  might have been disclosed:

$$D(A,t) = H^*(A) - H(A,t) \quad H(A,t) = \sum_{j=1}^{|A|} w_j \left( \sum_{\forall i} (-p_i \log_2(p_i)) \right)$$

$H^*(A)$  – the maximum entropy

Computed when probability distribution of  $p_i$ 's is uniform

$H(A,t)$  is entropy at time  $t$

$w_j$  – weights capturing relative privacy “value” of attributes

## Example : k-Anonymization of Medical Data



**87 % of the population in the USA can be uniquely re-identified by Zip-Code, Gender and date of birth**

Hospital Patient Data

Birthdate	Sex	Zipcode	Disease
1/21/76	Male	53715	Flu
4/13/86	Female	53715	Hepatitis
2/28/76	Male	53703	Brochitis
1/21/76	Male	53703	Broken Arm
4/13/86	Female	53706	Sprained Ankle
2/28/76	Female	53706	Hang Nail

Voter Registration Data

Name	Birthdate	Sex	Zipcode
Andre	1/21/76	Male	53715
Beth	1/10/81	Female	55410
Carol	10/1/44	Female	90210
Dan	2/21/84	Male	02174
Ellen	4/19/72	Female	02237



Sweeney, L. 2002. Achieving k-anonymity privacy protection using generalization and suppression. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10, (05), 571-588.

The amount of patient-related data produced in today's clinical setting poses many challenges with respect to collection, storage and responsible use. For example, in research and public health care analysis data must be anonymized before transfer, for which the k-anonymity measure was introduced and successively enhanced by further criteria. As k-anonymity is an NP-hard problem, modern approaches make use of approximation as well as heuristics based methods. This talk will give a short introduction into anonymization and its criteria followed by an overview of methods & state-of-the-art algorithms to tackle the problem. I will demonstrate currently available tools and outline their strengths and weaknesses, before concluding the session by contemplating an interactive machine learning (iML) approach to the problem.



## Anonymization of Patient Data



- **K-Anonymity** ... not fully protected against attribute disclosure
- **L-Diversity** ... extension requiring that the values of all confidential attributes within a group of  $k$  sets contain at least  $l$  clearly distinct values
- **t-Closeness** ... extension requiring that the distribution of the confidential attribute within a group of  $k$  records is similar to the confidential attribute in the whole data set

K-Anonymity ... eg. If the values of confidential attributes are very similar in a group of  $k$  records which overlap quasi-identifier values

A release of data is said to have the  $k$ -anonymity property if the information for each person contained in the release cannot be distinguished from at least  $k-1$  individuals whose information also appear in the release.

L-diversity ... The  $l$ -diversity model is an extension of the  $k$ -anonymity model which reduces the granularity of data representation using techniques including generalization and suppression such that any given record maps onto at least  $l$  other records in the data. The  $l$ -diversity model handles some of the weaknesses in the  $k$ -anonymity model where protected identities to the level of  $k$ -individuals is not equivalent to protecting the corresponding sensitive values that were generalized or suppressed, especially when the sensitive values within a group exhibit homogeneity.


T-closeness ... at most distance  $t$  between both distributions This reduction is a trade off that results in some loss of effectiveness of data management or mining algorithms in order to gain some privacy. The  $t$ -closeness model extends the  $l$ -diversity model by treating the values of an attribute distinctly by taking into account the distribution of data values for that attribute.


### Three Examples of Freeware




- Argus: <http://neon.vb.cbs.nl/casc>
- ARX: <http://arx.deidentifier.org>
- sdcTable: <http://cran.r-project.org/web/packages/sdcTable/>


## Privacy Aware Machine Learning for Health Data Science






### #1: OPEN DATA







- – Production of Open Data Sets
- – Design of Synthetic data sets
- – Privacy preserving ML, DM & KDD
- – Data leak detection
- – Data citation
- – Differential privacy
- – Anonymization and pseudonymization
- – Securing expert-in-the-loop machine learning systems
- – Evaluation and benchmarking

A. Holzinger 709.049
61/76
Med Informatics L11

**Machine learning** is the most growing field in computer science [Jordan, M. I. & Mitchell, T. M. 2015. Machine learning: Trends, perspectives, and prospects. [Science, 349, \(6245\), 255-260](#)], and it is well accepted that **health informatics** is amongst the greatest challenges [LeCun, Y., Bengio, Y. & Hinton, G. 2015. Deep learning. [Nature, 521, \(7553\), 436-444](#)]. To ensure privacy, data protection, safety and information security is of utmost importance.


The amount of patient-related data produced in today's clinical setting poses many challenges with respect to collection, storage and responsible use. For example, in research and public health care analysis, data must be anonymized before transfer, for which the k-anonymity measure was introduced and successively enhanced by further criteria. As k-anonymity is an NP-hard problem, which cannot be solved by automatic machine learning (aML) approaches we must often make use of approximation and heuristics. As data security is not guaranteed given a certain k-anonymity degree, additional measures have been introduced in order to refine results (l-diversity, t-closeness, delta-presence). This motivates methods, methodologies and algorithmic machine learning approaches to tackle the problem. As the resulting data set will be a tradeoff between utility and individual privacy, we need to optimize those measures to individual (subjective) standards. Moreover, the efficacy of an algorithm strongly depends on the background knowledge of a potential attacker as well as the underlying problem domain. One possible solution is to make use of [interactive machine learning \(iML\)](#) approaches and put a human-in-the-loop and a central question is: "could human intelligence

lead to general heuristics we can use to improve heuristics?”

Research topics covered by this special session include but are not limited to the following topics:

- Production of Open Data Sets
- Privacy preserving machine learning, data mining and knowledge discovery
- Data leak detection
- Data citation
- Anonymization and Pseudonymization
- Securing expert-in-the-loop machine learning systems
- Synthetic data sets for machine learning algorithm testing
- Evaluation and benchmarking

This special session will bring together scientists with diverse background, interested in both the underlying theoretical principles as well as the application of such methods for practical use in the biomedical, life sciences and health care domain. The cross-domain integration and appraisal of different fields will provide an atmosphere to foster different perspectives and opinions; it will offer a platform for novel crazy ideas and a fresh look on the methodologies to put these ideas into business.

<b>Slide 11-45 Future Outlook</b>		
<ul style="list-style-type: none"><li>▪ Privacy, Security, Safety and Data Protection are of enormous <b>increasing importance</b> in the future.</li><li>▪ Trend to <b>mobile and cloud</b> computing approaches.</li><li>▪ EHR are the fastest growing application which concern data privacy and <b>informed patient consent</b>.</li><li>▪ Personal health data are being stored for the purpose of maintaining a <b>life-long health record</b>.</li><li>▪ <b>Secondary use</b> of data, providing patient data for research.</li><li>▪ Production of <b>Open Data</b> to support international research efforts (e.g. cancer) without boundaries.</li><li>▪ <b>Data citation</b> approaches are needed for full transparency and replicability of research ...</li></ul>		
A. Holzinger 709.049	62/76	Med Informatics L11

Informed Patient Consent =

Data Citation = The scientific method and the credibility of science rely on full transparency and explicit references to both methods and data. These require that science data be open and available without undue and proprietary restriction. However, a consistent, rigorous approach to data citation is lacking.

For most secondary data use, it is necessary to use de-identified data, but for the remaining data protection issues are very important (Safran et al., 2007). The secondary use of data involves the linkage of data sets to bring different modalities of data together, which raises more concerns over the privacy of the data. The publication of the Human Genome gave rise to new ways of finding relationships between clinical disease and human genetics. The increasing use and storage of genetic information also impacts the use of familial records, since the information about the patient also provides information on the patient's relatives. The issues of data privacy and patient confidentiality and the use of the data for medical research are made more difficult in this post-genomic age.



# Thank you!

A. Holzinger 709.049

63/76

Med Informatics L11

My DEDICATION is to make data valuable ... Thank you!

**Sample Questions (1)**

- What is the core essence of the famous IOM report “Why do accidents happen”?
- What is a typical ultrasafe system – what is an example for a high risk activity?
- Which influence had the IOM report on safety engineering?
- What are the differences between the concepts of Privacy, Security and Safety?
- Why is privacy important in the health care domain?
- How do you classify errors when following the Eindhoven Classification Model?
- Please describe the basic architecture of a adverse event reporting and learning system?
- What is a typical example for medical errors?
- Please, explain the Swiss-Cheese Model of Human Error!



**Sample Questions (2)**

- What factors does the framework for understanding human error include?
- Which possibilities does ubiquitous computing offer to contribute towards enhancing patient safety?
- What different types of risk does the FAA System Safety Guideline explain?
- Ubiquitous computing offers benefits for health care, but which genuine security problems does ubiquitous computing bring?
- How can mobile computing device help in terms of patient safety?
- What is a context-aware patient safety approach?
- How can we describe patient safety both quantitatively and qualitatively?
- What is technical dependability?
- Which types of technical faults can be determined?

**Sample Questions (3)**

- What types of adverse events can be discriminated in medicine and health care?
- How is the safety level (measurement) defined?
- Which factors contribute to ultrasafe health care?
- What are the typical requirements of any electronic patient record?
- Why is Pseudonymization important?
- What is the basic idea of k-Anonymization?
- What is a potential threat of private personal health records?
- Please describe the concept of a personal health record system!
- How would you analyze personal health record systems?
- What does a privacy policy describe?
- Which ethical issues are related to quality improvement?

## Some Useful Links

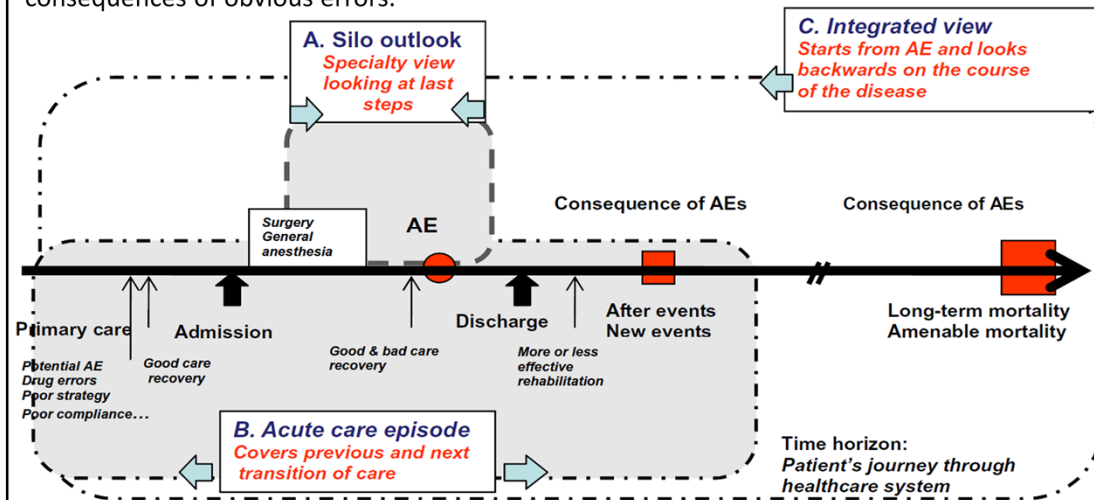


- <http://www.nap.edu/openbook.php?isbn=0309068371> (National Academy Press, To err is human)
- <http://medical-dictionary.thefreedictionary.com> (medical dictionary and thesaurus)
- <http://www.ico.gov.uk> (Information Commissioner's Office in the UK)
- [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm) (European Commission Protection of private personal data)
- <http://www.dsk.gv.at/> (Österreichische Datenschutz Kommission)
- [http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH\\_4084411](http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4084411) (Department of Health: Patient confidentiality and Access to Health Records)
- [http://videlectures.net/kdd09\\_mohammed\\_ahdcsbts](http://videlectures.net/kdd09_mohammed_ahdcsbts) (Anonymizing Healthcare Data: A Case Study on the Blood Transfusion Service)
- <http://www.hipaa.com/2009/09/hipaa-protected-health-information-what-does-phi-include> (HIPAA 'Protected Health Information': What Does PHI Include?)

## Appendix: Advances in patient safety are hampered by ...



... the silo and insurance-driven approaches, and by the narrow timeframe used in AE detection and analysis. Many AEs occurring at strategic points escape scrutiny, and the impact of widely publicized insurance claims on public health is often greater than that of the immediate consequences of obvious errors.



Amalberti, R., Benhamou, D., Auroy, Y. & Degos, L. (2011) Adverse events in medicine: Easy to count, complicated to understand, and complex to prevent. *Journal of Biomedical Informatics*, 44, 3, 390-394.

## Appendix: Example for a simple warning message



Clinical Application Suite [4.3.42] Thursday Aug 15, 2002 5:45 PM You are logged in as: Physician 1

Select pt **PATIENT 1** BWH 11489879 42y M Pt Details Pg

**Drug Warning(s) Found** Active Pt: PATIENT 1


**DRUG WARNING(S)**

Current Order:  
NAFCILLIN IV

Warning(s):

Status	Order
New Order	Allergy to : Penicillins Reaction: Anaphylaxis

Message:  
Reaction: Anaphylaxis. The patient has a DEFINITE sensitivity to NAFICILLIN.



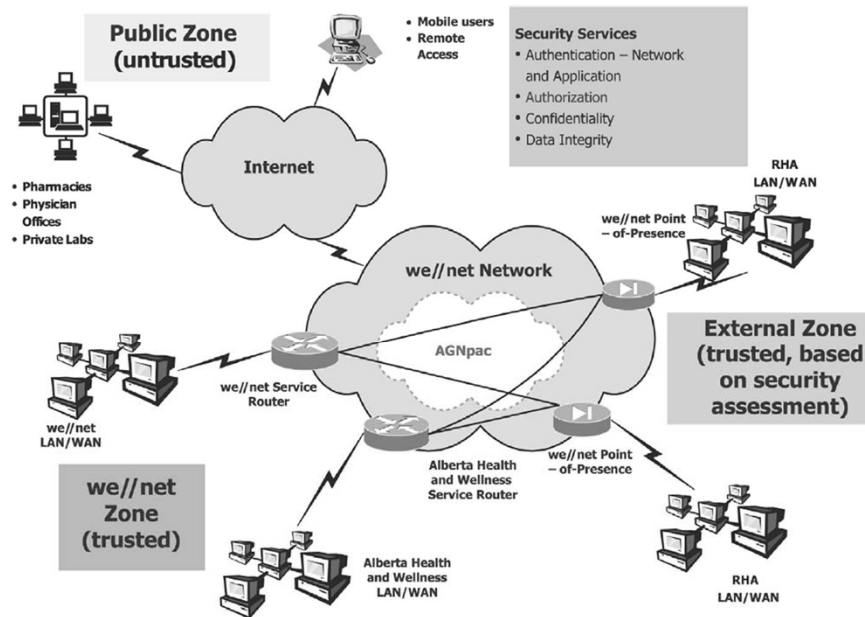
Keep (override) order Cancel (D/C) order

Use mouse or arrow keys to select an Order. Alt-K to Keep (override) order. Alt-C to cancel.

Start Clinical Application Suite 5:49 PM

Bates, D. W. & Gawande, A. A. (2003) Improving Safety with Information Technology. *New England Journal of Medicine*, 348, 25, 2526-2534.

## Appendix: Example for trust policies in HIS networks

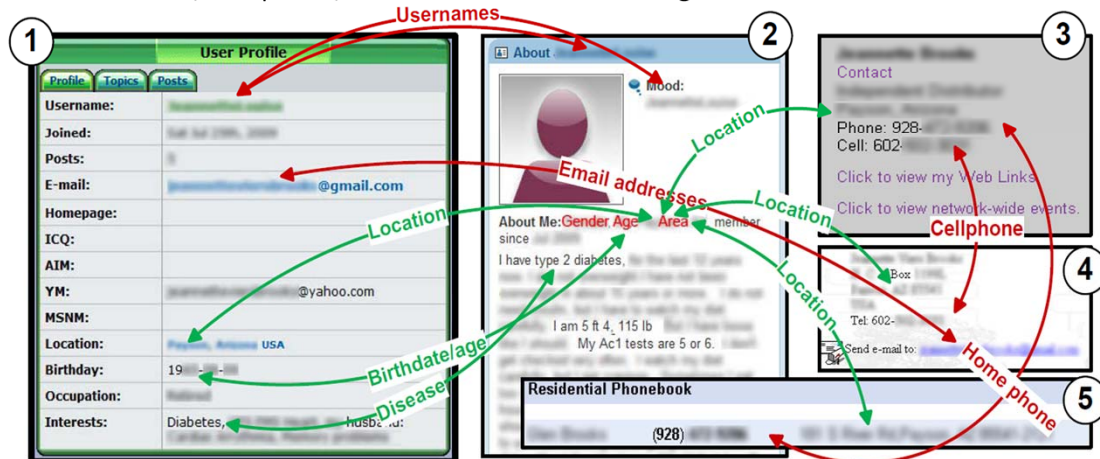


Mills, K. S., Yao, R. S. & Chan, Y. E. (2003) Privacy in Canadian Health Networks: challenges and opportunities. *Leadership in Health Services*, 16, 1, 1-10.

## Appendix: Example of new threats to health data privacy

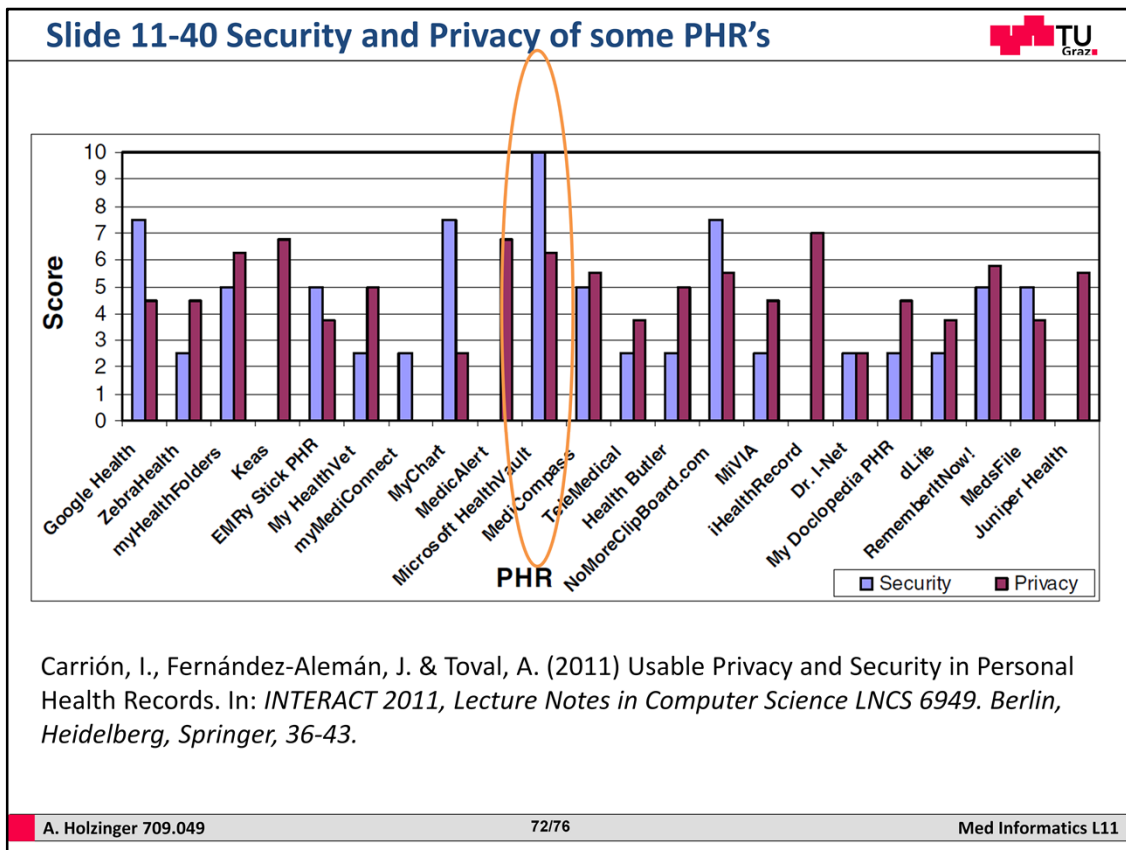


A real-world example of cross-site information aggregation: The target patient “Jean” has profiles on two online medical social networking sites (1) and (2). By comparing the attributes from both profiles, the adversary can link the two with high confidence. The attacker can use the attribute values to get more profiles of the target through searching the Web (3) and other online public data sets (4 and 5). By aggregating and associating the five profiles, Jean’s full name, date of birth, husband’s name, home address, home phone and cell phone number, two email addresses, occupation, medical information including lab test results are disclosed!



Li, F., Zou, X., Liu, P. & Chen, J. (2011) New threats to health data privacy. *BMC Bioinformatics*, 12, Supplement 12, 1-7.






### Slide 11-40 Security and Privacy of some PHR's

This work by (Carrión, Fernández-Alemán & Toval, 2011) is interesting for two reasons: 1) it provides a good overview of some personal health records and 2) it shows to what extent they addressed security and privacy issues.

The figure shows scores as two overlapping histograms: In general, quite a good level can be observed in the characteristics analyzed. Nevertheless, some improvements could be made to current PHR privacy policies to enhance specific capabilities such as: the management of other users' data, the notification of changes in the privacy policy to users and the audit of accesses to users' PHRs. The characteristics on how they reached these scores can be inferred from the following slides.

<b>Slide 11-41 9 Security Characteristics to analyze PHR's 1/2</b> 	
<ul style="list-style-type: none"> <li>▪ <b>1) Privacy Policy</b> <ul style="list-style-type: none"> <li>▪ 0. The Privacy Policy is not visible or not accessible.</li> <li>▪ 1. The Privacy Policy is accessed by clicking one link.</li> <li>▪ 2. The Privacy Policy is accessed by clicking two or more links.</li> </ul> </li> <li>▪ <b>2) Data Source</b> <ul style="list-style-type: none"> <li>▪ 0. Not indicated.</li> <li>▪ 1. User.</li> <li>▪ 2. User healthcare provider.</li> <li>▪ 3. User and his/her healthcare providers.</li> <li>▪ 4. User, other authorized users and other services/programs.</li> <li>▪ 5. Self-monitoring devices connected with the user.</li> </ul> </li> <li>▪ <b>3) Data Management</b> <ul style="list-style-type: none"> <li>▪ 0. Not indicated.</li> <li>▪ 1. Data user.</li> <li>▪ 2. Data user and his/her family data.</li> </ul> </li> <li>▪ <b>4) Access management</b> <ul style="list-style-type: none"> <li>▪ 0. Not indicated.</li> <li>▪ 1. Other users and services/programs.</li> <li>▪ 2. Healthcare professionals.</li> <li>▪ 3. Other users.</li> <li>▪ 4. Other users, healthcare professionals and services/programs.</li> </ul> </li> </ul>	
A. Holzinger 709.049	73/76
Med Informatics L11	

#### Slide 11-41 9 Security Characteristics to analyze PHR's 1/2


Carrión, Fernández-Alemán & Toval (2011) defined nine characteristics to analyze the Personal Health Records: Privacy policy, location, Data source, Data managed, Access management, Access audit, Data accessed without the user's permission, Security measures, Changes in privacy policy and Standards:

**Privacy Policy Location.** This characteristic is related to the question Where is the Privacy Policy on the PHR web site? PHRs should provide a Privacy Policy which describes how users' data are used in order for users to be informed. The Privacy Policy should be easily accessible by users. The difficulty of Privacy Policy access is assessed by counting the number of links clicked. The values that this characteristic may take are: 0. The Privacy Policy is not visible or not accessible. 1. The Privacy Policy is accessed by clicking one link. 2. The Privacy Policy is accessed by clicking two or more links.

**Data Source.** This characteristic is related to the question Where do users' PHR data proceed from? Generally, the user is his/her data source, but there are PHRs which do not only use this source. Some contact the users' healthcare providers, others allow other users and different programs to enter users' data and others use self-monitoring devices to obtain users' data. The values that this characteristic may take are: 0. Not indicated. 1. User. 2. User healthcare provider. 3. User and his/her healthcare providers. 4. User, other authorized users and other services/programs. 5. Self-monitoring devices connected with the user.

**Data Managed.** This characteristic is related to the question Who do the data managed by the users belong to? The users can manage their own data, but they can sometimes manage other users' data, such as that of their family. The values that this characteristic may take are: 0. Not indicated. 1. Data user. 2. Data user and his/her family data.

**Access management.** This characteristic is related to the question Who can obtain access granted by the users? The users decide who can access their PHR data. The PHR systems analyzed allow access to be given to different roles. The values that this characteristic may take are: 0. Not indicated. 1. Other users and services/programs. 2. Healthcare professionals. 3. Other users. 4. Other users, healthcare professionals and services/programs. To be continued on the next slide.

<b>Slide 11-42 9 Security Characteristics to analyze PHR's 2/2</b> 	
<ul style="list-style-type: none"> <li>▪ <b>5) Access audit</b> <ul style="list-style-type: none"> <li>▪ 0. No.</li> <li>▪ 1. Yes.</li> </ul> </li> <li>▪ <b>6) Data access without the end user's permission</b> <ul style="list-style-type: none"> <li>▪ 0. Not indicated.</li> <li>▪ 1. Information related to the accesses.</li> <li>▪ 2. De-identified user information.</li> <li>▪ 3. Information related to the accesses and de-identified user information.</li> <li>▪ 4. Information related to the accesses and identified user information.</li> </ul> </li> <li>▪ <b>7) Security measures</b> <ul style="list-style-type: none"> <li>▪ 0. Not indicated.</li> <li>▪ 1. Physical security measures.</li> <li>▪ 2. Electronic security measures.</li> <li>▪ 3. Physical security measures and electronic security measures.</li> </ul> </li> <li>▪ <b>8) Changes in Privacy Policy</b> <ul style="list-style-type: none"> <li>▪ 0. Not indicated.</li> <li>▪ 1. Changes are notified to users.</li> <li>▪ 2. Changes are announced on home page.</li> <li>▪ 3. Changes are notified to users and changes are announced on home page.</li> <li>▪ 4. Changes may not be notified.</li> </ul> </li> <li>▪ <b>9) Standards</b> <ul style="list-style-type: none"> <li>▪ 0. Not indicated.</li> <li>▪ 1. HIPAA is mentioned.</li> <li>▪ 2. System is covered by HONcode (HON = Health on the Net).</li> <li>▪ 3. HIPAA is mentioned and system is covered by HONcode.</li> </ul> </li> </ul>	
A. Holzinger 709.049	Med Informatics L11

#### Slide 11-42 9 Security Characteristics to analyze PHR's 2/2

**Access audit.** This characteristic is related to the question Can users see an audit of accesses to their PHRs? The values that this characteristic may take are: 0. No. 1. Yes. **Data accessed without the user's permission.** This characteristic is related to the question What data are accessed without the user's explicit consent? The PHR systems typically access certain data related to the users in order to verify that everything is correct. The values that this characteristic may take are: 0. Not indicated. 1. Information related to the accesses. 2. De-identified user information. 3. Information related to the accesses and de-identified user information. 4. Information related to the accesses and identified user information.

**Security measures.** This characteristic is related to the question What security measures are used in PHR systems? There are two types of security measures: physical measures and electronic measures. The physical security measures are related to the protection of the servers in which the data are stored. The electronic security measures are related to how stored and transmitted data are protected, for example, by using a Secure Sockets Layer (SSL) scheme. The values that this characteristic may take are: 0. Not indicated. 1. Physical security measures. 2. Electronic security measures. 3. Physical security measures and electronic security measures.

**Changes in Privacy Policy.** This characteristic is related to the question Are changes in privacy policy notified to users? Changes in Privacy Policy should be notified to users in order to make them aware of how their data are managed by the PHR system. The values that this characteristic may take are: 0. Not indicated. 1. Changes are notified to users. 2. Changes are announced on home page. 3. Changes are notified to users and changes are announced on home page. 4. Changes may not be notified. **Standards.** This characteristic is related to the question Are PHR systems based on privacy and security standards? The PHR systems analyzed use or are based on two standards: the Health Insurance Portability and Accountability Act (HIPAA) and the Health On the Net Code of Conduct (HONcode). The values that this characteristic may take are: Usable Privacy and Security in Personal Health Records 41 0. Not indicated. 1. HIPAA is mentioned. 2. System is covered by HONcode. 3. HIPAA is mentioned and system is covered by HONcode (Carrión, Fernández-Alemán & Toval, 2011).

Slide 11-43 Overview Personal Health Records (PHR)										TU Graz	
Tool	PL	DS	DM	AM	AA	DA	SM	CP	S		
1. Google Health	1	4	1	1	1	3	3	2	1		
2. ZebraHealth	2	1	0	0	0	1	3	4	1		
3. myHealthFolders	1	1	2	2	1	1	3	1	0		
4. Keas	1	4	1	0	0	2	3	3	0		
5. EMRy Stick Personal Health Record	2	1	1	0	1	1	0	0	0		
6. My HealthVet	2	1	1	2	0	1	2	0	1		
7. myMediConnect	0	3	1	2	0	0	3	0	1		
8. MyChart	1	2	1	0	1	4	0	0	1		
9. MedicAlert	1	1	1	3	0	2	3	2	0		
10. Microsoft HealthVault	1	4	1	4	1	1	3	2	3		
11. MediCompass	1	5	1	2	0	2	3	0	3		
12. TeleMedical	1	1	2	0	0	0	2	2	2		
13. Health Butler	1	1	1	2	0	2	0	4	0		
14. NoMoreClipboard.com	1	3	2	2	1	2	2	2	1		
15. MiVIA	1	0	1	2	0	3	3	2	1		
16. iHealthRecord	1	0	0	0	0	1	2	4	0		
17. Dr. I-Net	1	3	1	2	0	0	3	0	0		
18. My Doclopedia PHR	1	2	1	2	0	3	2	2	1		
19. dLife	1	0	0	0	0	4	2	2	0		
20. RememberItNow!	1	4	1	4	1	3	2	3	0		
21. MedsFile	1	1	1	0	1	4	1	1	0		
22. Juniper Health	1	1	2	0	0	2	3	2	0		

Legend: PL = Privacy policy location; DS = Data source; DM = Data managed; AM = Access management; AA = Access audit; DA = Data accessed without the user's permission; SM = Security measures; CP = Changes in privacy policy; S = Standards

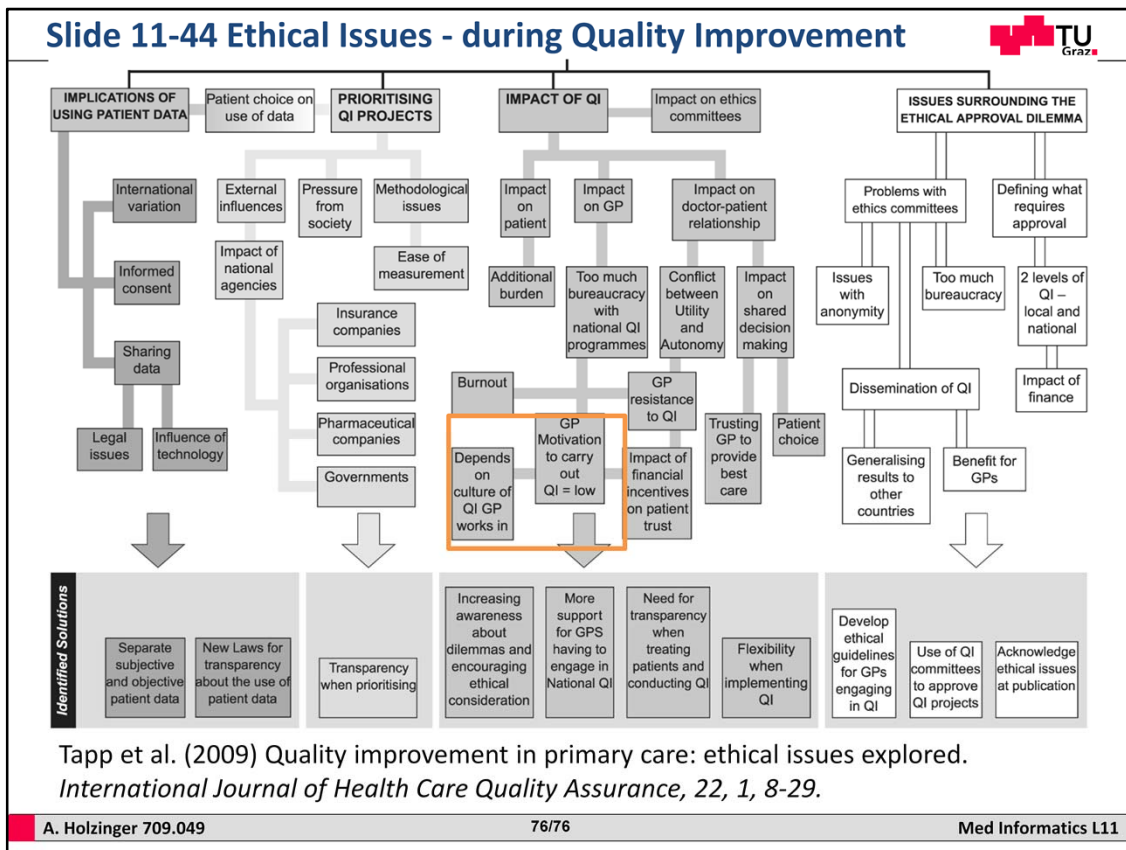
Carrión et al. (2011)

### Slide 11-43 Overview Personal Health Records (PHR)

The last slide shows the summary of the researched personal health records (Carrión, Fernández-Alemán & Toval, 2011). Note: By 2013 the Google Health record is not longer in operation: Google Health has been permanently discontinued. All data remaining in Google Health user accounts as of January 2, 2013 has been systematically destroyed, and Google is no longer able to recover any Google Health data for any user, see:

[http://www.google.com/intl/en\\_us/health/about](http://www.google.com/intl/en_us/health/about)

See also this blog: <http://googleblog.blogspot.co.at/2011/06/update-on-google-health-and-google.html>



### Slide 11-44 Ethical Issues - during Quality Improvement

Here a summary of ethical issues by a work of (Tapp et al., 2009): They identified the experiences of professionals involved in planning and performing QI programmes in European family medicine on the ethical implications involved in those processes. For this purpose they used four focus groups with 29 general practitioners (GPs) and administrators of general practice quality work in Europe. Two focus groups comprised EQuiP members and two focus groups comprised attendees to an invitational conference on QI in family medicine held by EQuiP in Barcelona. Four overarching themes were identified, including implications of using patient data, prioritizing QI projects, issues surrounding the ethical approval dilemma and the impact of QI. Each theme was accompanied by an identified solution. Practical implications – Prioritising is necessary and in doing that GPs should ensure that a variety of work is conducted so that some patient groups are not neglected. Transparency and flexibility on various levels is necessary to avoid harmful consequences of QI in terms of bureaucratisation, increased workload and burnout on part of the GP and harmful effects on the doctor-patient relationship. There is a need to address the system of approval for national QI programmes and QI projects utilising more sophisticated methodologies (Tapp et al., 2009).