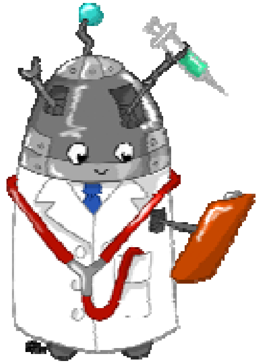


Andreas Holzinger

VO 709.049 Medical Informatics

25.01.2017 11:15-12:45

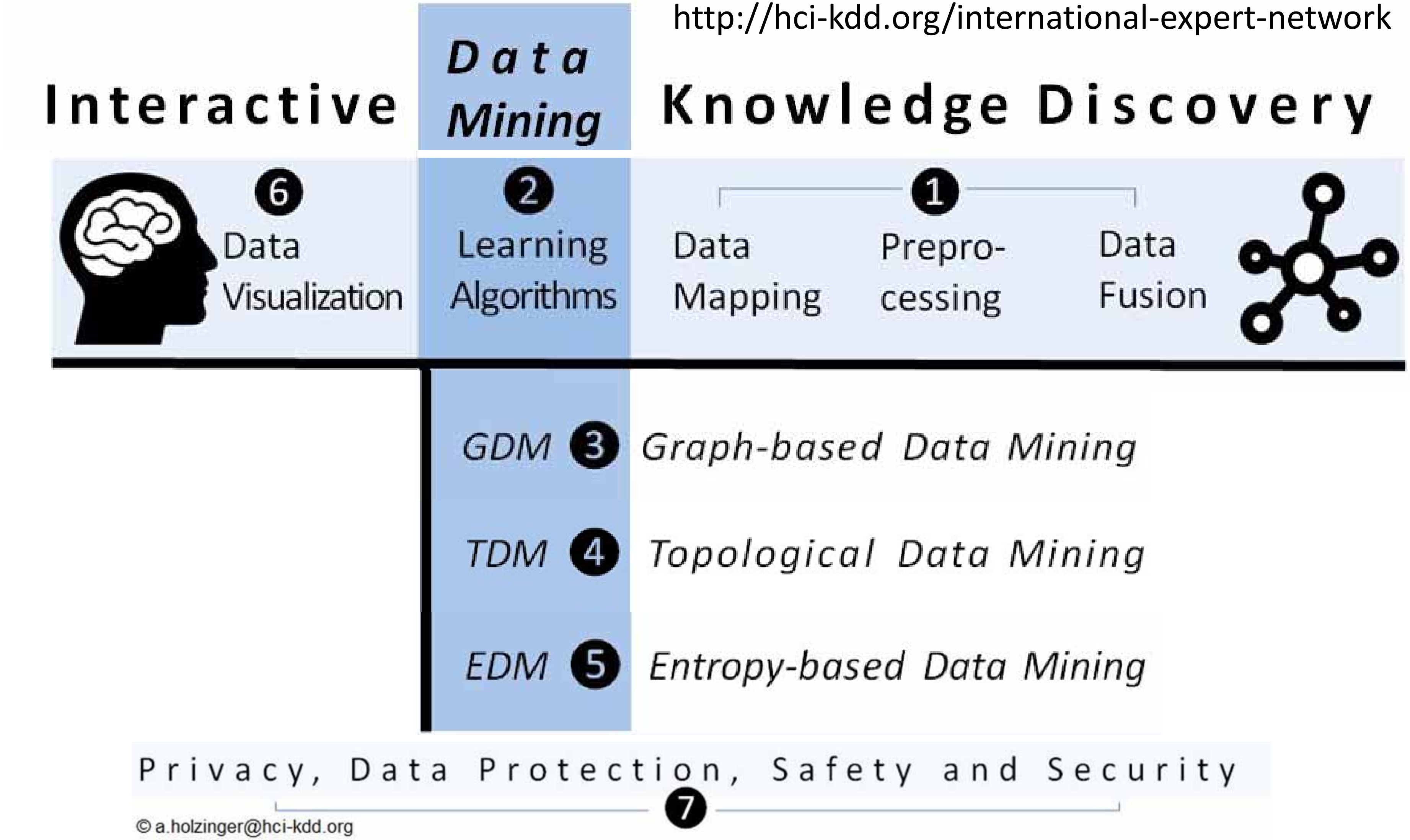
Lecture 11 Biomedical Data: Privacy, Data Protection, Safety, Security & Privacy Aware Machine Learning

a.holzinger@tugraz.at

Tutor: markus.plass@student.tugraz.at

http://hci-kdd.org/biomedical-informatics-big-data

ML needs a concerted effort fostering integrated research



Holzinger, A. 2014. Trends in Interactive Knowledge Discovery for Personalized Medicine: **Cognitive Science meets Machine Learning.** IEEE Intelligent Informatics Bulletin, 15, (1), 6-14.

Keywords

- Adverse events
- Anoynmization
- 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 inaccurateness, 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;

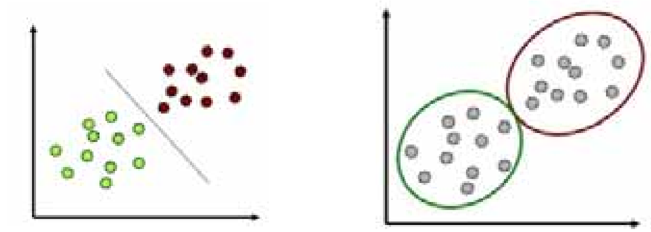
Learning Goals: At the end of this 11th lecture you …

- 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;

- 00 Reflection – follow-up from last lecture
- 01 Decision Support Systems (DSS)
- 02 History of DSS = History of AI
- 03 Development of DSS
- 04 Further Practical Examples
- 05 Towards Precision Medicine (P4)
- 06 Case Based Reasoning (CBR)


00 Reflection

Warm-up Quiz

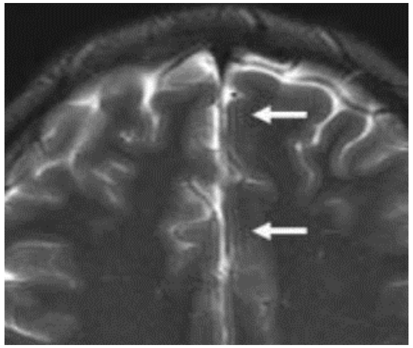


1

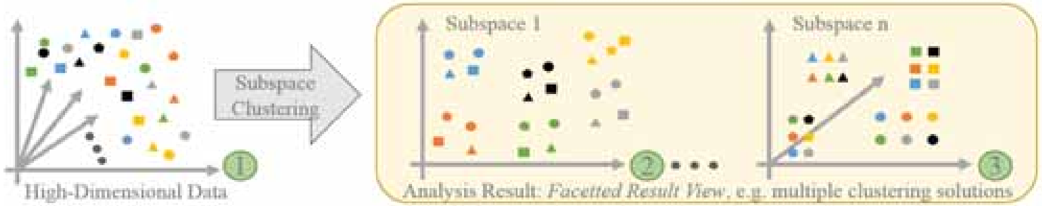
$$\begin{bmatrix}x_1\\x_2\\\vdots\\x_N\end{bmatrix} \longrightarrow \begin{bmatrix}x_{i_1}\\x_{i_2}\\\vdots\\x_{i_M}\end{bmatrix} \qquad \begin{bmatrix}x_1\\x_2\\\vdots\\x_N\end{bmatrix} \longrightarrow \begin{bmatrix}y_1\\y_2\\\vdots\\y_M\end{bmatrix} = f\left(\begin{bmatrix}x_1\\x_2\\\vdots\\x_N\end{bmatrix}\right)$$

2

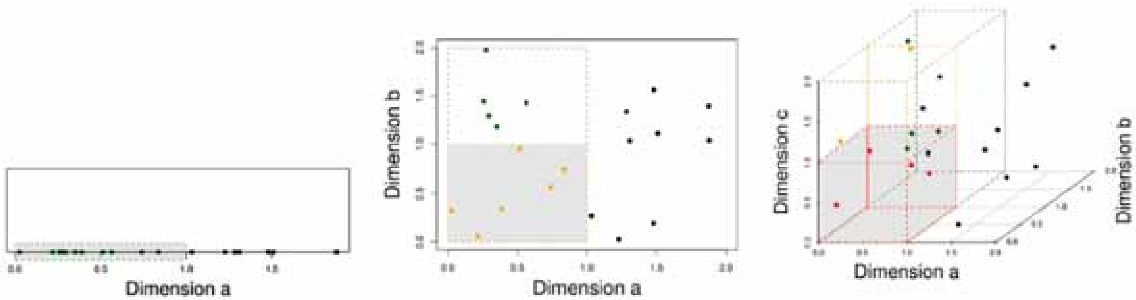
3



4



5



6

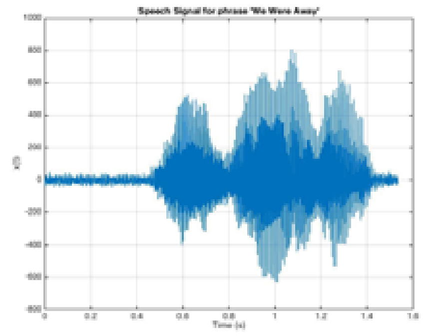
Diagnostic Decision

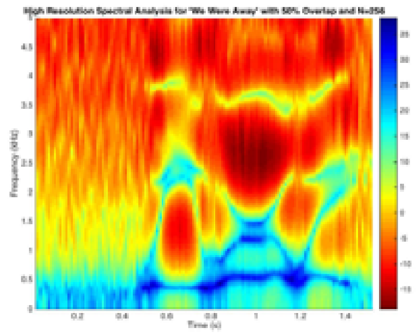
True State		Present	Absent
	Present	Hit	Miss
	Absent	False Alarm	Correct Rejection

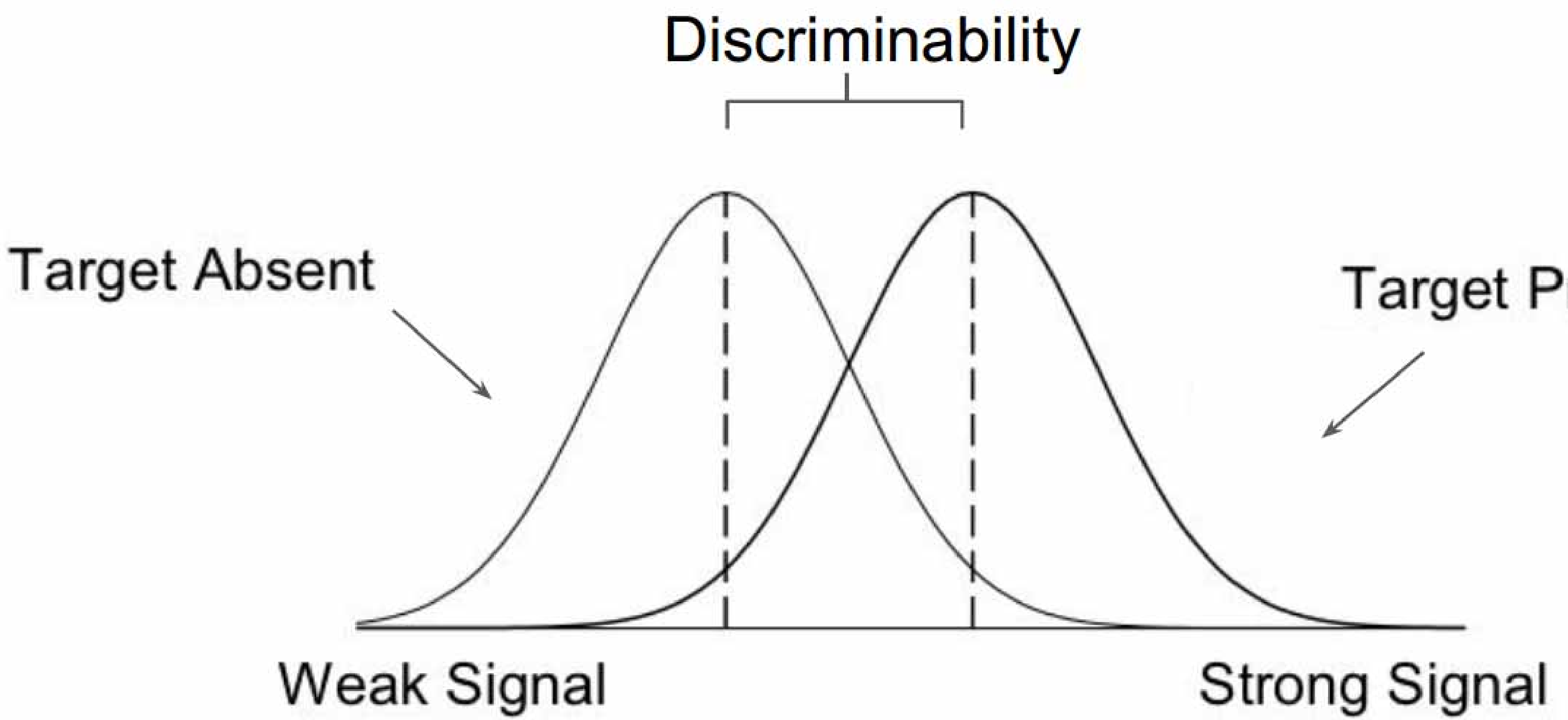
7

Fundamental Signal Detection Problem

Swets, J. A. 1961. Detection theory and psychophysics: a review. Psychometrika, 26, (1), 49-63, doi:10.1007/BF02289684.







11

01 Safety first …

- 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!**

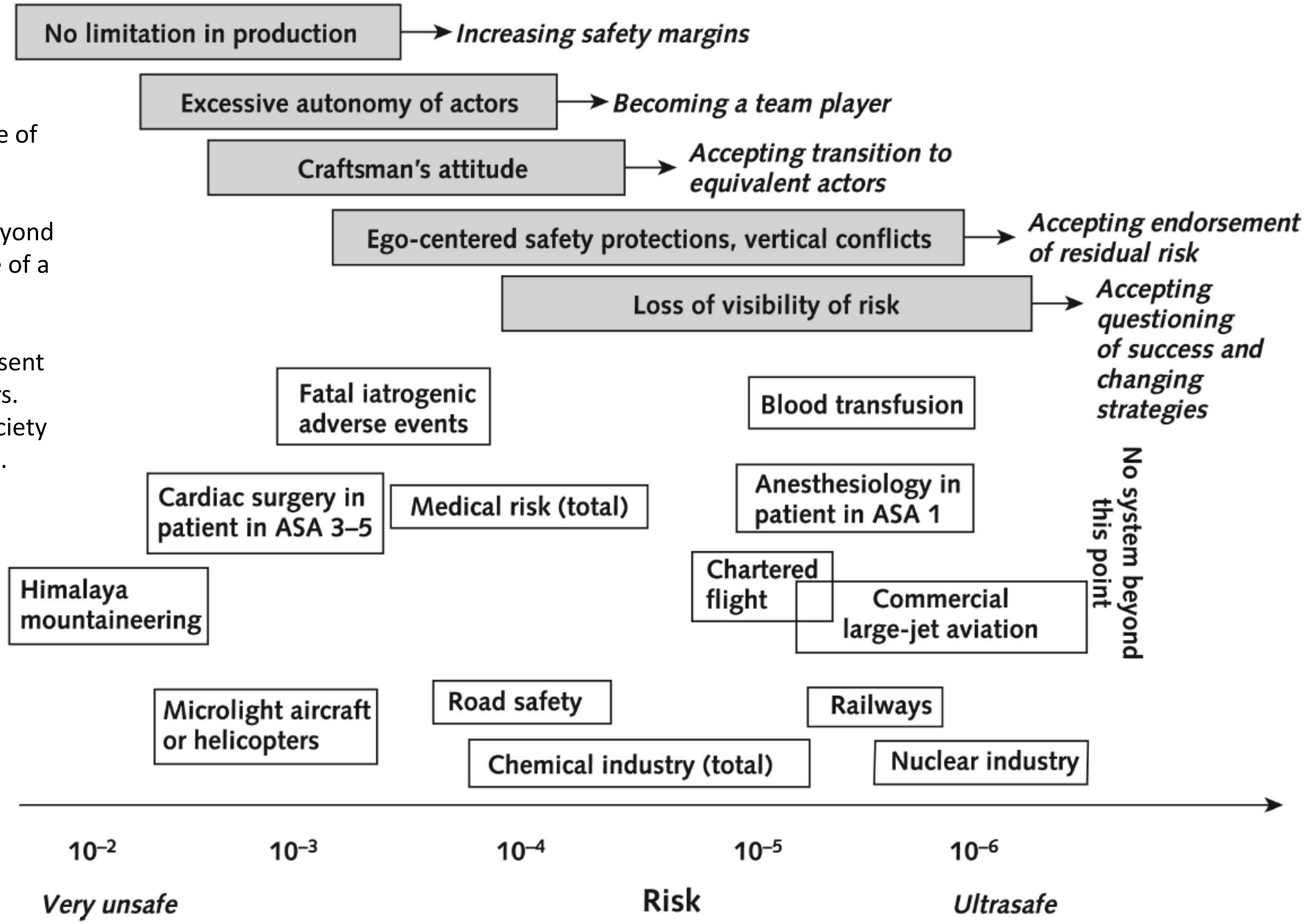
Horvitz, E. & Mulligan, D. 2015. Data, privacy, and the greater good. Science, 349, (6245), 253-255.

Slide 11-2 We start with thinking about safety first …

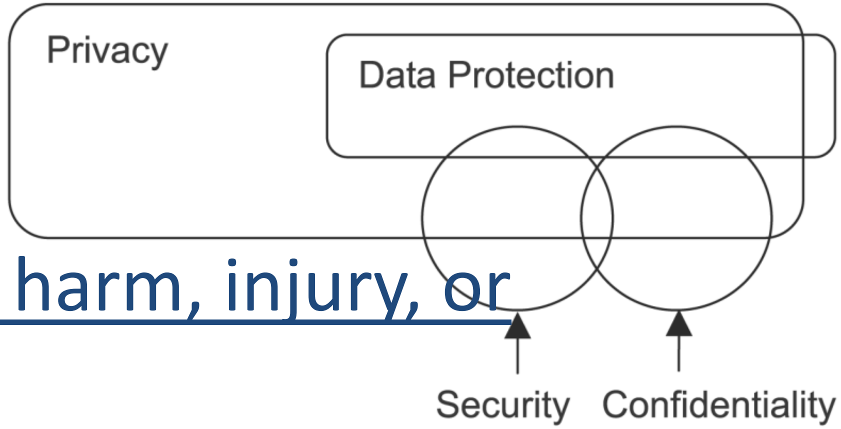
http://ngadventure.typepad.com/blog/news-k2-death-trap-is-sec.html

Slide 11-3 Exposure of catastrophes - associated deaths

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.



Amalberti, R., Auroy, Y., Berwick, D. & Barach, P. (2005) Five system barriers to achieving ultrasafe health care. *Annals of Internal Medicine, 142, 9, 756-764.*



- **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.*

Slide 11-4b Definitions (2/2)…

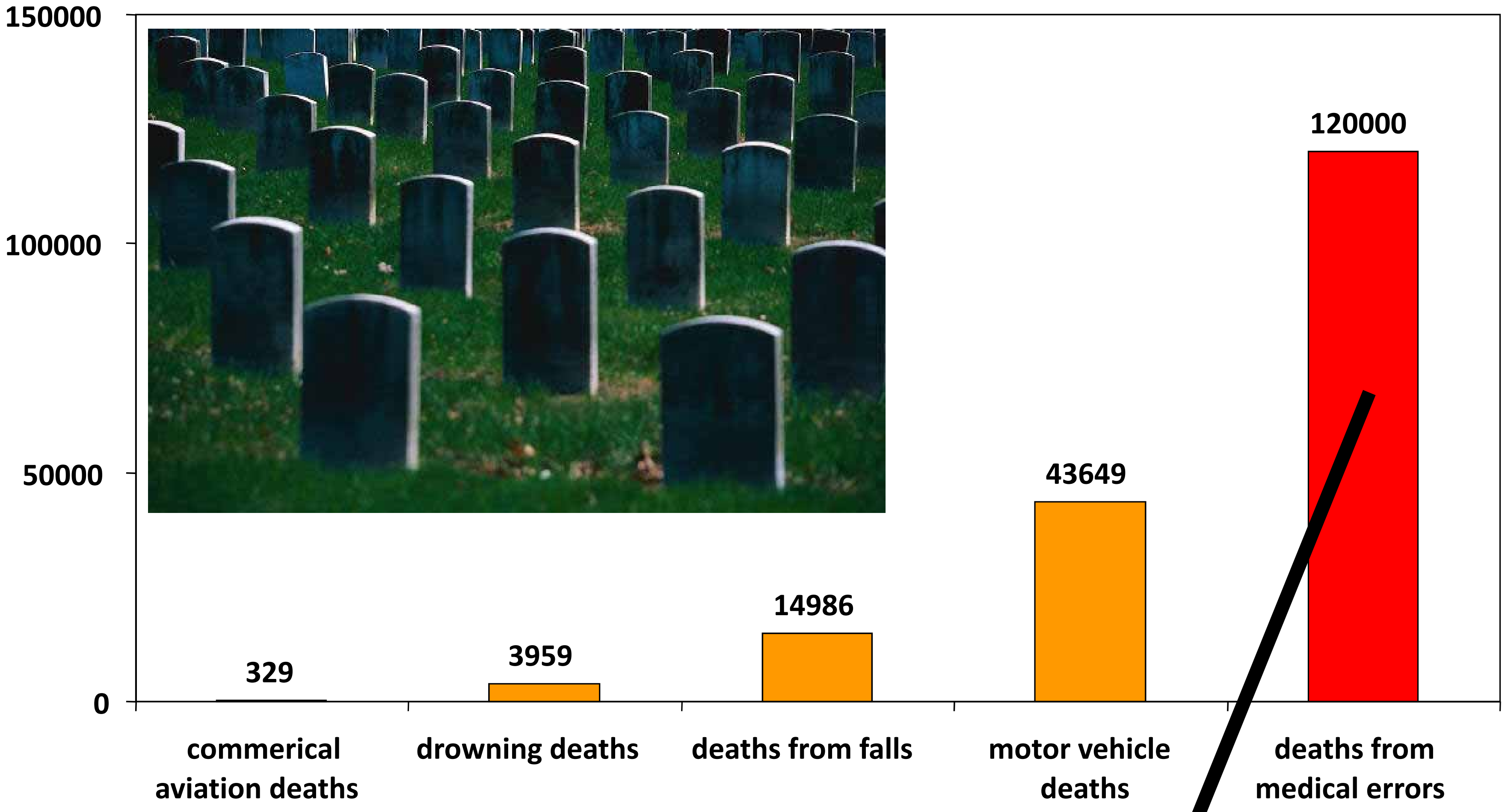
- **Availability =** p(x) that a system is operational at a given time, i.e. the amount of time a device is actually operating as the percentage of total time it should be operating;
- **Reliability =** the probability that a system will produce correct outputs up to some given time;
- **Security =** (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

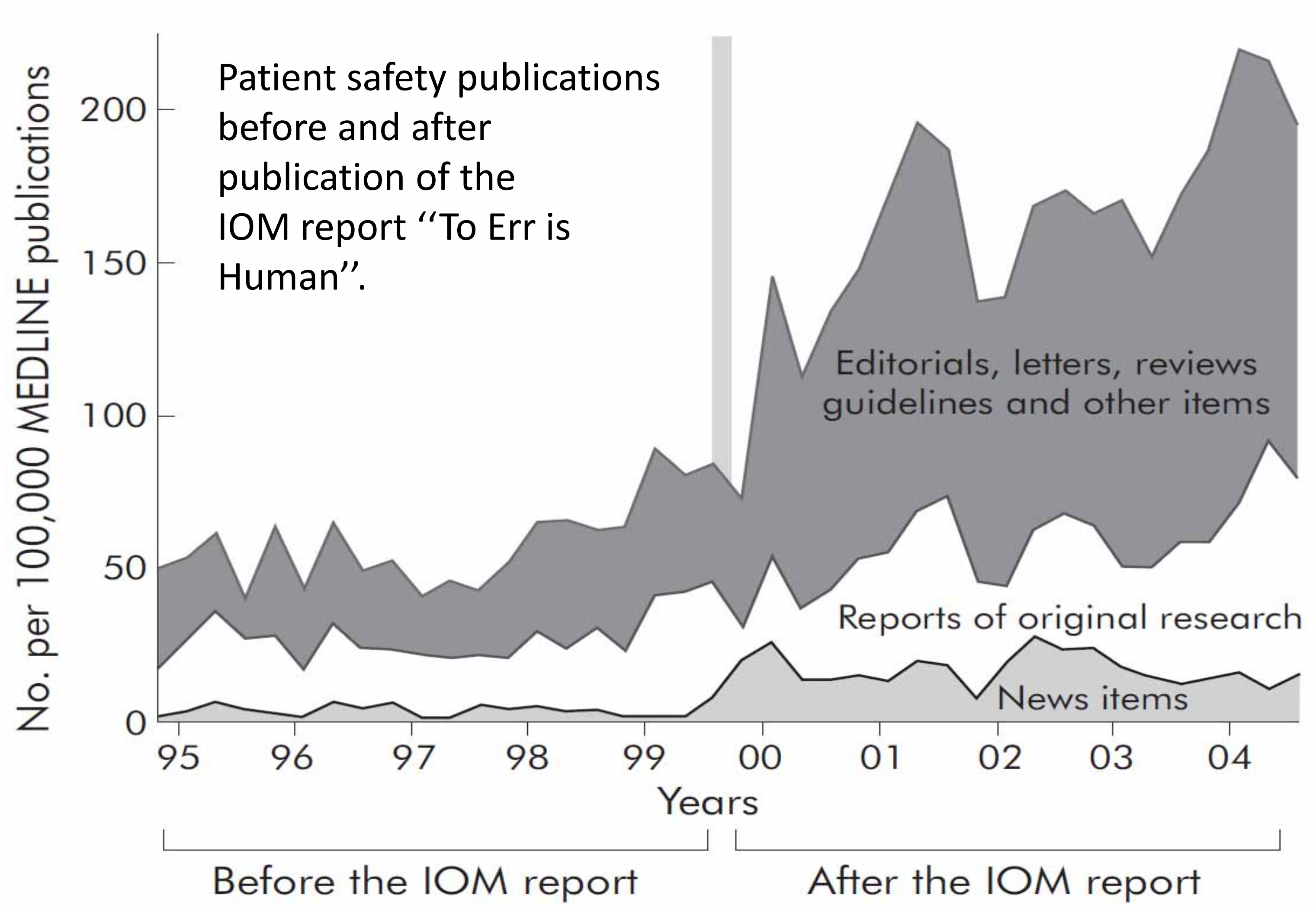
Slide 11-5 The famous report “Why do accidents happen”



Kohn, L. T., Corrigan, J. & Donaldson, M. S. (2000) *To err is human: building a safer health system. Washington (DC), National Academy Press.*

One jumbo jet crash every day

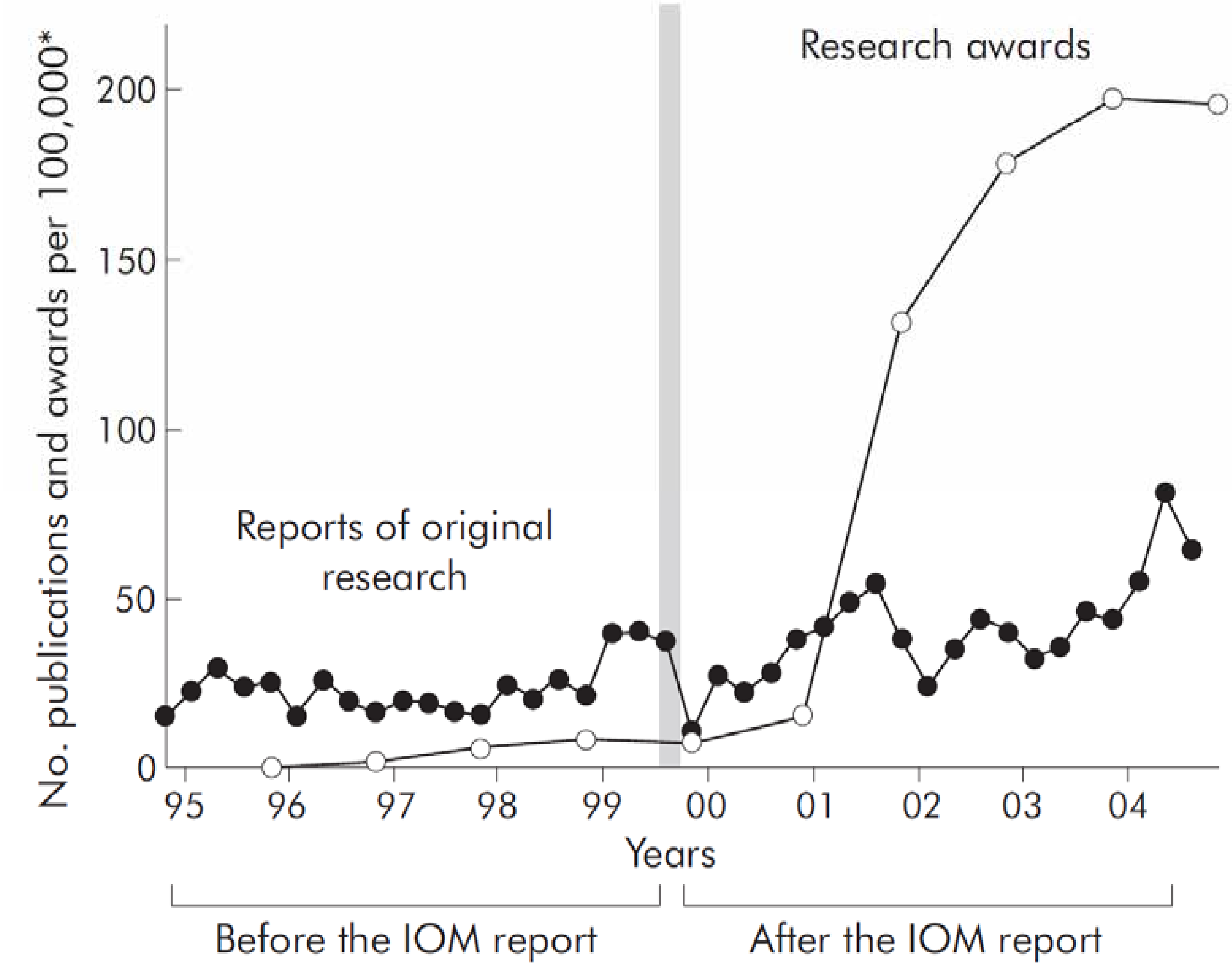
Slide 11-6 The impact of the “To err is human” IOM study



Stelfox, H. T., Palmisani, S., Scurlock, C., Orav, E. & Bates, D. (2006) The “To Err is Human” report and the patient safety literature. *Quality and Safety in Health Care, 15, 3, 174-178.*

Slide 11-7 Research activities stimulated by the IOM report

Patient safety research before and after publication of the IOM report ‘‘To Err is Human’’. Number of patient safety research publications and research awards per 100 000 MEDLINE publications and 100 000 federally funded biomedical research awards.



Stelfox, H. T., Palmisani, S., Scurlock, C., Orav, E. & Bates, D. (2006) The “To Err is Human” report and the patient safety literature. *Quality and Safety in Health Care, 15, 3, 174-178.*

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 »

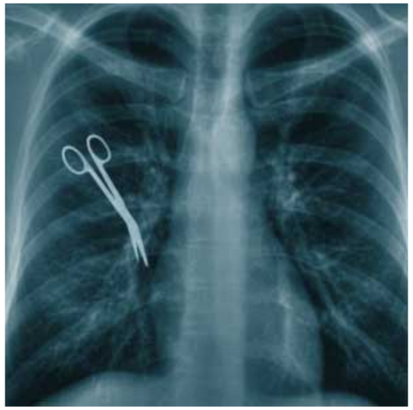
News Blog

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

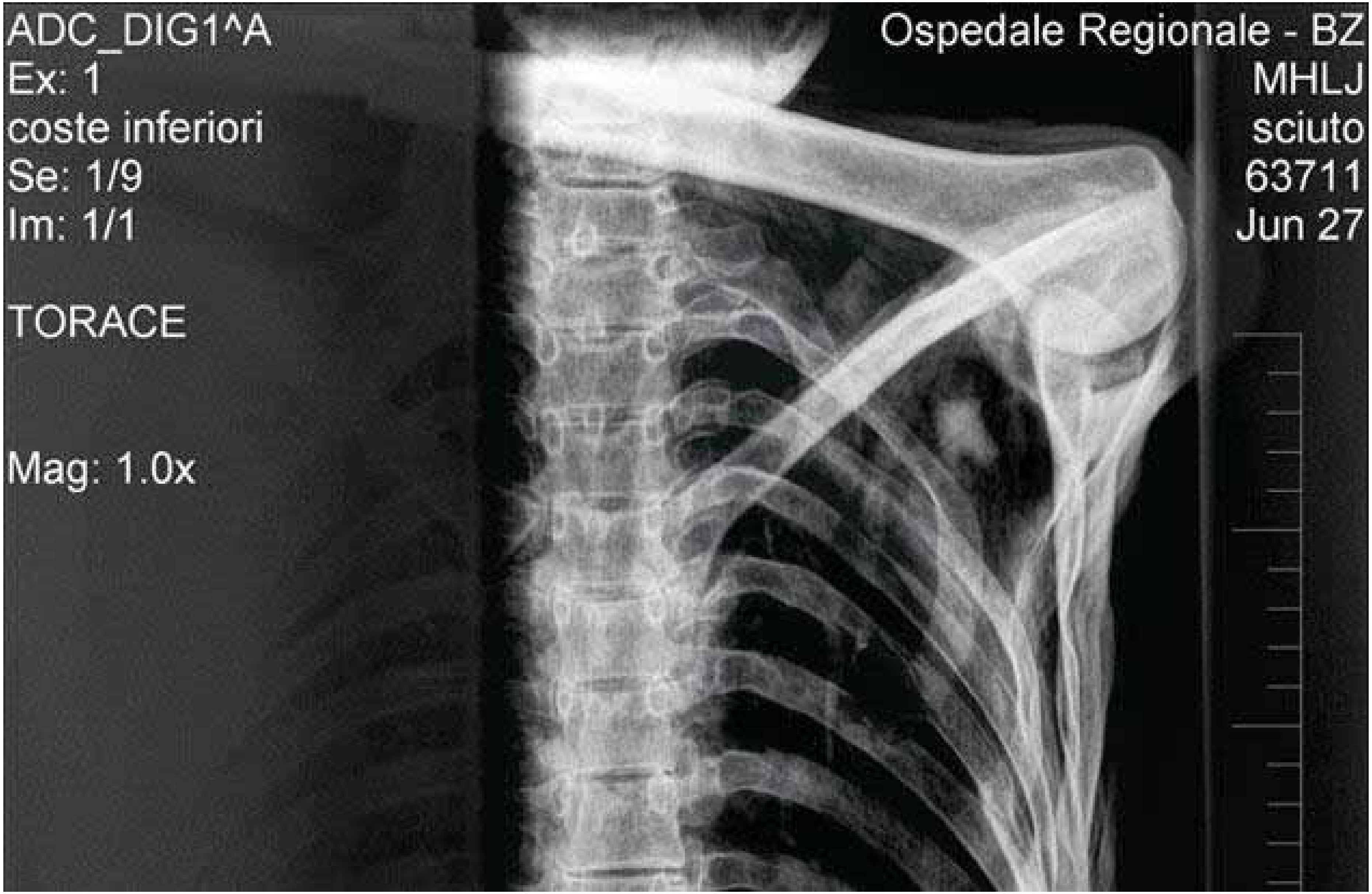
Share Email Print



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.

What do you see in this picture?



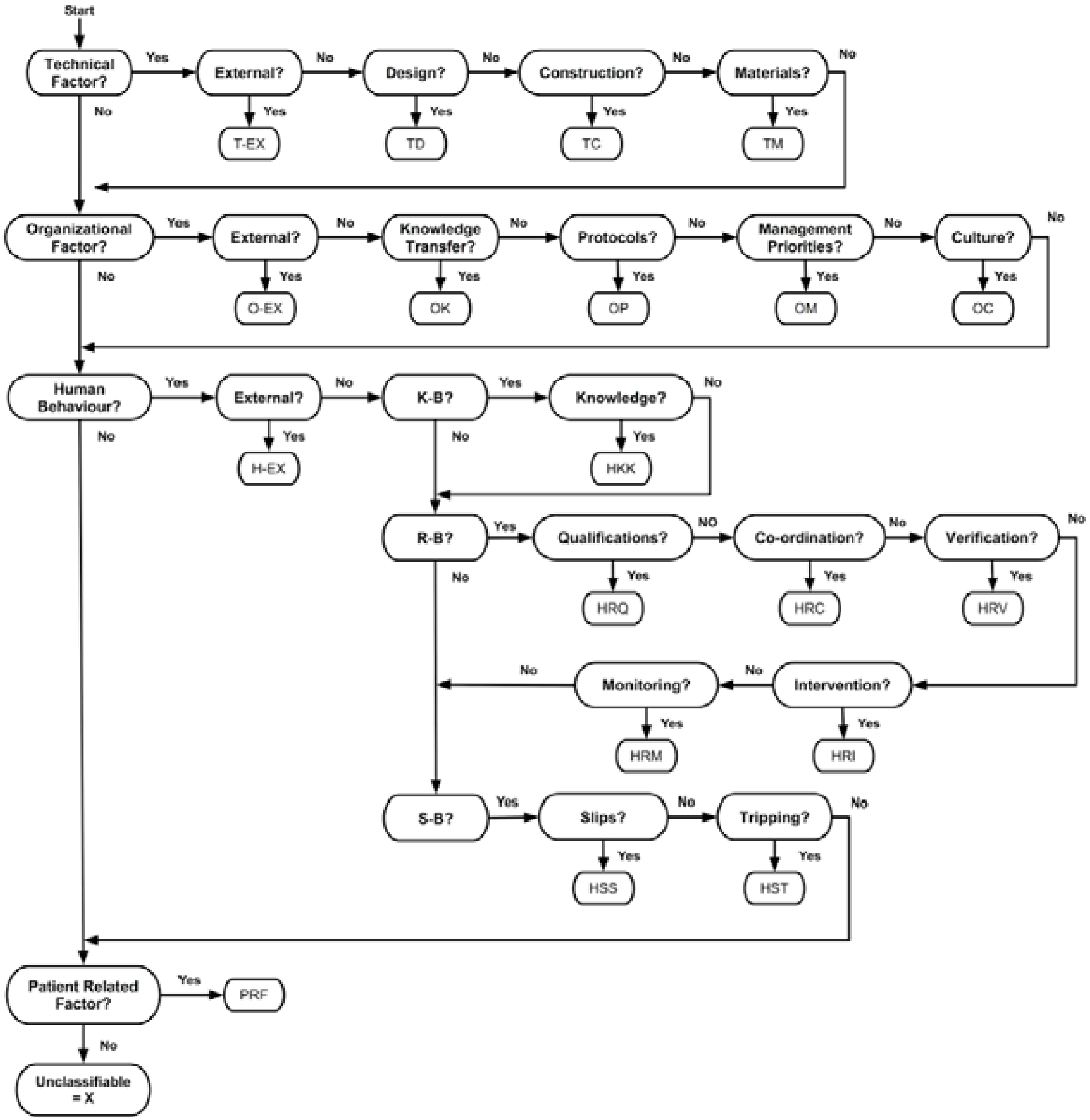
Slide 11-9 Medical Error Example: Wrong-Site Surgery

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

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.

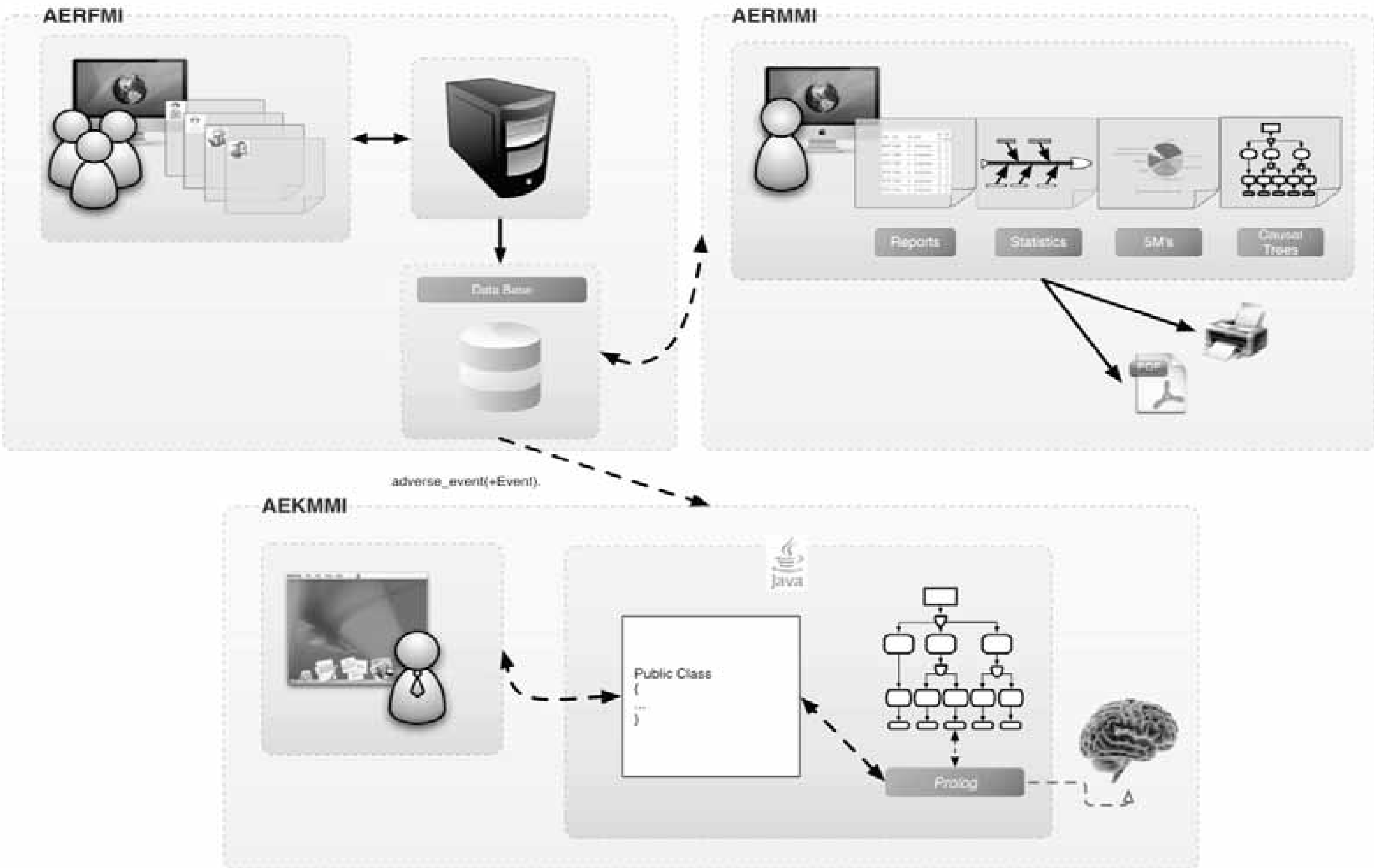
Starling, J. & Coldiron, B. M. (2011) Outcome of 6 years of protocol use for preventing wrong site office surgery. *Journal of the American Academy of Dermatology, 65, 4, 807-810.*

Slide 11-10 Deal with errors: Eindhoven Classification Model



Rodrigues, S., Brandao, P., Nelas, L., Neves, J. & Alves, V. (2010) A Logic Programming Based Adverse Event Reporting and Learning System. *IEEE/ACIS 9th International Conference on Computer and Information Science (ICIS). 189-194.*

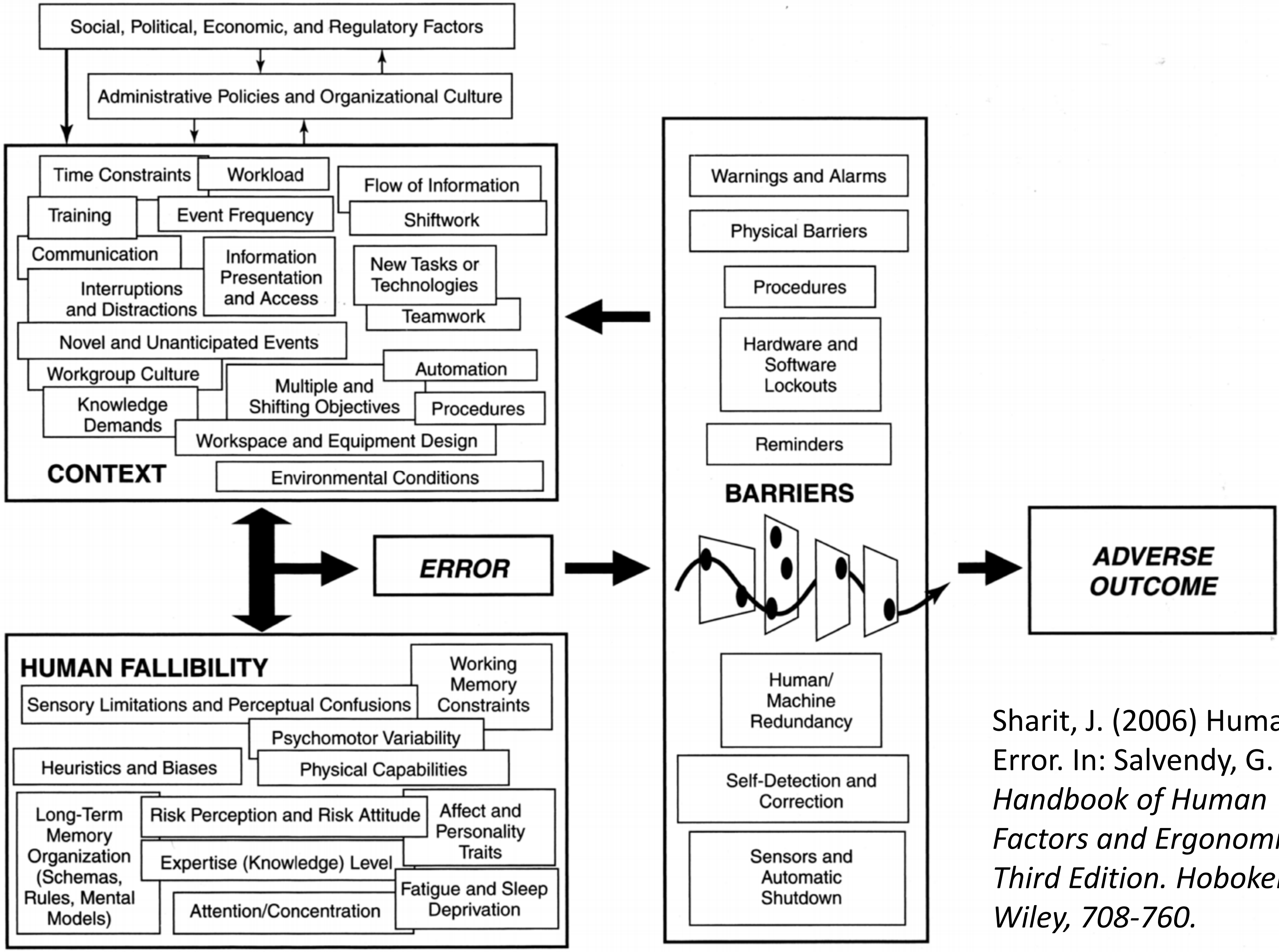
Slide 11-11 Adverse event reporting and learning system



3 Modules:
AERFMI =Adverse Events Reporting Forms in Medical Imaging
AERMMI = Adverse Events Manager Reports in Medical Imaging
AEKMMI = Adverse Events Knowledge Manager in Medical Imaging

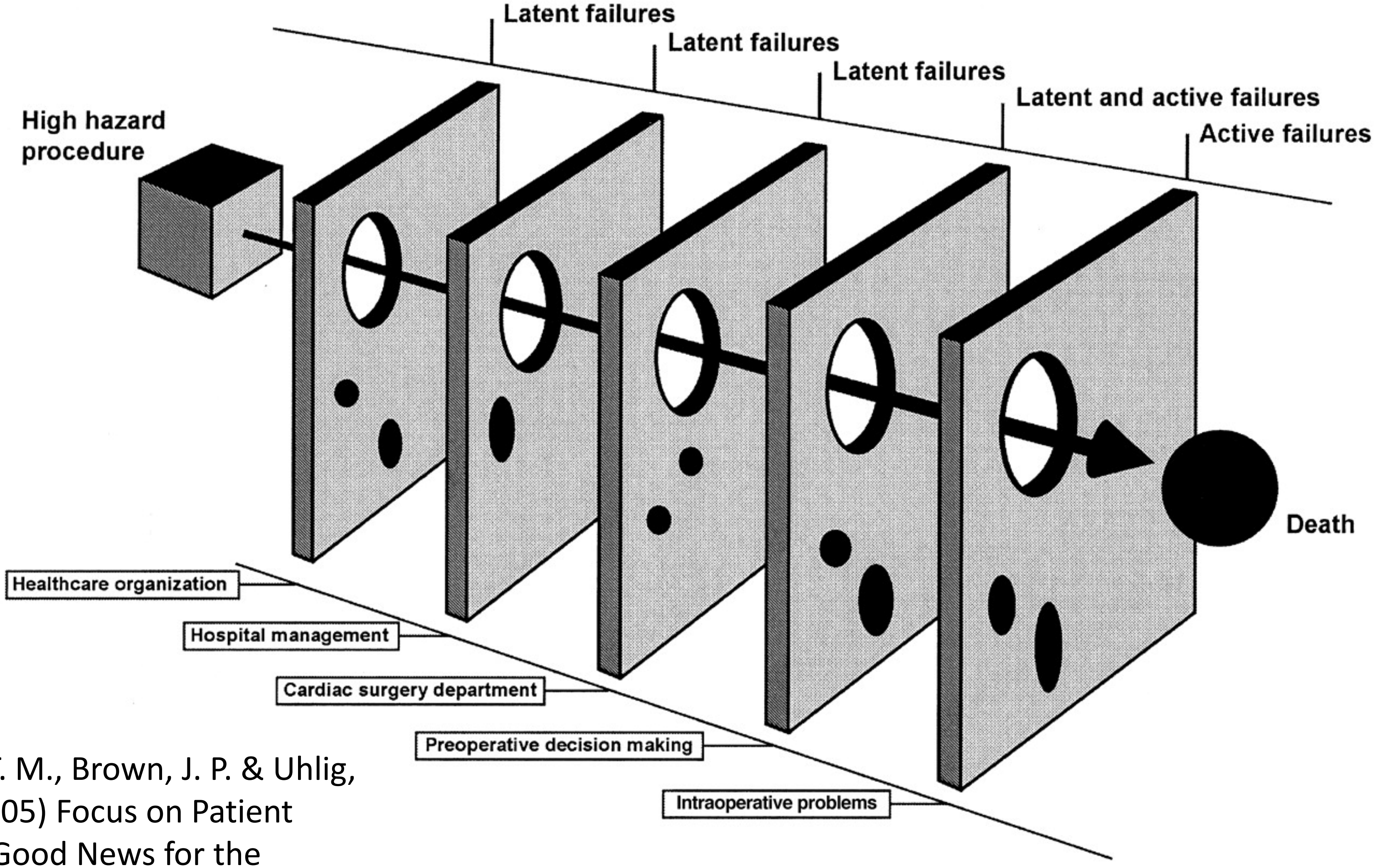
Rodrigues et al. (2010)

Slide 11-12 Re: Framework for understanding human error



Sharit, J. (2006) Human Error. In: Salvendy, G. (Ed.) *Handbook of Human Factors and Ergonomics, Third Edition. Hoboken (NJ), Wiley, 708-760.*

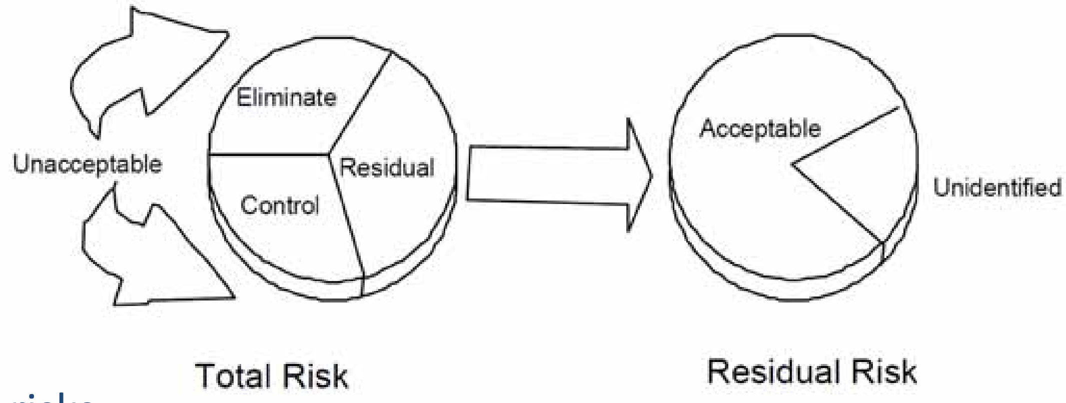
Reason JT (1997) Managing the risk of organizational accidents. Brookfield: Ashgate Publishing



Sundt, T. M., Brown, J. P. & Uhlig, P. N. (2005) Focus on Patient Safety: Good News for the Practicing Surgeon. *The Annals of Thoracic Surgery, 79, 1, 11-15.*

Slide 11-14 Risk management - FAA System Safety

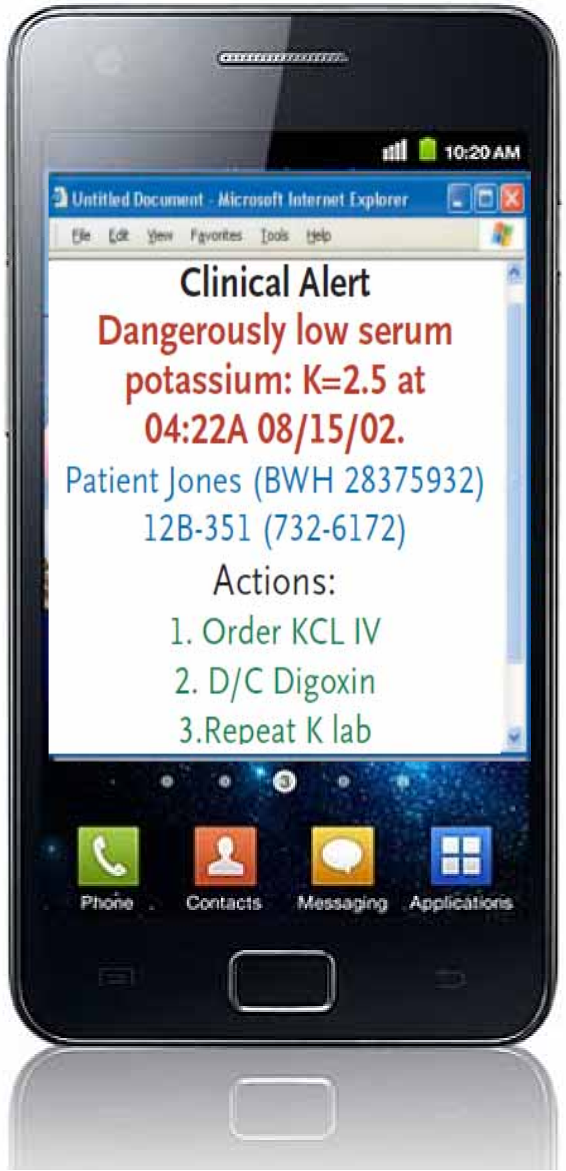
Note: Now just definitions, refer to risk management in Lecture 12



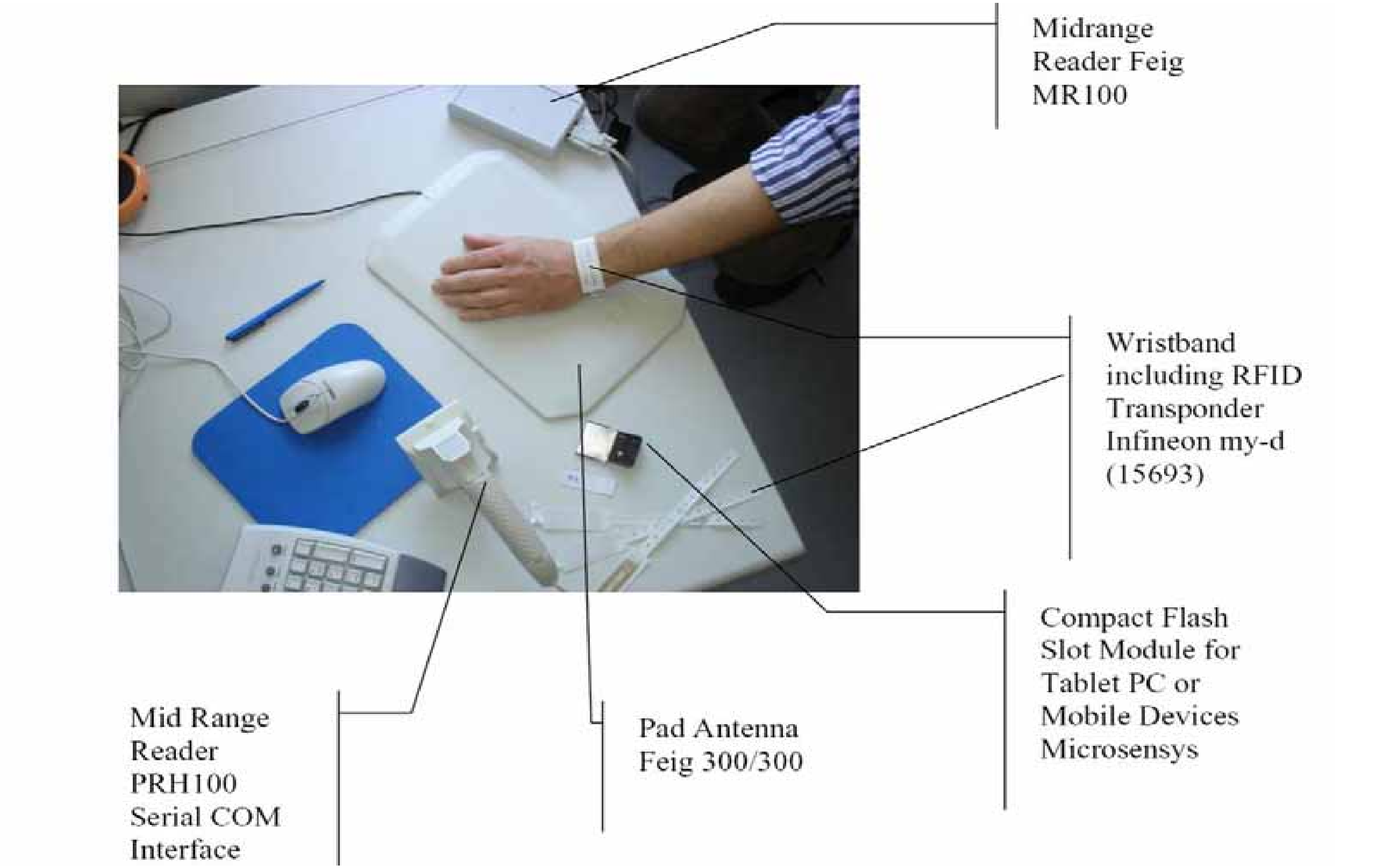
- **Total risk =** identified + unidentified risks.
- **Identified risk =** determined through various analysis techniques. The first task of system safety is to identify, within practical limitations, all possible risks. This step precedes determine the significance of the risk (severity) and the likelihood 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.*



Slide 11-16: Enhancing Patient Safety with ubiquitous devices



Holzinger, A., Schwaberger, 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.*

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.*

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

Bardram & Norskov (2008)

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

Bardram, J. E. & Norskov, 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.*

- (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

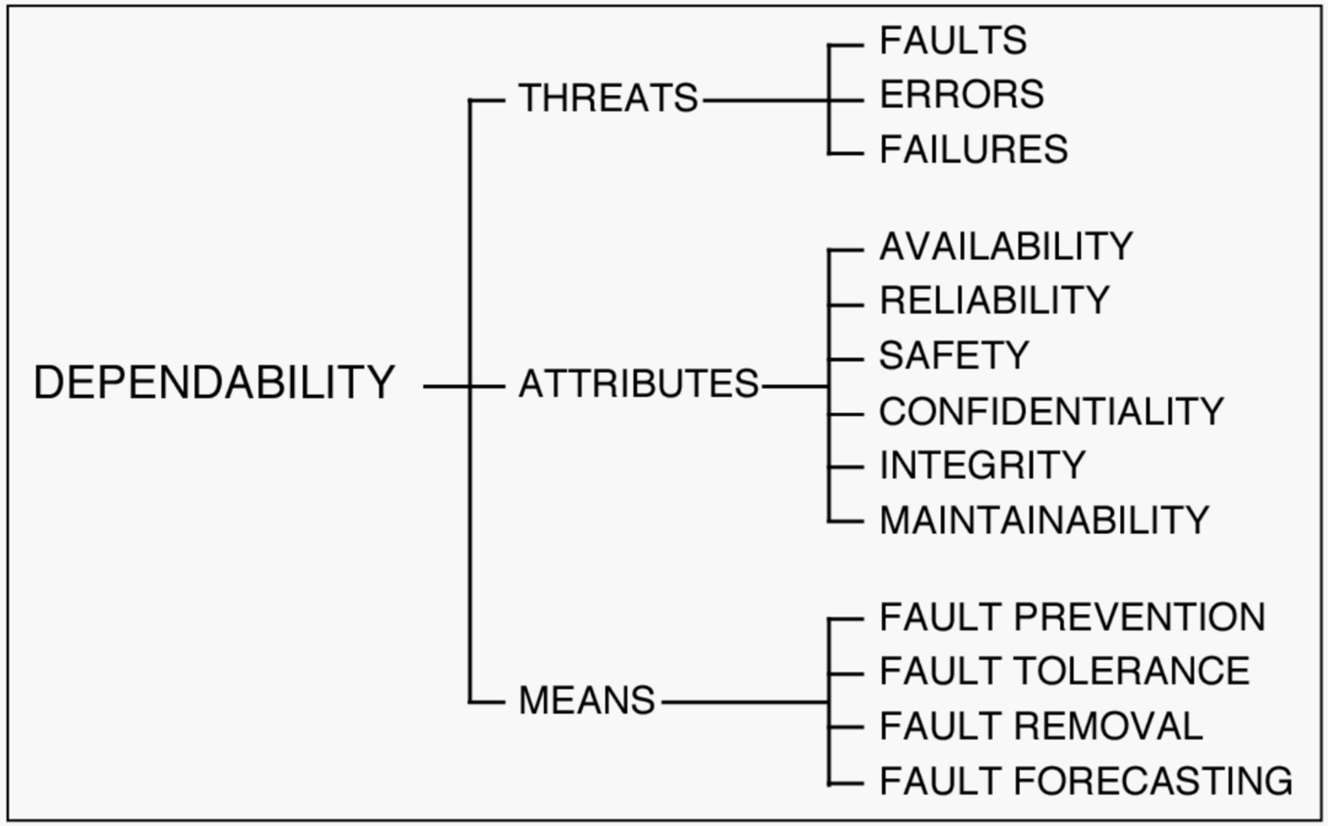
Amalberti, R., Benhamou, D., Auroy, Y. & Degos, L. (2011) Adverse events in medicine: Easy to count, complicated to understand, and complex to prevent. *Journal of Biomedical Informatics, 44, 3, 390-394.*

Slide 11-21 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,.
2	Accident	The person is not intentionally, indiscriminately, or unsuitable behavior that forms un-expect or unfortunate events.
3	Incident	Manual error or equipment shutdown causes fault of processing sporadically. No matter what, operation of the system was broken.
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.
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.
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.
10	High-alert drugs	The event maybe cause critical harm to patient result from un-normal use or manage drugs.
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) : ● Do not using any drugs (drugs were either therapy nor diagnosis) ● To change medicine therapy ● To adjust dosage (to adjust a bit dosage) ● Go to hospital over night ● Extension in hospital day ● Assisted therapy ● Causing diagnosis complicated ● Producing negative effect Result in temporary or permanent harm(disabled or death)
12	Adverse drug event ,ADE	Because the patient take medicine or medical employee has not get medicine result in the event.

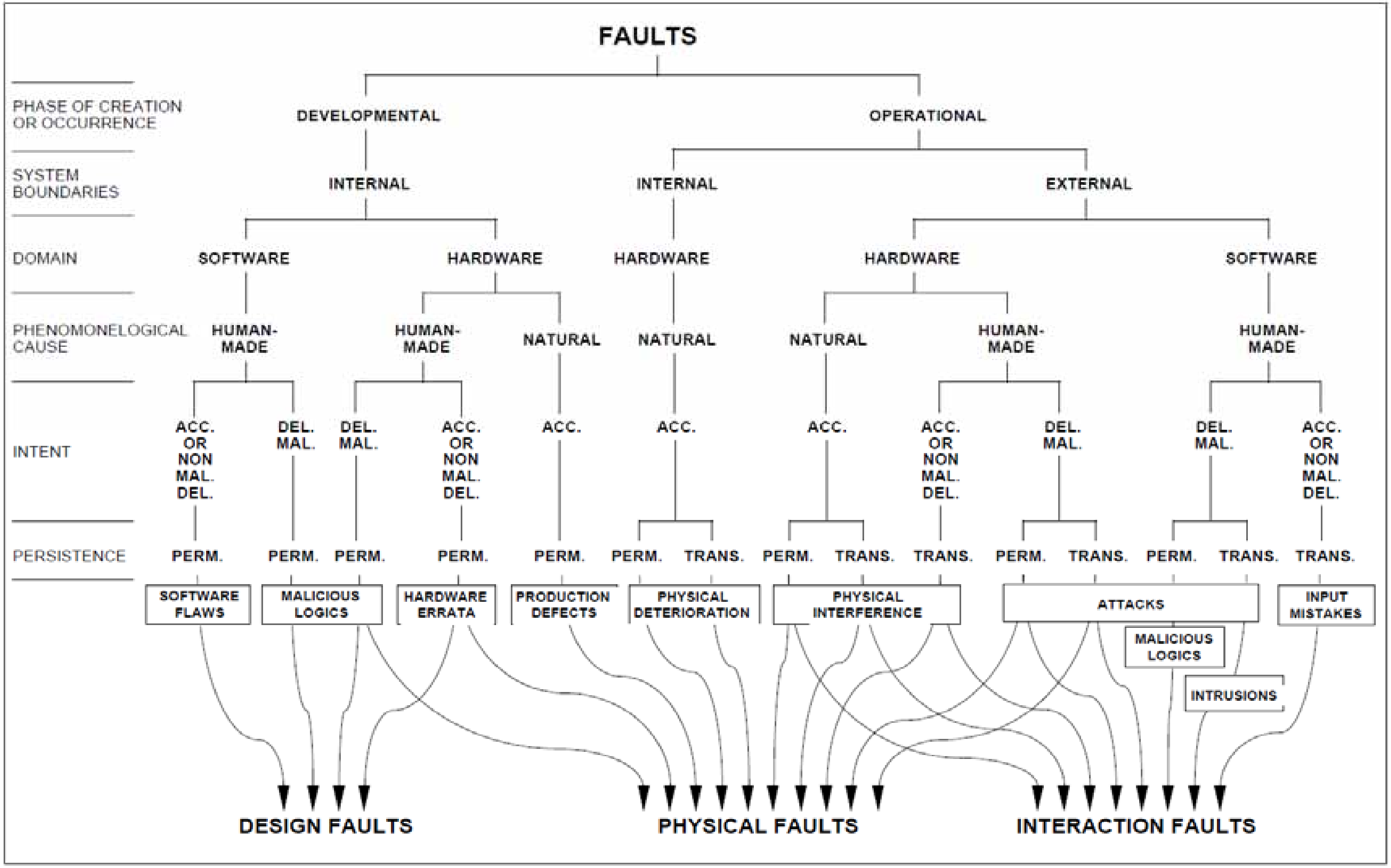
Chen, R. C., Tsan, P. C., Lee, I. Y. & Hsu, J. C. (2009). *Medical Adverse Events Classification for Domain Knowledge Extraction. 2009 Ninth International Conference on Hybrid Intelligent Systems, Shenyang (China), IEEE, 298-303.*

Slide 11-22 Safety, Security -> Technical Dependability



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.*

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



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.*

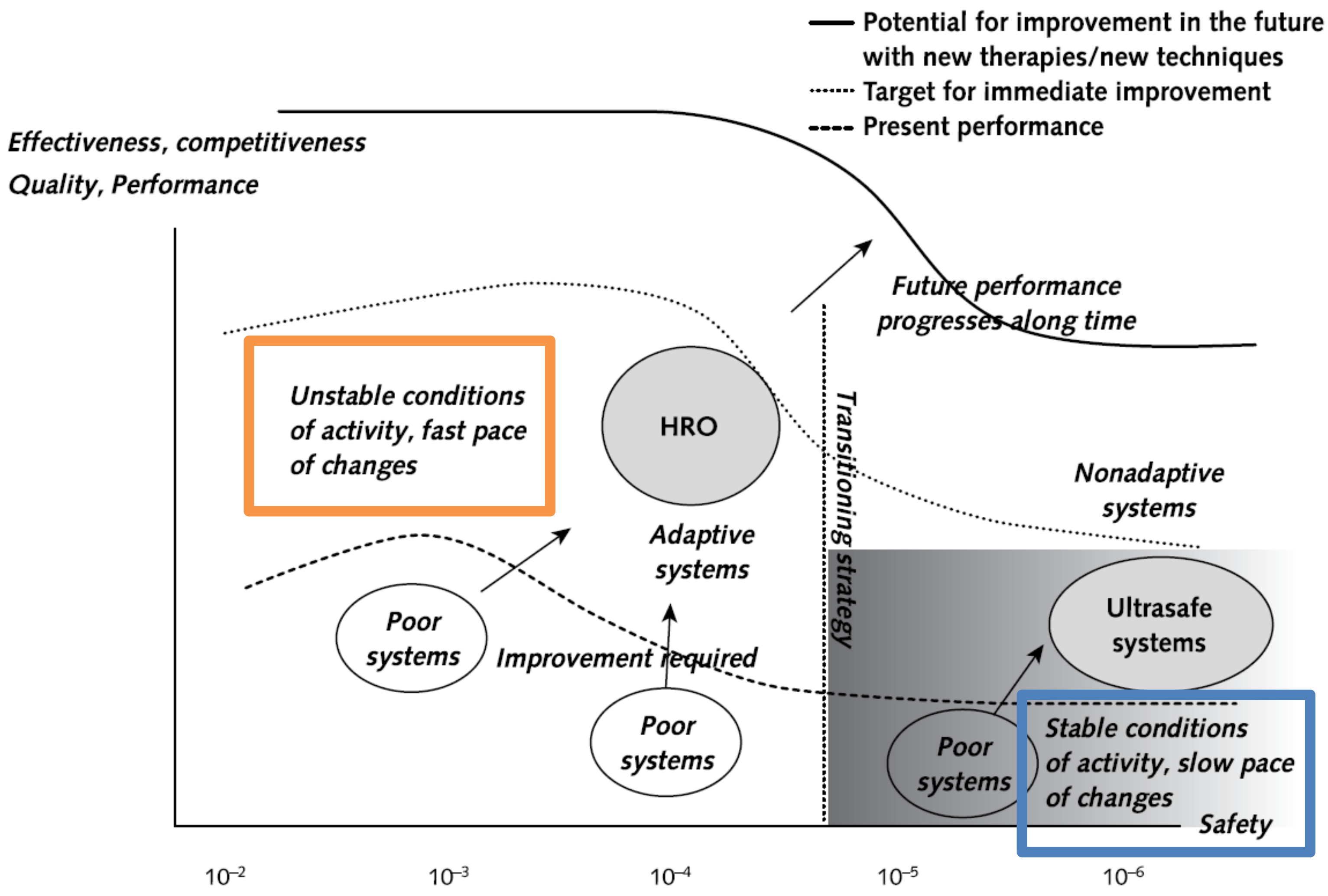
Slide 11-24 A Two-Tiered System of Medicine

Amalberti et al. (2005)

Category	Type of System: 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 1×10^{-5}, possibly 1×10^{-6}	Better than 1×10^{-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!

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



Amalberti, R., Auroy, Y., Berwick, D. & Barach, P. (2005) Five system barriers to achieving ultrasafe health care. *Annals of Internal Medicine, 142, 9, 756-764.*

02 Privacy Awareness

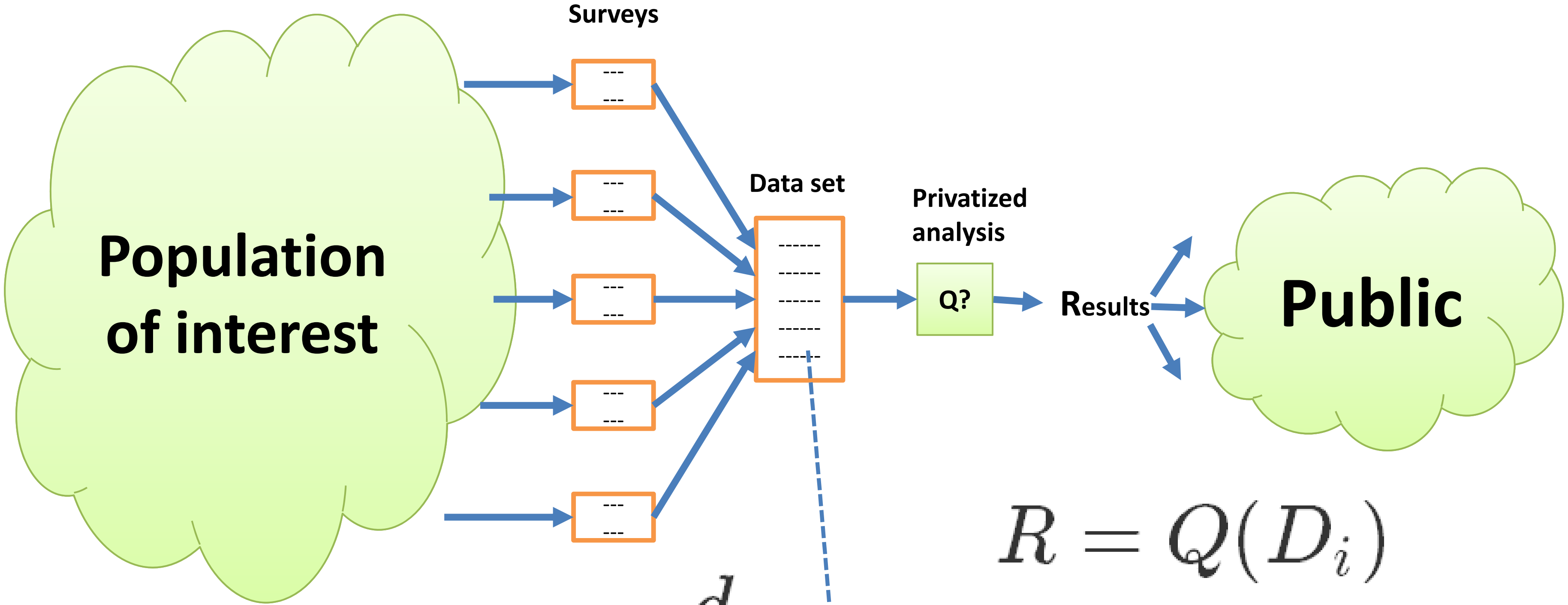
Data Privacy Training Video

https://www.youtube.com/watch?v=wAe4358amJc

Example: Survey about your music taste

- Do you like Justin Bieber?
- How many albums do you own?
- What is your gender?
- What is your age?
- Is your music taste sensitive information?
- What make you feel safe?
- Anonymous survey?

Mathematical Notation



$$R = Q(D_i)$$

$$d_i$$

$$Pop \qquad I \subseteq Pop$$

$$D_i = \{d_i | i \in I\}$$

- Would you feel safer submitting a survey if you knew that your answer would have no impact on the released results?

$$R = Q(D_{i-me}) = Q(D_i)$$

- Would you feel safer if you knew that any attacker looking at the published results R could not learn any new information about my person?

$$p(secret(me)|R) = p(secret(me))$$

Why can you not achieve that?

- If individual answers would have no impact on the released results, then the results R would have no utility at all!

$$Q(D_{i-me}) = Q(D_i) \implies Q(D_i) = Q(D_\varnothing)$$

- If R reveals that there is a strong trend in your population – everyone is age 18-22 and loves Justin Bieber – with high $p(x)$ the trend is true for you as well (even if you do not submit your survey)!

$$p(secret(me)|(secret(Pop) > p(secret(me))$$

It is getting even worse …

- If an attacker knows a function about me which is dependent on general facts about the Pop , e.g. You are twice the average age or you are in the minority gender -> releasing just those general facts provides the attacker with specific information about you!

$$(age(me) = 2 * mean_{age}) \wedge (gender(me) \neq mode_{gender}) \wedge (mean_{age} = 14) \wedge (mode_{gender} = F)$$
$$\implies (age(me) = 28) \wedge (gender(me) = M)$$

Disappointed?

Data can not be fully anonymized and remain the same useful as non-anonymized

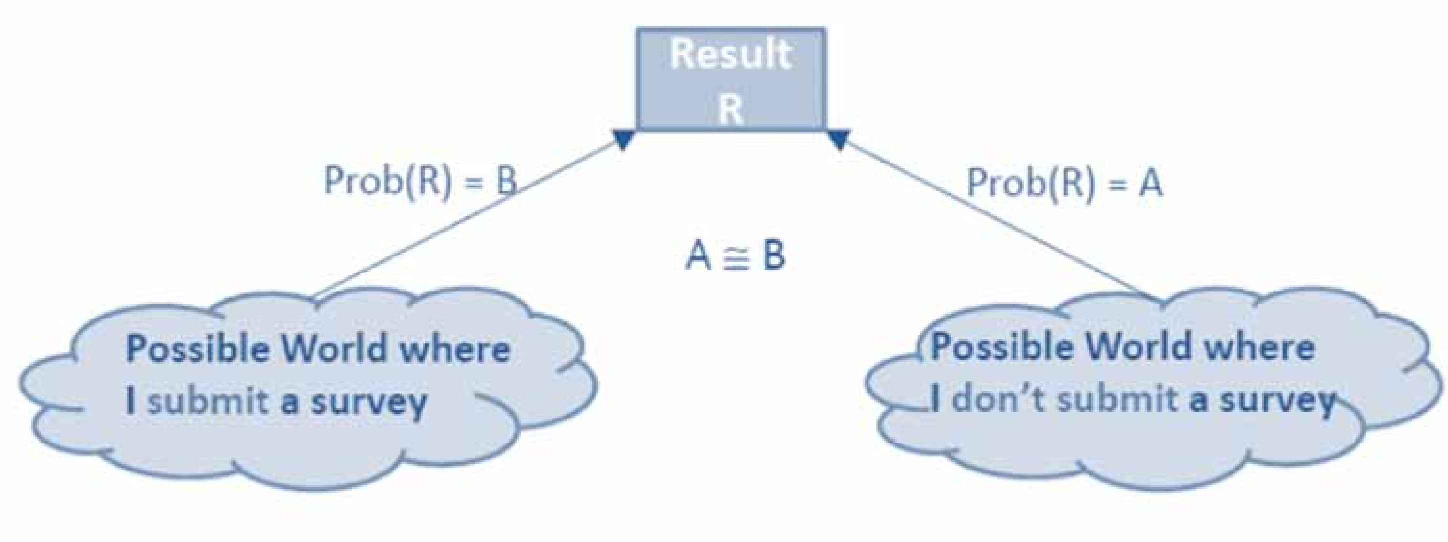
Dwork, C. & Roth, A. 2014. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9, (3–4), 211-407, doi:http://dx.doi.org/10.1561/0400000042.

One solution: Differential Privacy (Dwork, 2006)

$$\frac{\Pr(M(D) = C)}{\Pr(M(D_{\pm i}) = C)} < e^{\epsilon}$$

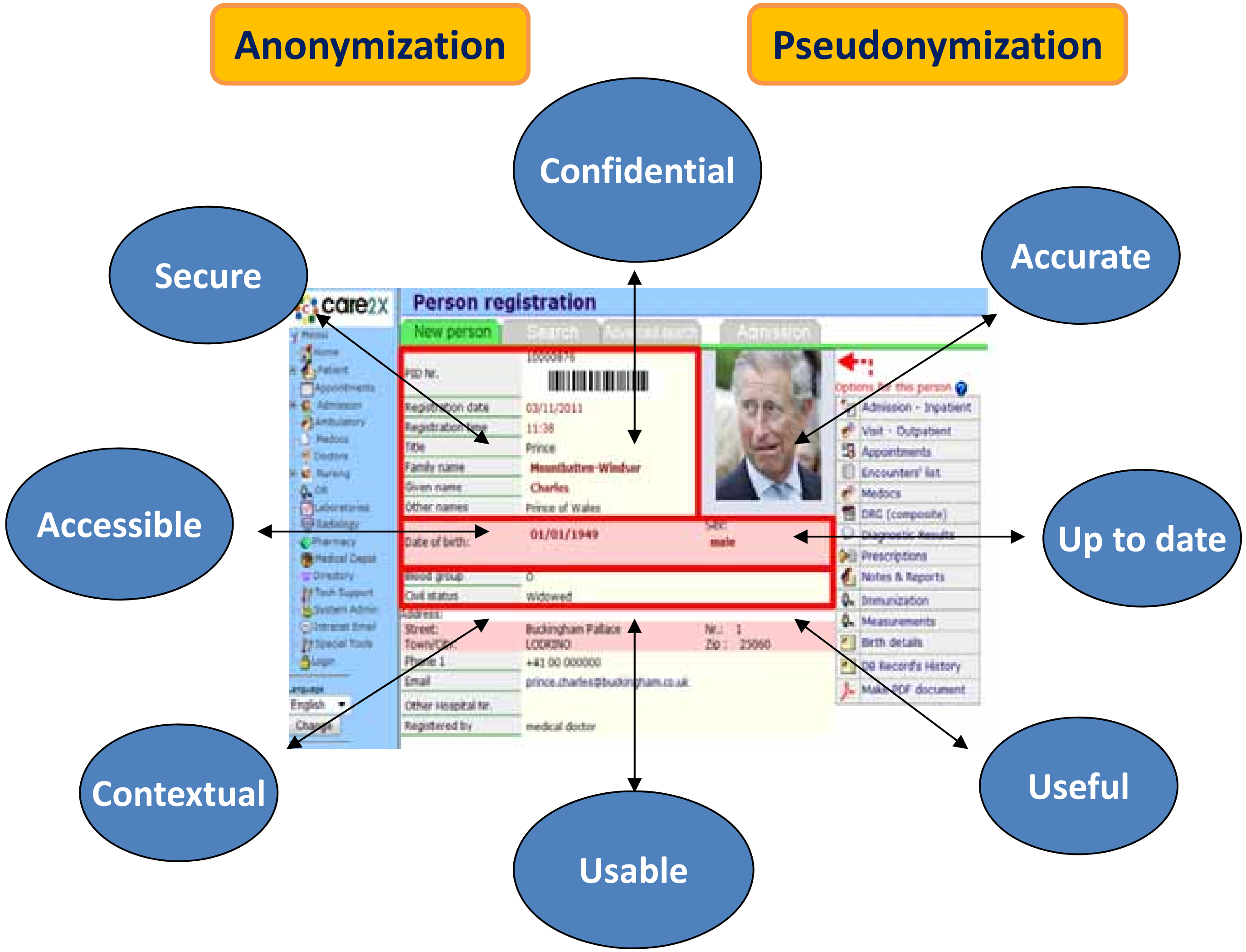
For any $|D_{\pm i} - D| \leq 1$ and any $C \in Range(M)$.

$$\frac{Prob(R \mid true\ world\ = DI)}{Prob(R \mid true\ world = D_{I\pm i})} \leq e^{\varepsilon}, \qquad for\ all\ I, i, R\ and\ small\ \varepsilon > 0$$



Dwork, C. & Roth, A. 2014. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9, (3–4), 211-407, doi:http://dx.doi.org/10.1561/0400000042.

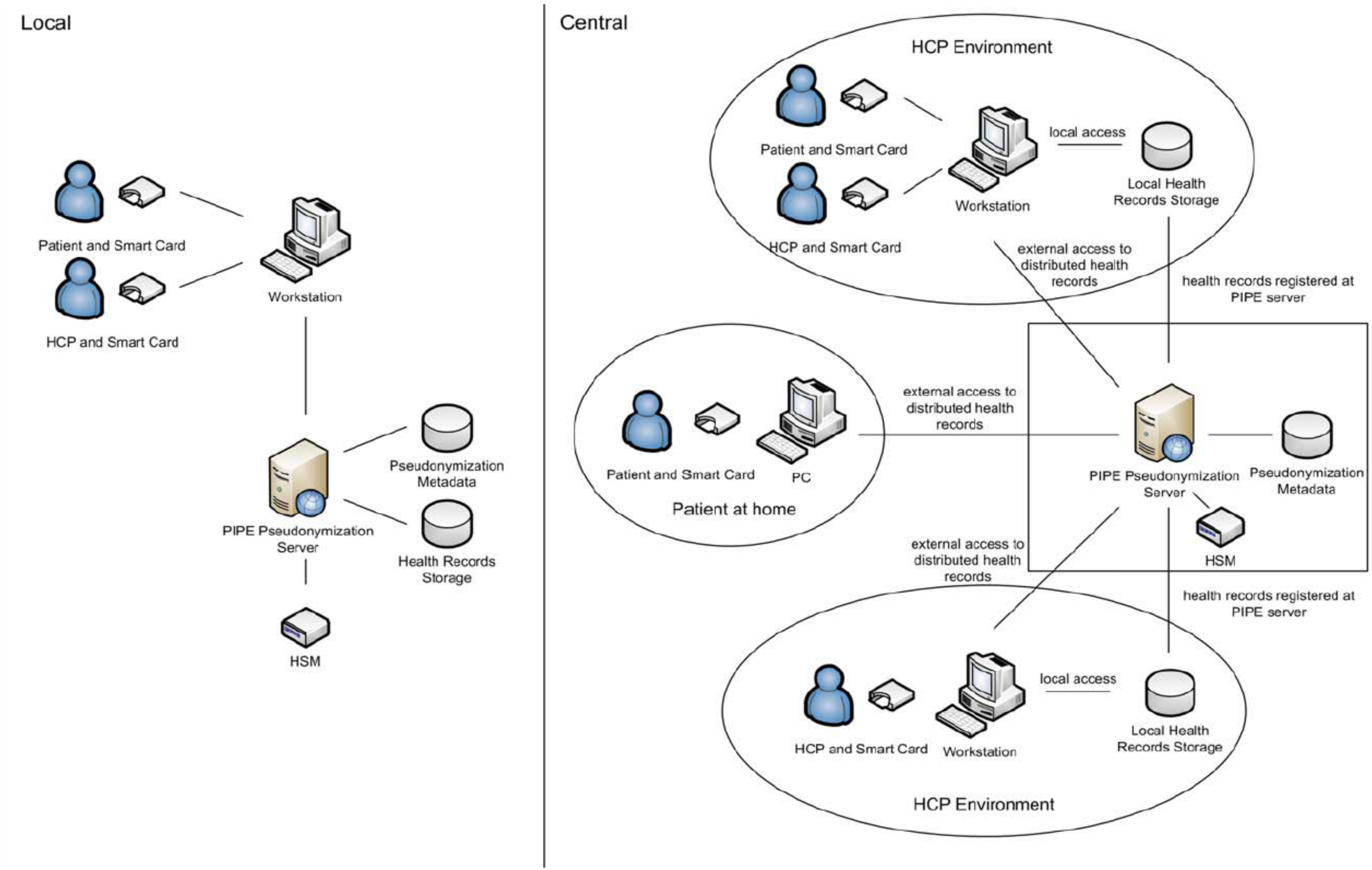
03 Privacy of Medical Data



Anonymization: Personal data cannot be re-identified (e.g. k-Anonymization)

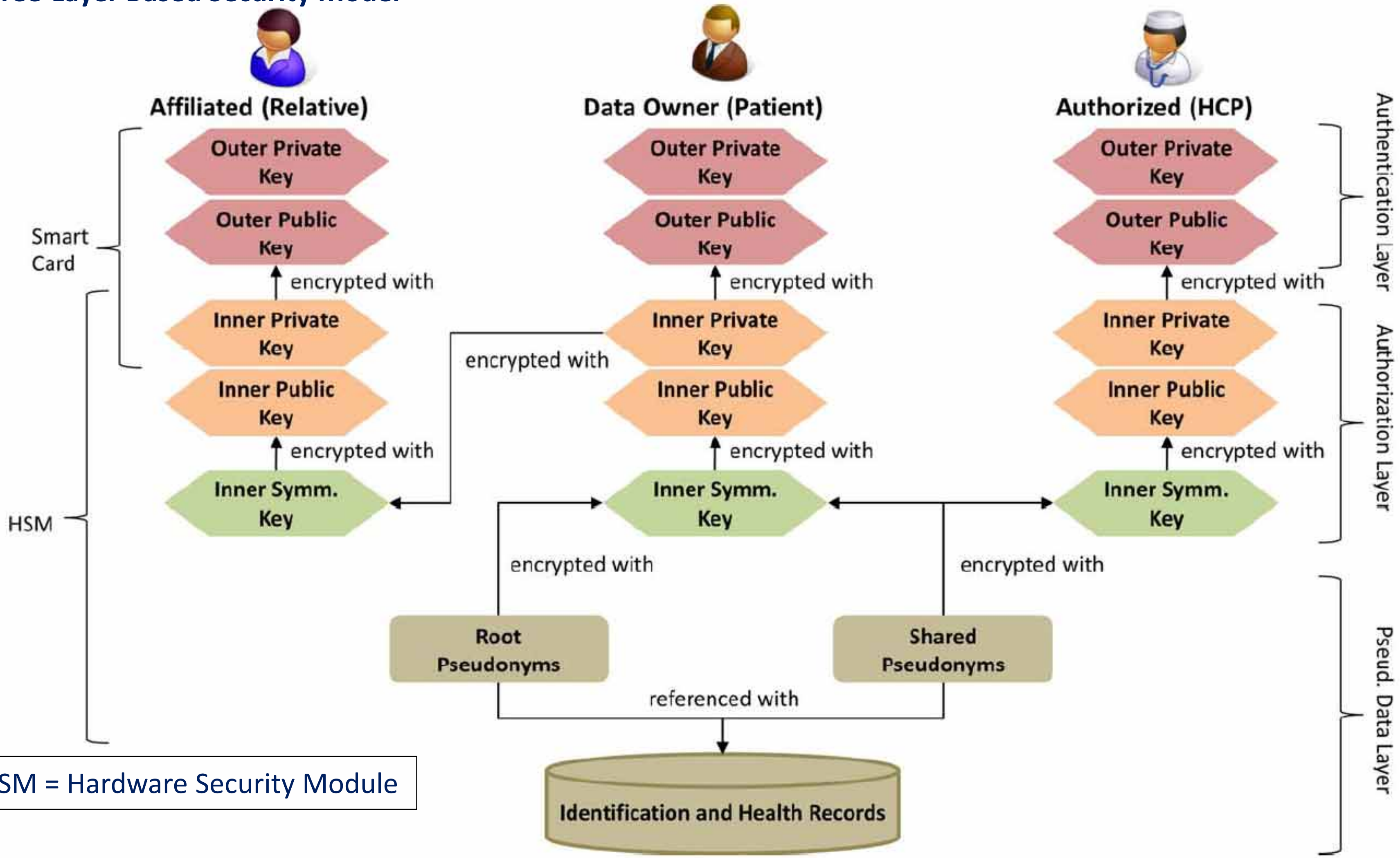
Pseudonymization: The personal data is replaced by a "pseudonym“, which allows later tracking back to the source data (re-identification)

Slide 11-27 Pseudonymization of Information for Privacy 1/8



Neubauer, T. & Heurix, J. (2011) A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics, 80, 3, 190-204.*

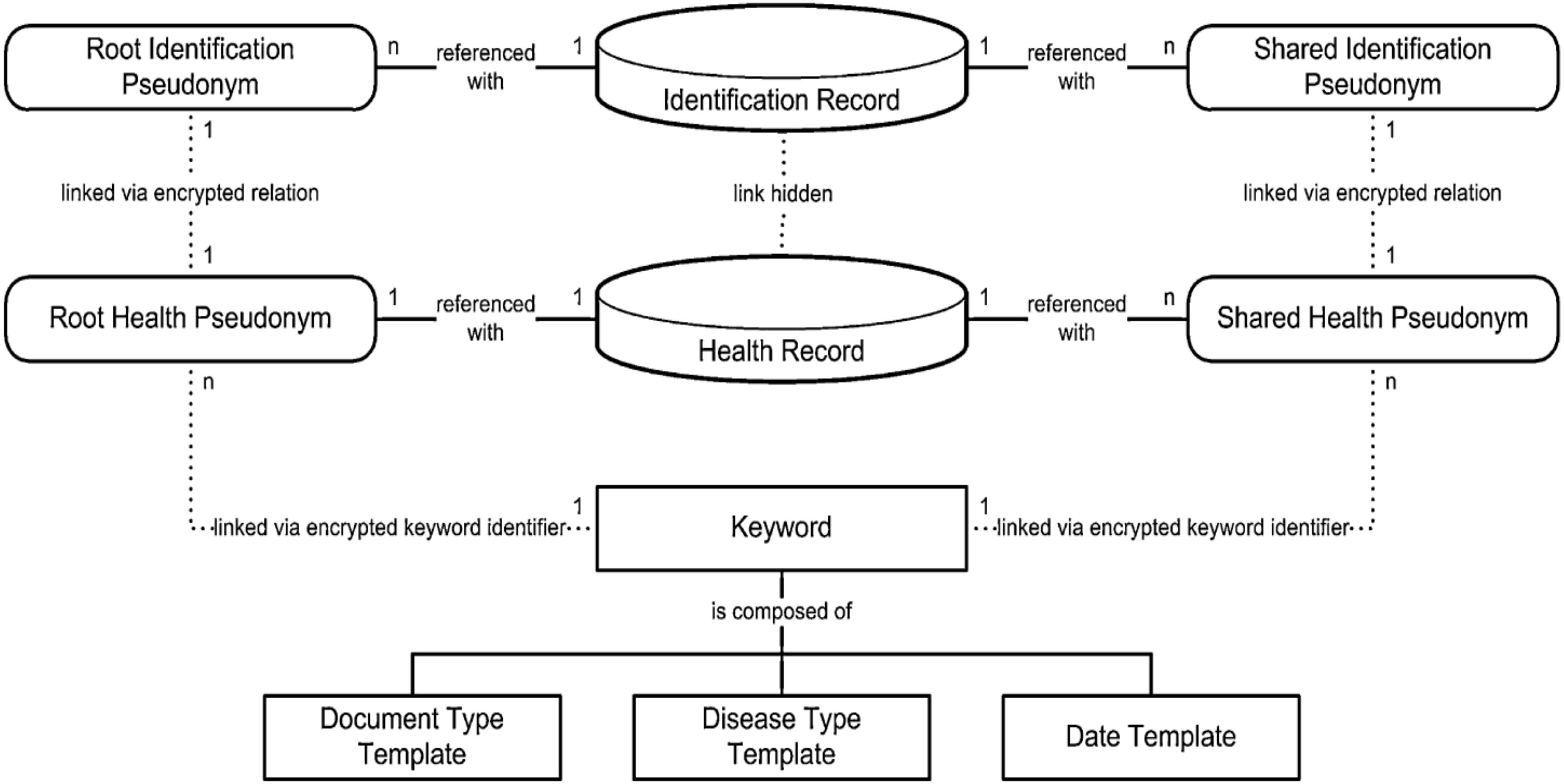
Three-Layer Based Security Model



HSM = Hardware Security Module

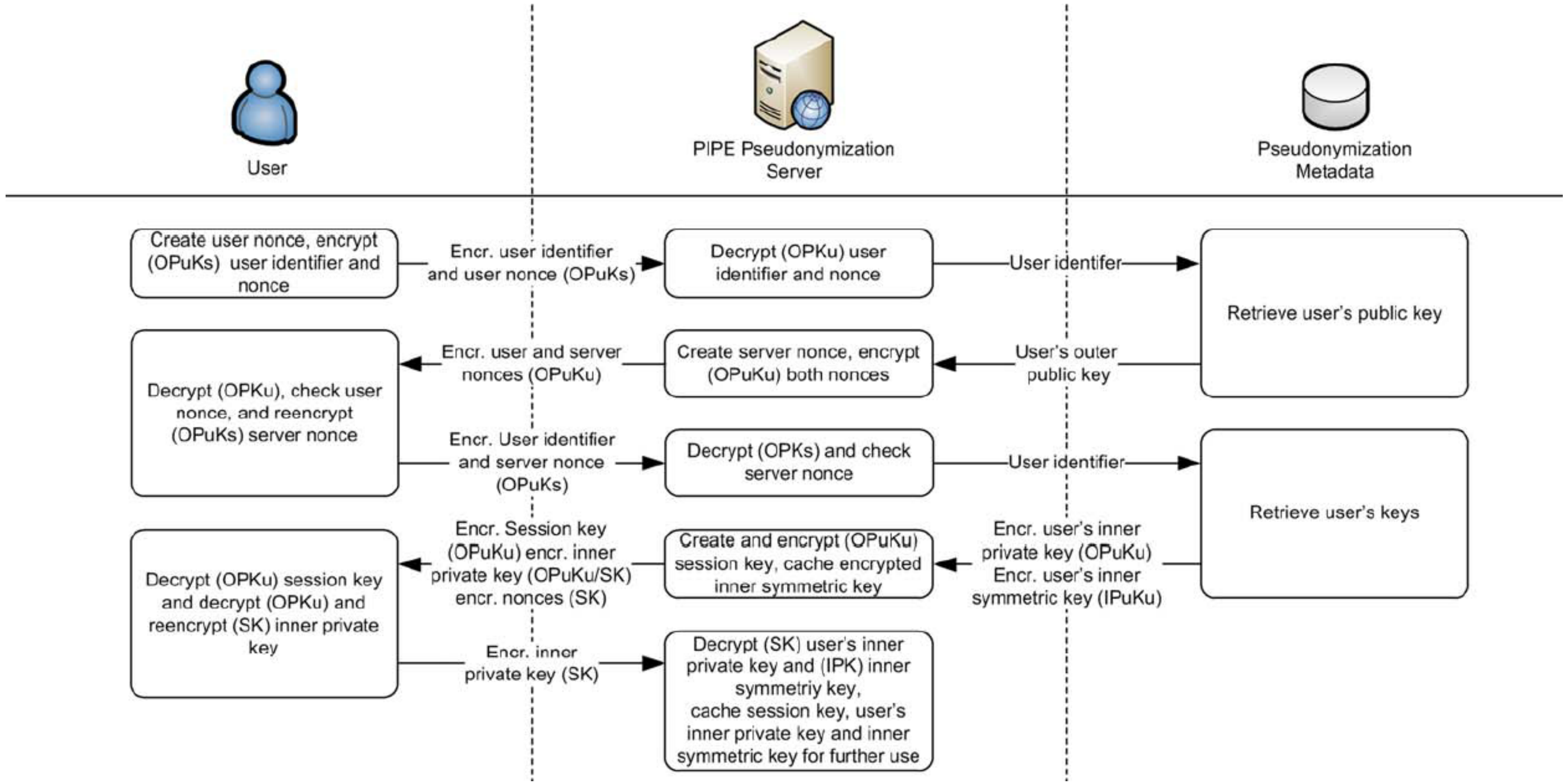
Neubauer, T. & Heurix, J. (2011) A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics, 80, 3, 190-204.*

Slide 11-29 Pseudonymization of Information for Privacy 3/8



Neubauer, T. & Heurix, J. (2011) A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics, 80, 3, 190-204.*

Slide 11-30 Pseudonymization of Information for Privacy 4/8

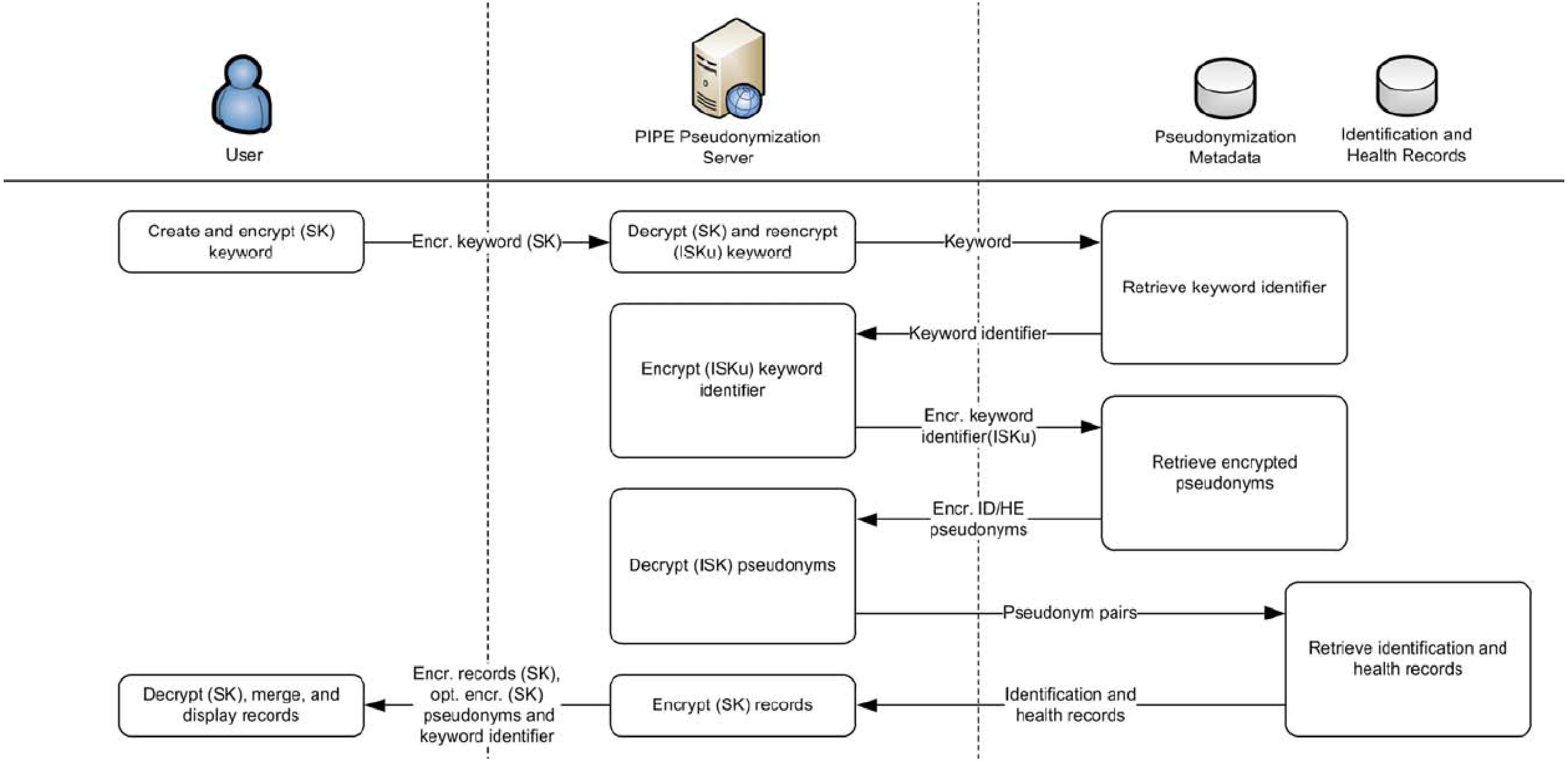


OPuK	Outer public key
OPK	Outer private key
IPuK	Inner public key
IPK	Inner private key
SK	Session key
ISK	Inner symmetric key

ID	Identification (pseudonym or record)
HE	Health (pseudonym or record)
u	User
ow	Data owner
au	Authorized user
af	Affiliated user

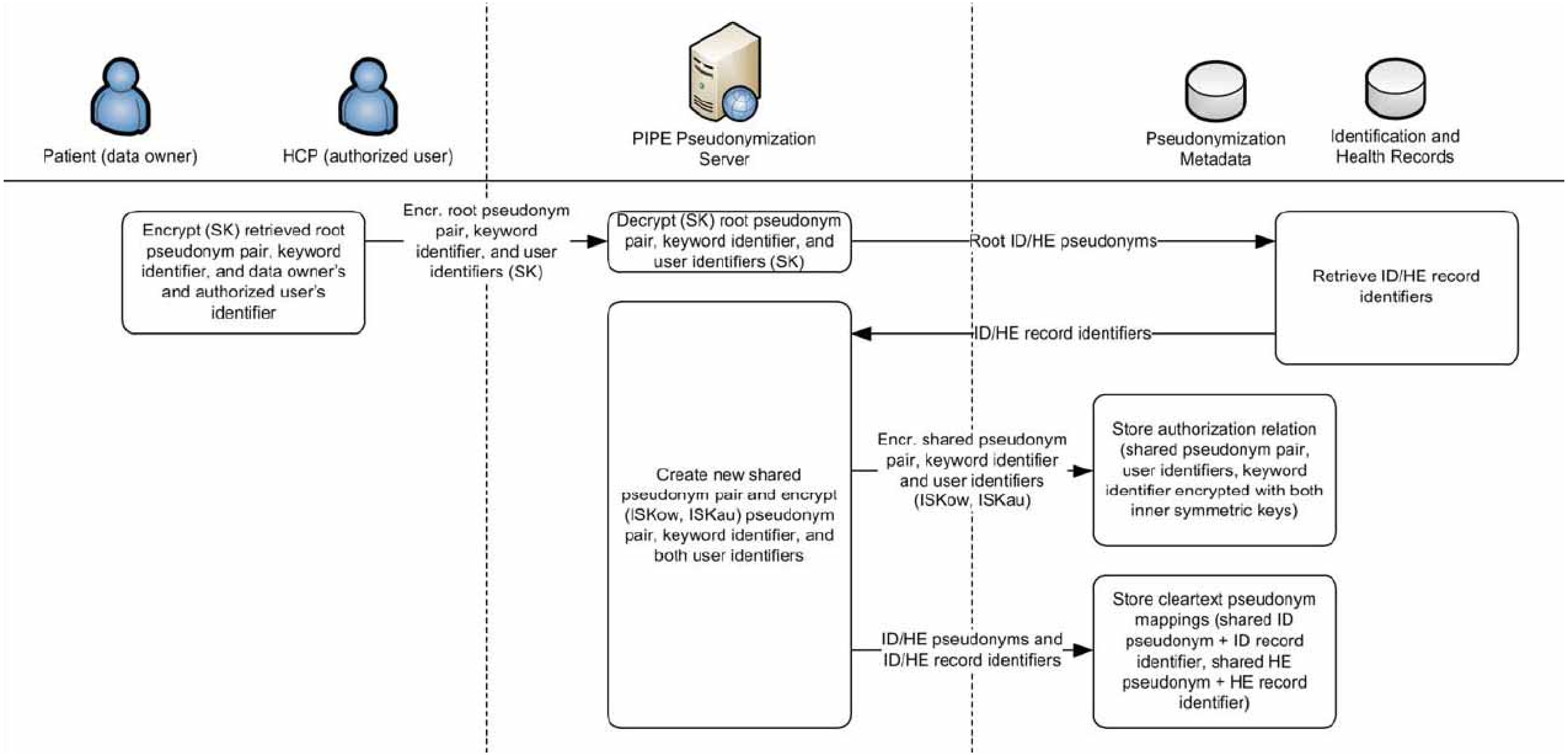
Neubauer, T. & Heurix, J. (2011) A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics, 80, 3, 190-204.*

Slide 11-31 Pseudonymization of Information for Privacy 5/8



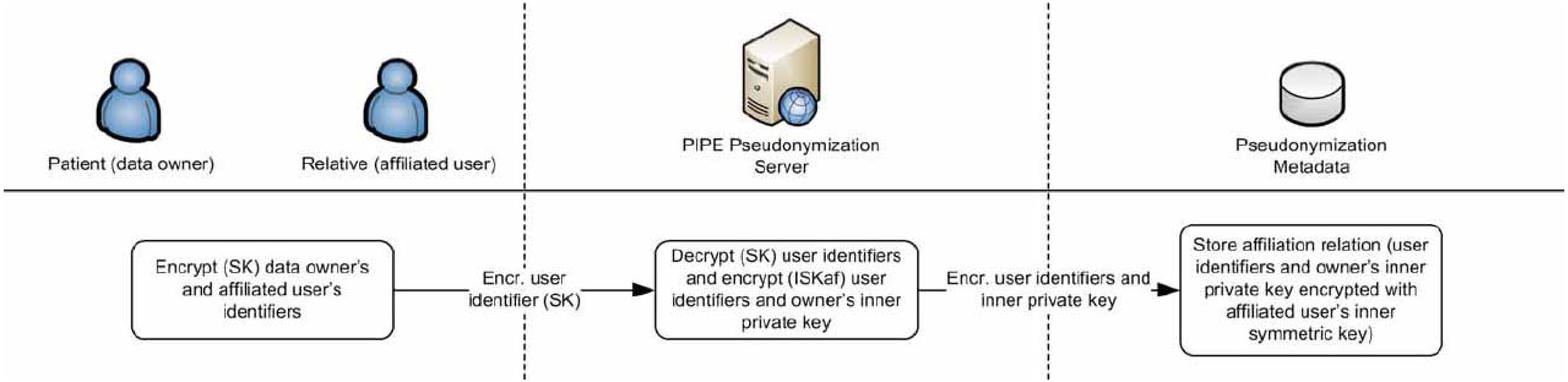
Neubauer, T. & Heurix, J. (2011) A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics, 80, 3, 190-204.*

Slide 11-32 Pseudonymization of Information for Privacy 6/8



Neubauer, T. & Heurix, J. (2011) A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics, 80, 3, 190-204.*

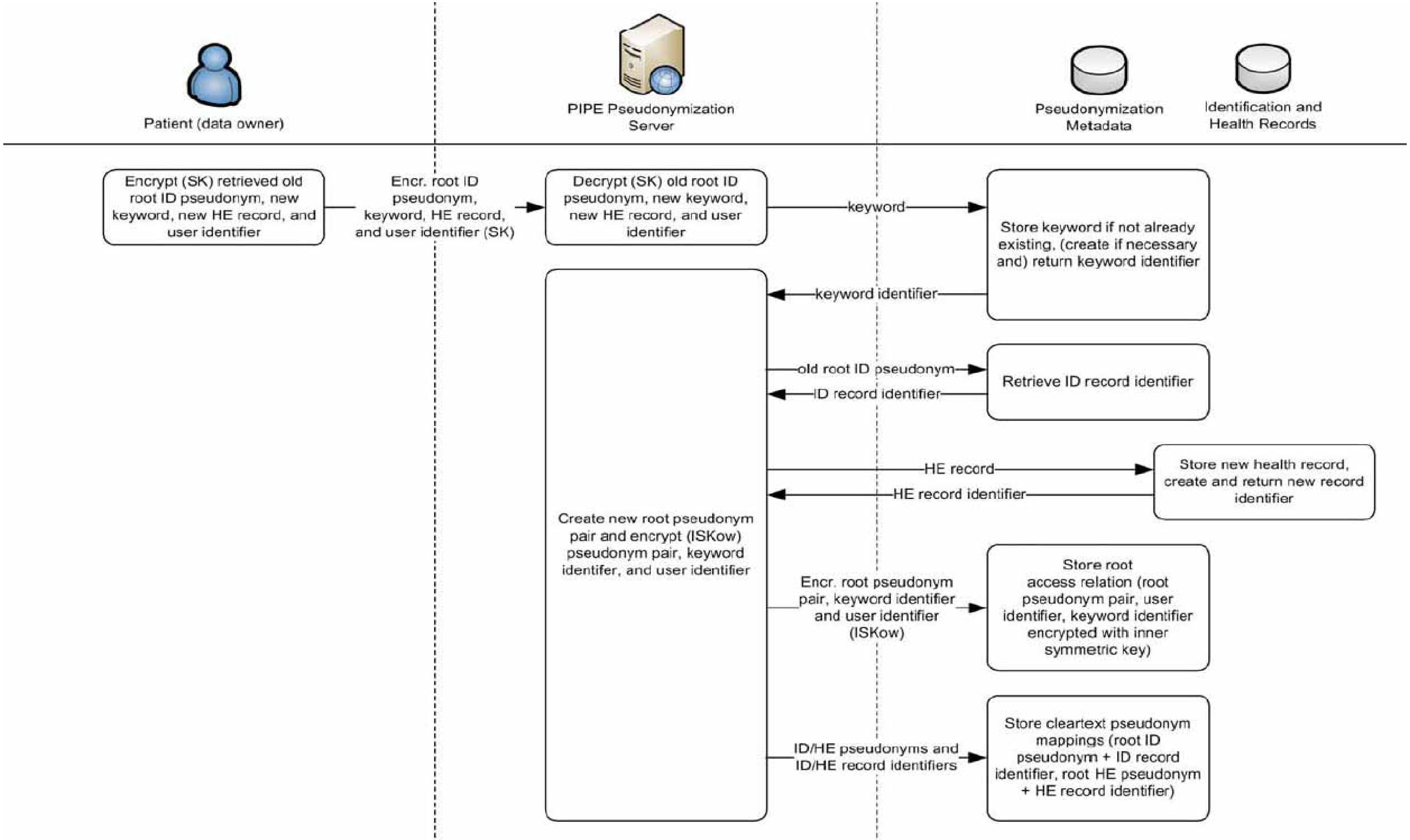
Slide 11-33 Pseudonymization of Information for Privacy



Note: Similar to authorization, a user affiliation requires that both the patient as data owner and the trusted relative as affiliated user are authenticated at the same workstation. Consequently, both user identifiers are transferred to the pseudonymization server where they are encrypted with both the users' inner symmetric keys. 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, T. & Heurix, J. (2011) A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics, 80, 3, 190-204.*

Slide 11-34 Pseudonymization of Information for Privacy (8)



Neubauer, T. & Heurix, J. (2011) A methodology for the pseudonymization of medical data. *International Journal of Medical Informatics, 80, 3, 190-204.*

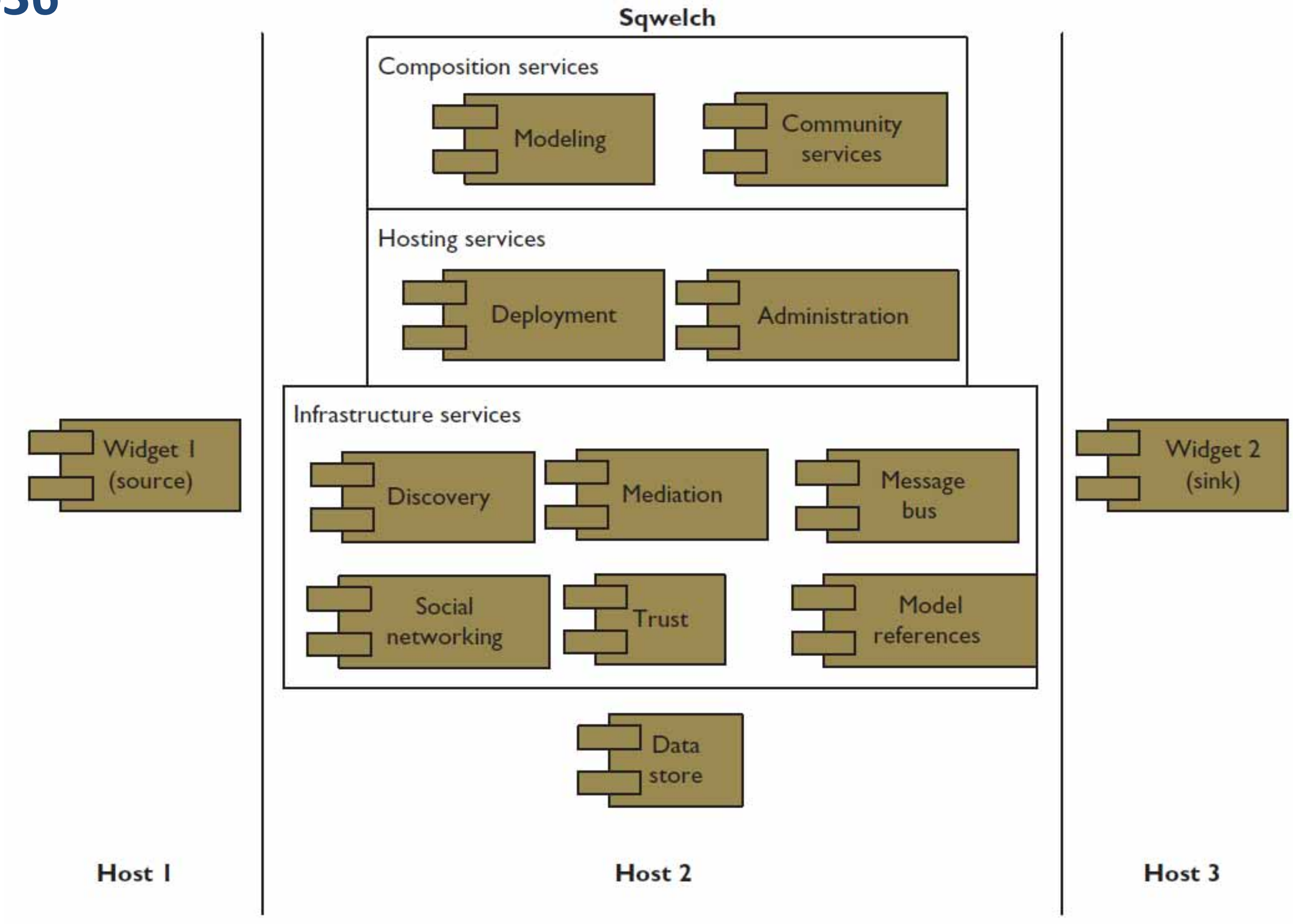
Slide 11-35 Example: private personal health record

http://healthbutler.com/

https://www.healthcompanion.com

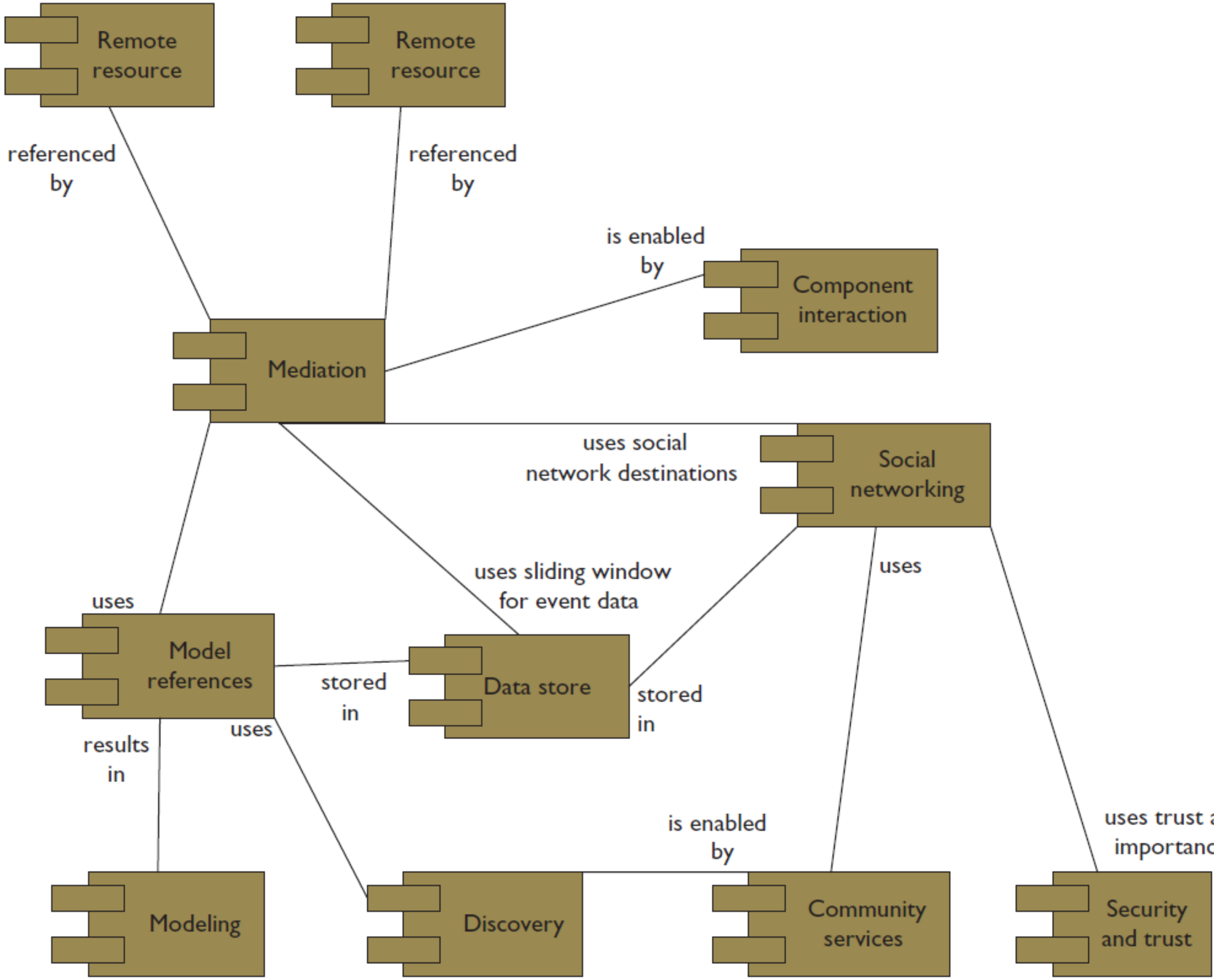
Example: Concept of a Personal Health Record System 1/4

Slide 11-36



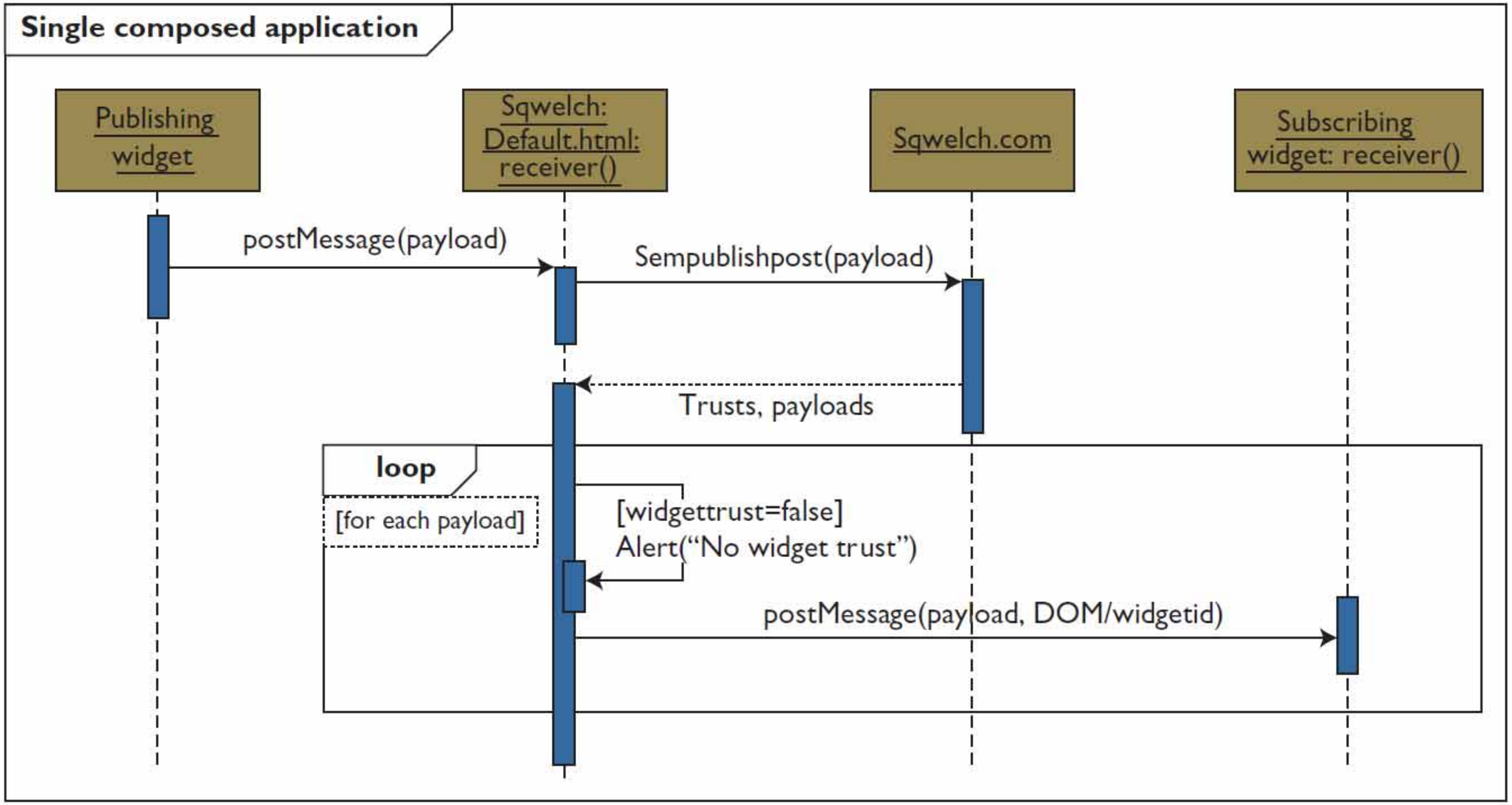
Fox, R., Cooley, J. & Hauswirth, M. (2011) Creating a Virtual Personal Health Record Using Mashups. *IEEE Internet Computing, 15, 4, 23-30.*

Slide 11-37 Example for component relationships 2/4



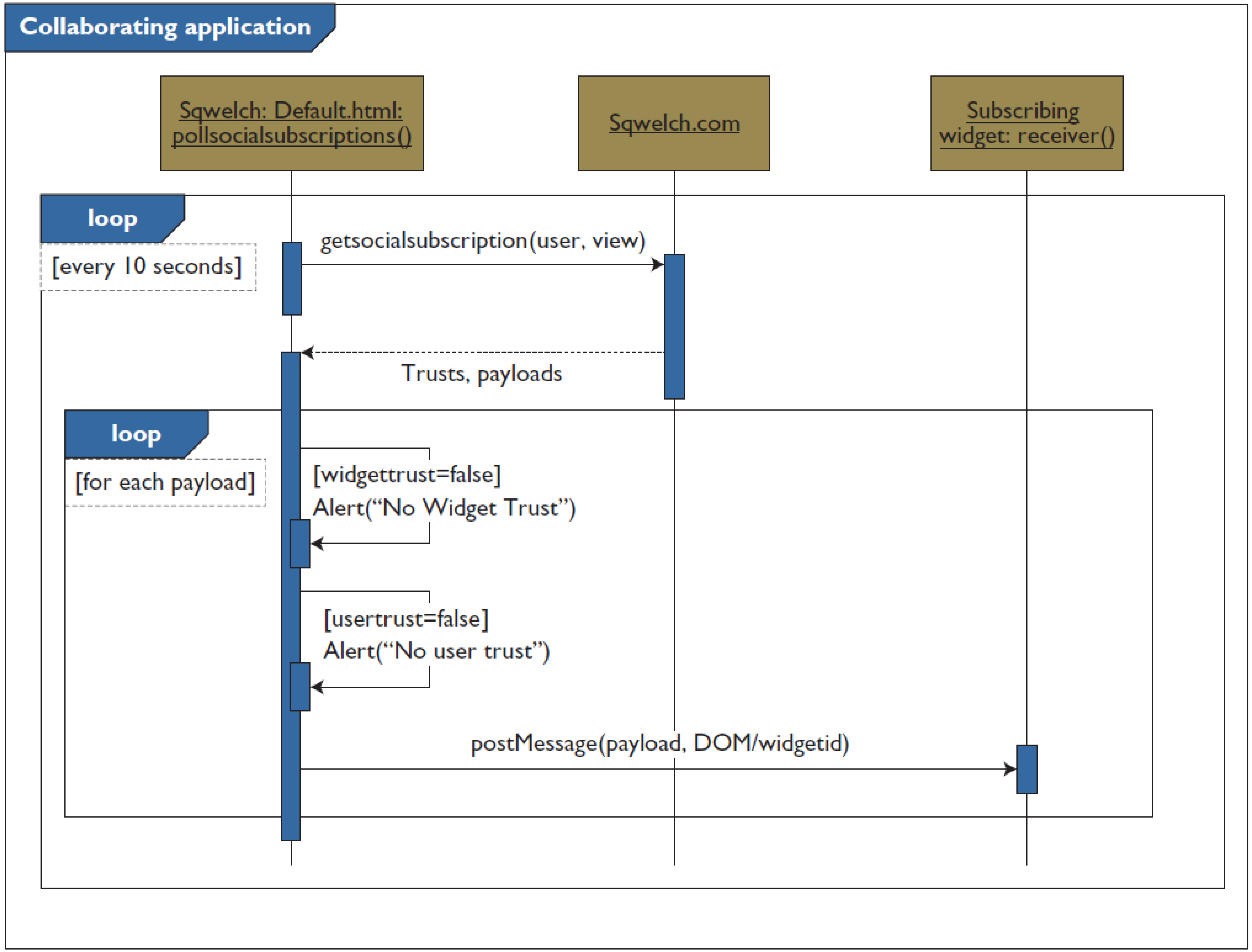
Fox et al.(2011)

Slide 11-38 Widget collaboration sequence 3/4

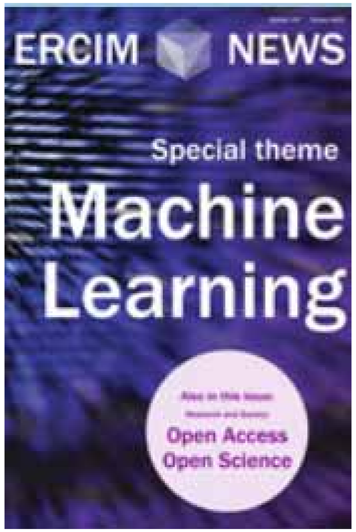


Fox et al.(2011)

Slide 11-39 User collaboration sequence 4/4



Fox et al.(2011)



04 Privacy Aware Machine Learning

Malle, B., Kieseberg, P., Schrittwieser, S. & Holzinger, A. 2016. Privacy Aware Machine Learning and the “Right to be Forgotten”. ERCIM News (special theme: machine learning), 107, (3), 22-23.

http://ercim-news.ercim.eu/en107/special/privacy-aware-machine-learning-and-the-right-to-be-forgotten


ETTA ©1999 FORT WORTH STAR-TELEGRAM
HULME
WE CHECKED YOUR CONFIDENTIAL MEDICAL RECORDS ON THE INTERNET. CHEESE AND ANCHOVIES WOULD BE BAD FOR YOU, SO WE LEFT THEM OFF.
PIZZA

General Privacy Principles

- Lawfulness, **fairness** and transparency
- **Necessity** of data collection and processing
- **Purpose** specification and purpose binding
- There are **no "non-sensitive" data**
- The right to information **correction**
- Deleting or blocking of incorrect/ illegally stored data
- Supervision by independent data protection authority with sanctions
- Adequate organizational and technical safeguards

Fischer-Hübner, S. 2001. IT-security and privacy: design and use of privacy-enhancing security mechanisms, Springer.

Privacy protection can be undertaken by …

- Privacy and data protection **laws** promoted by government
- **Supervision** by independent data protection authority (Datenschutzbeauftragte(r))
- Self-regulation for fair information practices by **codes of conducts** promoted by businesses
- **Privacy-enhancing technologies (PETs)** adopted by individuals
- Privacy education of consumers and IT professionals

With 2018 EU law: The right to be forgotten

- Basically: A user has the right to have their data deleted from a database upon request
- In some past cases, the requirement only meant deletion from a search index (due to EU tech ignorance)
- From 2018 onwards, the "right to be forgotten" will be part of the new EU data protection & privacy act (look up exact wording)
- Since one cannot foresee which (non-existing) laws will be enforced by the European bureaucracy in the future (see Apple..), it would be wise to be prepared…

Malle, B., Kieseberg, P., Weippl, E. & Holzinger, A. 2016. The right to be forgotten: Towards Machine Learning on perturbed knowledge bases. Springer Lecture Notes in Computer Science LNCS 9817. Heidelberg, Berlin, New York: Springer, pp. 251-256, doi:10.1007/978-3-319-45507-5_17.

This poses a big privacy problem

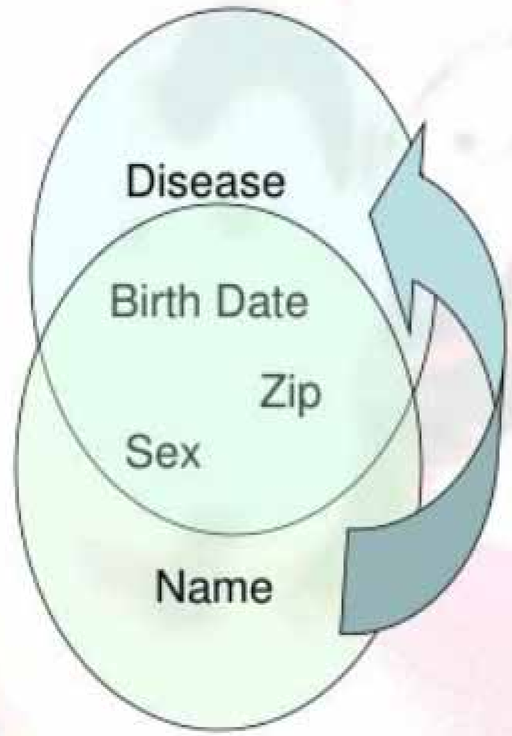
87 % of the population in the USA can be uniquely re-identified by Zip-Code, Gender and date of birth

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



Samarati, P. 2001. Protecting respondents identities in microdata release. IEEE Transactions on Knowledge and Data Engineering, 13, (6), 1010-1027, doi:10.1109/69.971193.

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.

- **K-Anonymity** … 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** … 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's distribution in the whole data set (local distribution must resemble the global distribution)

Example Privacy Aware Machine Learning (PAML)

The Right to Be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases

Bernd Malle[1,2], Peter Kieseberg[1,2], Edgar Weippl[2], and Andreas Holzinger[1](✉)

[1] Holzinger Group HCI-KDD, Institute for Medical Informatics, Statistics and Documentation, Medical University Graz, Graz, Austria
{b.malle,a.holzinger}@hci-kdd.org

[2] SBA Research gGmbH, Favoritenstrae 16, 1040 Vienna, Austria
PKieseberg@sba-research.org

Abstract. Today's increasingly complex information infrastructures represent the basis of any data-driven industries which are rapidly becoming the 21st century's economic backbone. The sensitivity of those infrastructures to disturbances in their knowledge bases is therefore of crucial interest for companies, organizations, customers and regulating bodies. This holds true with respect to the direct provisioning of such information in crucial applications like clinical settings or the energy industry, but also when considering additional insights, predictions and personalized services that are enabled by the automatic processing of those data. In the light of new EU Data Protection regulations applying from 2018 onwards which give customers the right to have their data deleted on request, information processing bodies will have to react to these changing jurisdictional (and therefore economic) conditions. Their choices include a re-design of their data infrastructure as well as preventive actions like anonymization of databases per default. Therefore, insights into the effects of perturbed/anonymized knowledge bases on

Malle, B., Kieseberg, P., Weippl, E. & Holzinger, A. 2016. The right to be forgotten: Towards Machine Learning on perturbed knowledge bases. Springer Lecture Notes in Computer Science LNCS 9817. Heidelberg, Berlin, New York: Springer, pp. 251-256, doi:10.1007/978-3-319-45507-5_17.

Keywords: Machine learning · Knowledge bases · Right to be forgotten · Perturbation · Anonymization · k-anonymity · SaNGreeA ·

Properties & General Approach (see Malle et al. 2016)

Data properties => Reduce granularity

Name	Age	Zip	Gender	Disease
Alex	25	41076	Male	Allergies
…	…	…	…	…

- Identifiers := immediately reveal identity
  - name, email, phone nr., SSN

  => DELETE

- Sensitive data
  - medical diagnosis, symptoms, drug intake, income

  => NECESSARY, KEEP

- Quasi-Identifiers := used in combination to retrieve identity
  - Age, zip, gender, race, profession, education

  => MAYBE USEFUL

  => MANIPULATE / GENERALIZE

K Anonymization criterion

k-anonymity: for every entry in the DS, there must be at least k-1 identical entries (w.r.t. QI's) => this is 3-anon:

Node	Name	Age	Zip	Gender	Disease
X1	Alex	25	41076	Male	Allergies
X2	Bob	25	41075	Male	Allergies
X3	Charlie	27	41076	Male	Allergies
X4	Dave	32	41099	Male	Diabetes
X5	Eva	27	41074	Female	Flu
X6	Dana	36	41099	Female	Gastritis
X7	George	30	41099	Male	Brain Tumor
X8	Lucas	28	41099	Male	Lung Cancer
X9	Laura	33	41075	Female	Alzheimer

Node	Age	Zip	Gender	Disease
X1	25-27	4107*	Male	Allergies
X2	25-27	4107*	Male	Allergies
X3	25-27	4107*	Male	Allergies
X4	30-36	41099	*	Diabetes
X5	27-33	410**	*	Flu
X6	30-36	41099	*	Gastritis
X7	30-36	41099	*	Brain Tumor
X8	27-33	410**	*	Lung Cancer
X9	27-33	410**	*	Alzheimer

Limits of anonymization

Trade-off between:

- Data utility => min. information loss
- Privacy => max. information loss

Both can be easily achieved (but not together ☺)

Node	Name	Age	Zip	Gender	Disease
X1	Alex	25	41076	Male	Allergies
X2	Bob	25	41075	Male	Allergies
X3	Charlie	27	41076	Male	Allergies
X4	Dave	32	41099	Male	Diabetes
X5	Eva	27	41074	Female	Flu
X6	Dana	36	41099	Female	Gastritis
X7	George	30	41099	Male	Brain Tumor
X8	Lucas	28	41099	Male	Lung Cancer
X9	Laura	33	41075	Female	Alzheimer

Node	Age	Zip	Gender	Disease
X1	*	*	*	Allergies
X2	*	*	*	Allergies
X3	*	*	*	Allergies
X4	*	*	*	Diabetes
X5	*	*	*	Flu
X6	*	*	*	Gastritis
X7	*	*	*	Brain Tumor
X8	*	*	*	Lung Cancer
X9	*	*	*	Alzheimer

- Generalization (hierarchies)
  - fixed ruleset
  - range partitioning (numerical values...)

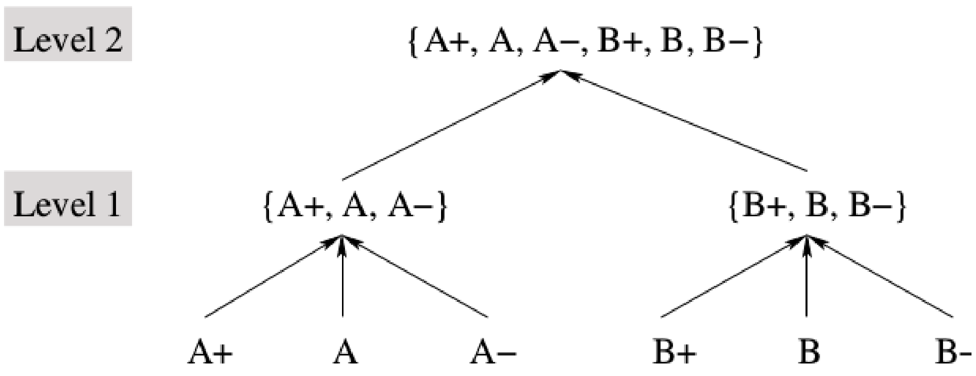


Figure 1: A possible generalization hierarchy for the attribute "Quality".

- Suppression
  - Special case of generalization (with one level)

Graphics Source: Bayardo, R. J., & Agrawal, R. (2005, April). Data privacy through optimal k-anonymization. In Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on (pp. 217-228). IEEE.

"Social Network Greedy Anonymization" (SaNGreeA)

- Anonymizes a dataset w.r.t 2 information categories:
  - Feature vector values => traditional, tabular
  - Graph structure => edge configuration
- Based on the concept of 'greedy' clustering
- Which poses the question:
  - How do we choose the next node to add to a cluster w.r.t the above two criteria?

! We need some (good) cost functions !

- Generalization Information loss (GIL)
  - Based on content of nodes

- We assume
  - Continuous properties (age, body height, …)
    - Candidate Nodes hold a particular value
    - Clusters have either particular value (at the start) or a generalized range
    - In order to incorporate the node into the cluster, we may have to generalize this range further, increasing the cost.

  - Categorical properties (work class, native-country, …)
    - Same preconditions as above
    - We use generalization hierarchies to determine the cost of clustering

Anonymization – Greedy clustering 3/4

- Generalization information loss function:

$$GIL(cl) = |cl| \cdot \left(\sum_{j=1}^{s} \frac{size(gen(cl)[N_j])}{size(min_{X \in \mathcal{N}}(X[N_j]), max_{X \in \mathcal{N}}(X[N_j]))} + \sum_{j=1}^{t} \frac{height(\Lambda(gen(cl)[C_j]))}{height(\mathcal{H}_{C_j})}\right),$$

where:

- $|cl|$ denotes the cluster cl's cardinality;
- $size([i_1, i_2])$ is the size of the interval $[i_1, i_2]$, i.e., $(i_2 - i_1)$;
- $\Lambda(w)$, $w \in \mathcal{H}_{C_j}$ is the subhierarchy of $\mathcal{H}_{C_j}$ rooted in w;
- $height(\mathcal{H}_{C_j})$ denotes the height of the tree hierarchy $\mathcal{H}_{C_j}$.

Campan, A. and Truta, T.M., 2009. Data and structural k-anonymity in social networks. In Privacy, Security, and Trust in KDD (pp. 33-54). Springer Berlin Heidelberg.

Anonymization – Greedy clustering 4/4

- Example GIL:

  - age_range overall = [11 – 91]
  - In order to cluster some nodes, we need to generalize 27 to [20 - 30]
  - Cost = (30-20)/(91-11) = 1/8

  - Given a generalization hierarchy 'native-country' with 4 levels
  - In order to cluster, we need to generalize 'Austria', 'France', or 'Portugal' to 'Western Europe', which is 1 level higher
  - Cost = 1/4

Greedy anonymization Main Loop

```python
## MAIN LOOP
for node in adults:
    if node in added and added[node] == True:
        continue
    # Initialize new cluster with given node
    cluster = CL.NodeCluster(node, adults, adj_list, gen_hierarchies)
    # Mark node as added
    added[node] = True
    # SaNGreeA inner loop - Find nodes that minimize costs and
    # add them to the cluster since cluster_size reaches k
    while len(cluster.getNodes()) < GLOB.K_FACTOR:
        best_cost = float('inf')
        for candidate, v in ((k, v) for (k, v) in adults.items() if k > node):
            if candidate in added and added[candidate] == True:
                continue
            cost = cluster.computeNodeCost(candidate)
            if cost < best_cost:
                best_cost = cost
                best_candidate = candidate
        cluster.addNode(best_candidate)
        added[best_candidate] = True
    # We have filled our cluster with k entries, push it to clusters
    clusters.append(cluster)
```

Weight Vectors 1/2

[51 - 76]	*	North_America	Male	*	Married-civ-spouse
[51 - 76]	*	North_America	Male	*	Married-civ-spouse
[51 - 76]	*	North_America	Male	*	Married-civ-spouse

57 | Private | United-States | Male | White | Married-civ-spouse

[48 - 70]	Private	America	Male	White	*
[48 - 70]	Private	America	Male	White	*
[48 - 70]	Private	America	Male	White	*

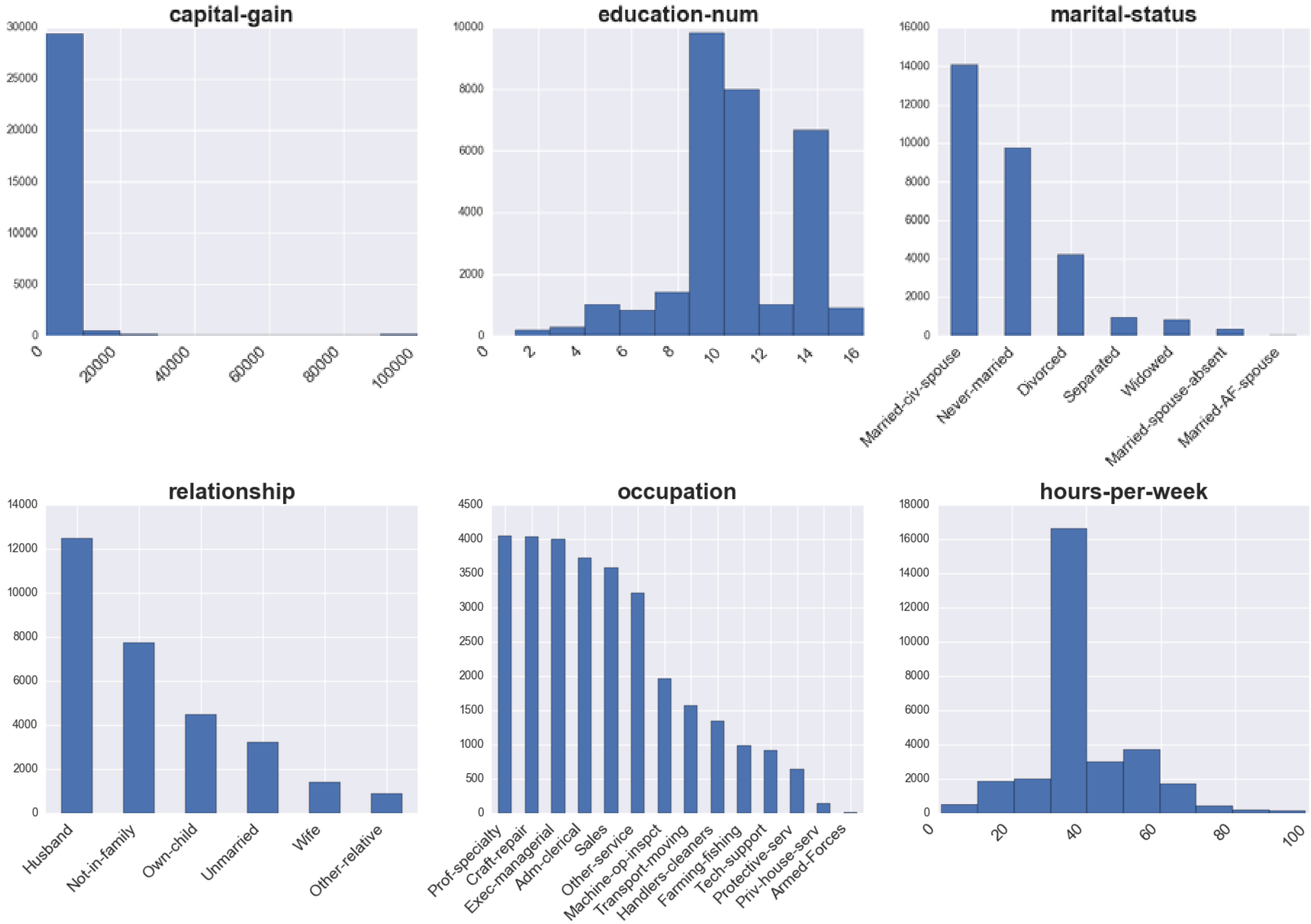
Weight Vectors 2/2

Applying a weight vector to our desired columns wil l change our cost function and thereby produce diff erent anonymization results:

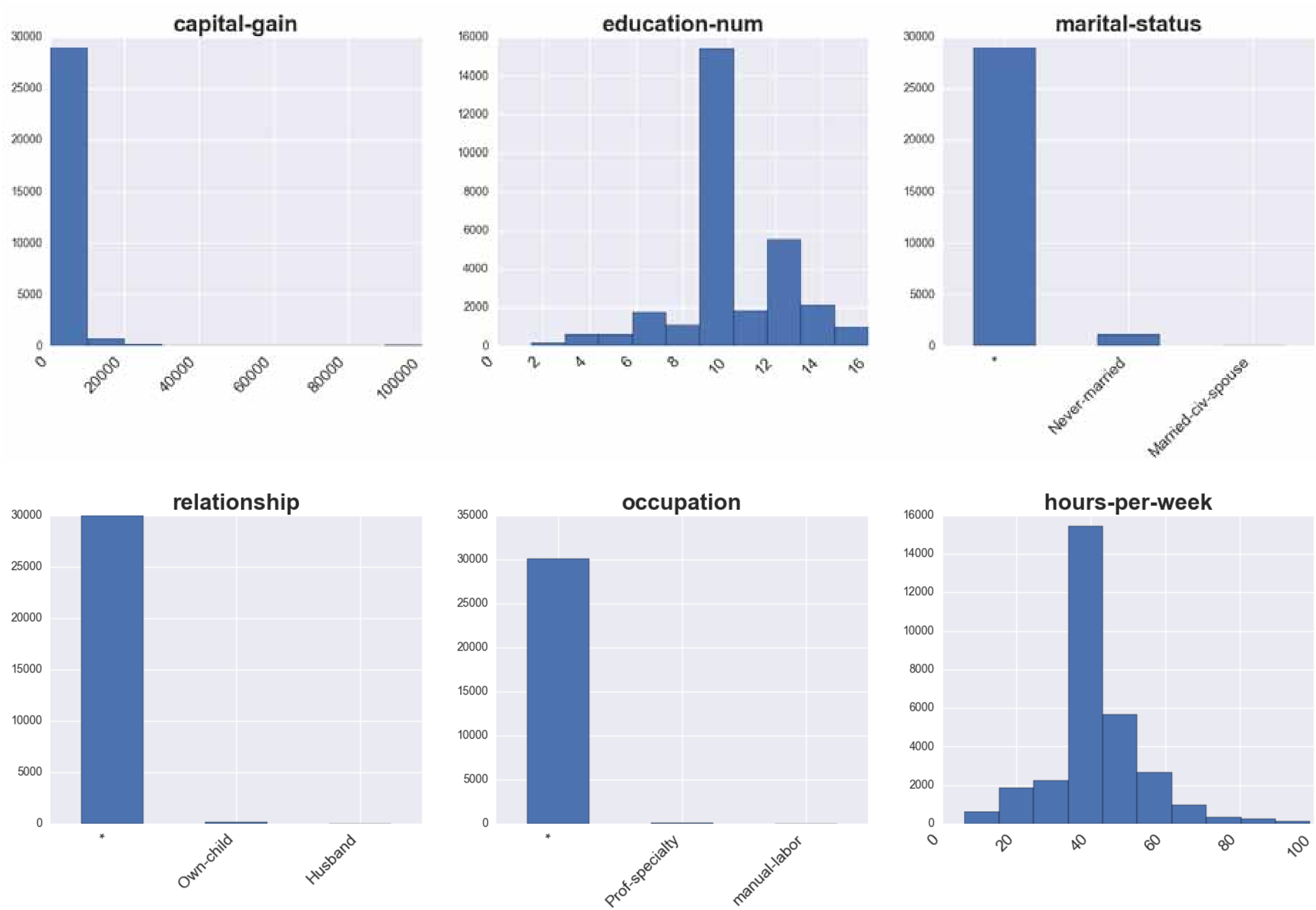
age	workclass	native-country	sex	race	marital-status
0.1667	0.1667	0.1667	0.1667	0.1667	0.1667

age	workclass	native-country	sex	race	marital-status
0.95	0.01	0.01	0.01	0.01	0.01

Experiments – original dataset



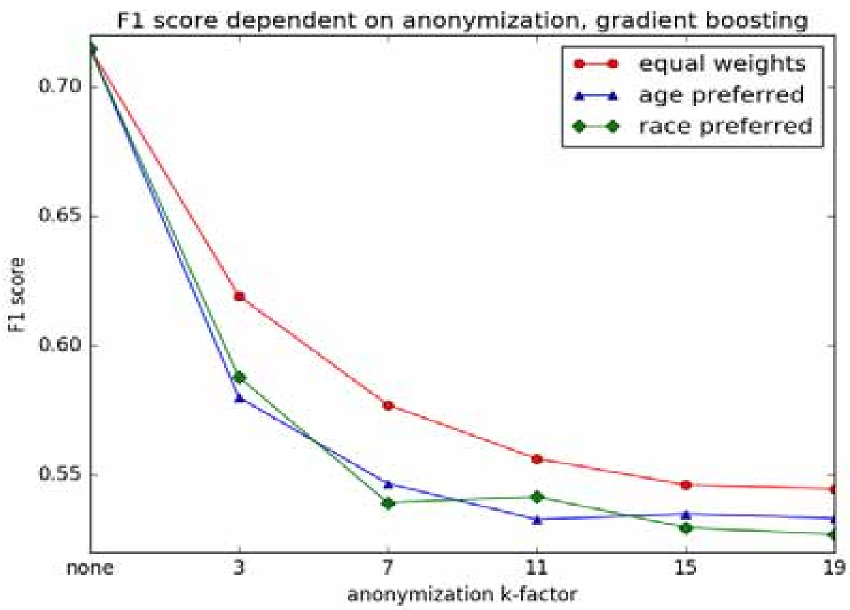
Experiments – example anonymized dataset

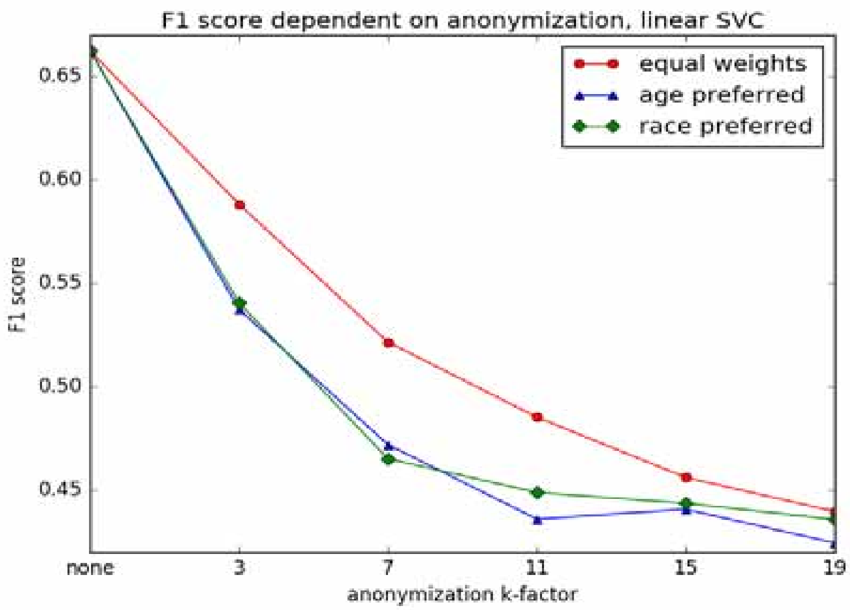


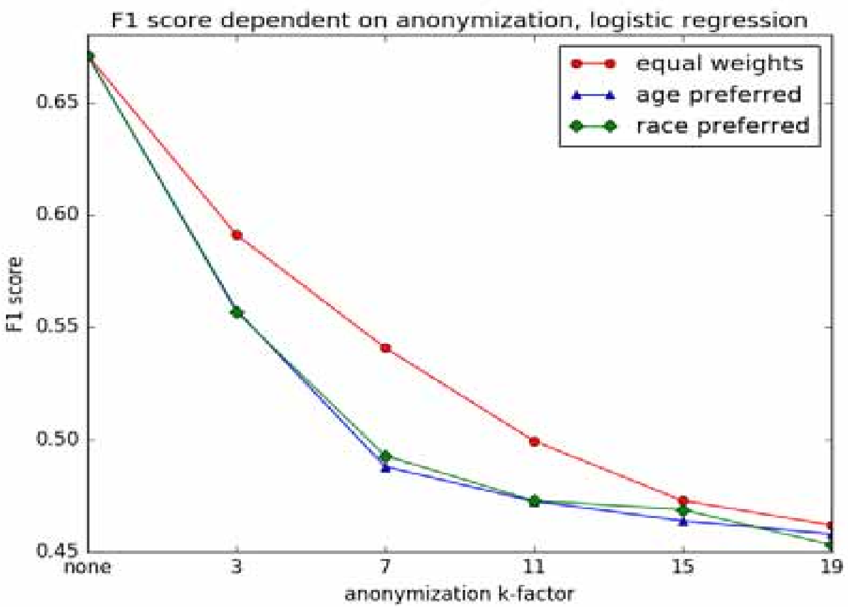
Experiments – prepared datasets

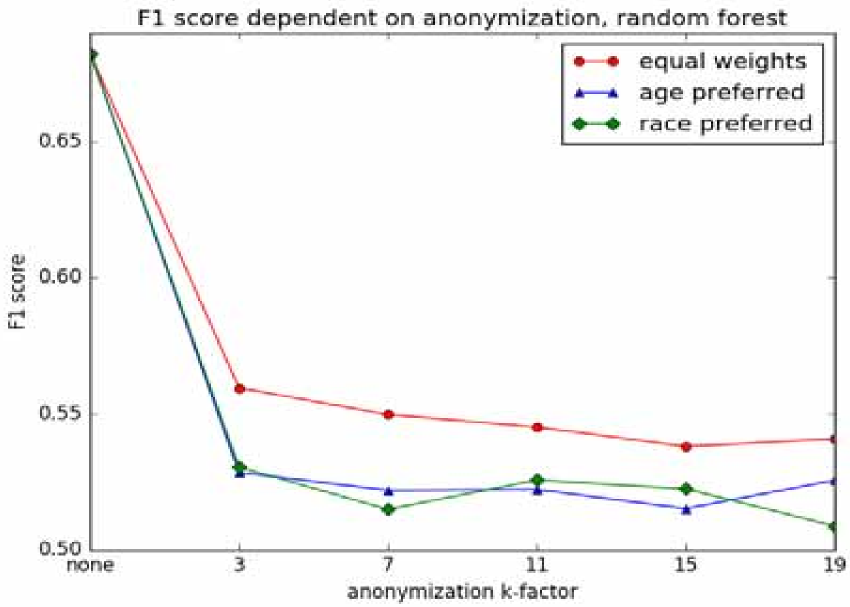
- We used k-factors of:
- 3, 7, 11, 15 and 19
- Each combined with three different weight vectors
    - ➢ Equal weights for all columns
    - ➢ Age preferred (0.88 vs 0.01 rest)
    - ➢ Race preferred (0.88 vs. 0.01 rest)
- Resulting in 15 differently anonymized data sets

Experiments - ML on Anonymization - Results

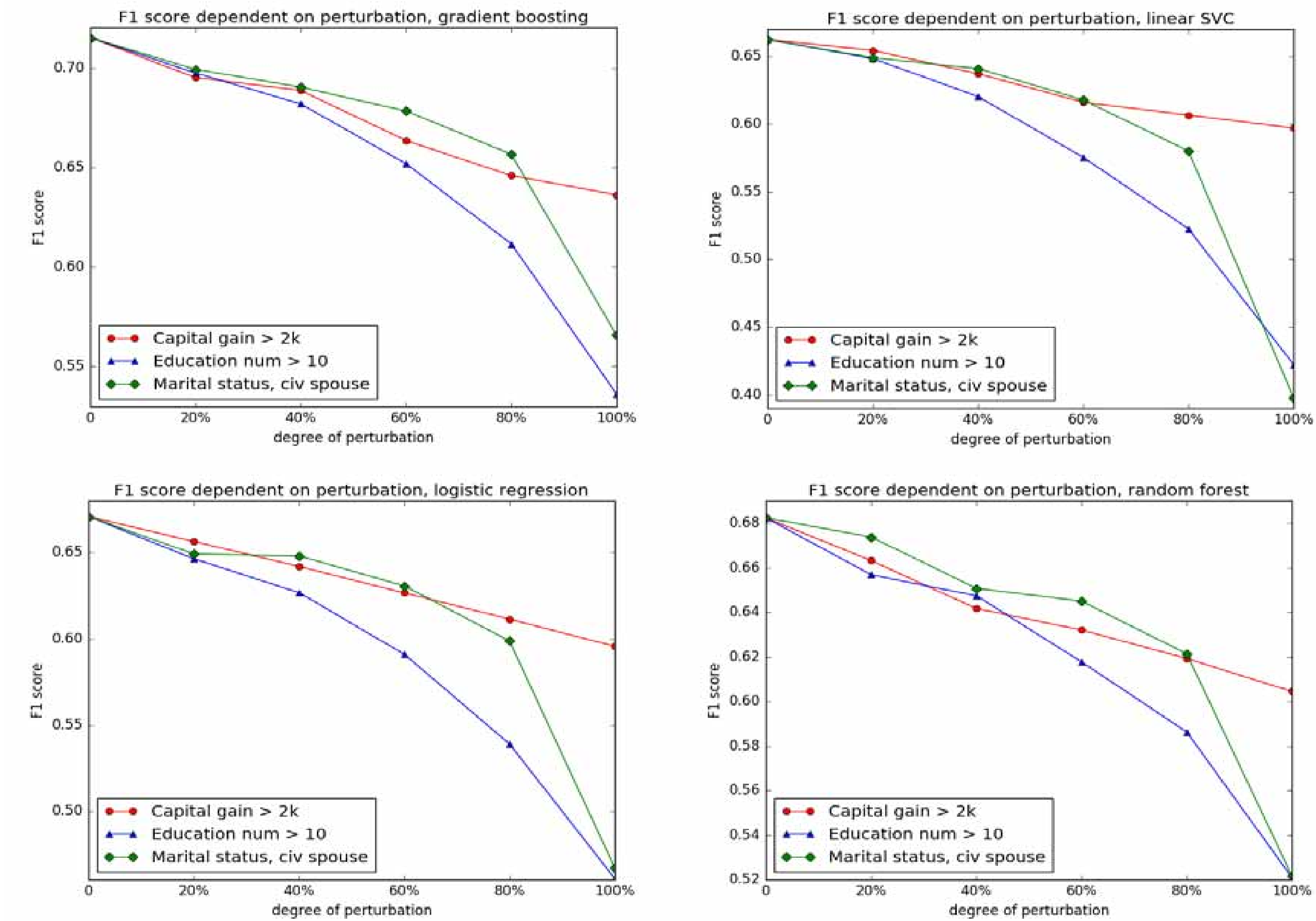








Experiments - ML on Anonymization - Results



Conclusions

1. Succumbing to the “right-to-be-forgotten” still seems better than performing ML on anonymized DBs

2. A whole lot of future research is needed in order to corroborate and expand on those results

   - Extension to other datasets
   - Extension to other ML approaches
     => Prediction, Clustering, Dim. Reduction
   - Other perturbation techniques
   - Graph-based datasets

Other Perturbation techniques (tab)

- Adding noise (only distribution counts)
  - Value perturbation => numerical attributes
    - Idea: alter individual data points, keep distribution
- Microaggregation / Clustering
  - Replace node data by centroid data
  - good for numerical data, but possible also for others given respective rules
  - Ensures k-anonymity only when computed over all attributes at the same time
  - Exact optimal only in P when computed over just 1 attribute (else heuristic)

- Graph data / social network data, in which
  - nodes represent microdata
  - edges represent their structural context
  - graph data are harder to anonymize
    - It's harder to model the background knowledge of an attacker.
    - It is harder to quantify the information loss of modifications.

- Graph perturbation
  - (randomly) adding / deleting nodes / edges
  - very efficient
  - hard to reconstruct - (sub)graph iso-, homomorphism problem

05 Conclusion and Future Outlook

- Privacy, Security, Safety and Data Protection are of enormous **increasing importance** in the future …
- due to the trend to **mobile and cloud** computing
- EHR are the fastest growing application which concern data privacy and **informed patient consent.**
- Personal health data are being stored for the purpose of maintaining a **life-long health record.**
- **Secondary use** of data, providing patient data for research.
- Production of **Open Data** to support international research efforts (e.g. cancer) without boundaries.
- **Data citation** approaches are needed for full transparency and replicability of research …

Thank you!

Questions

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!

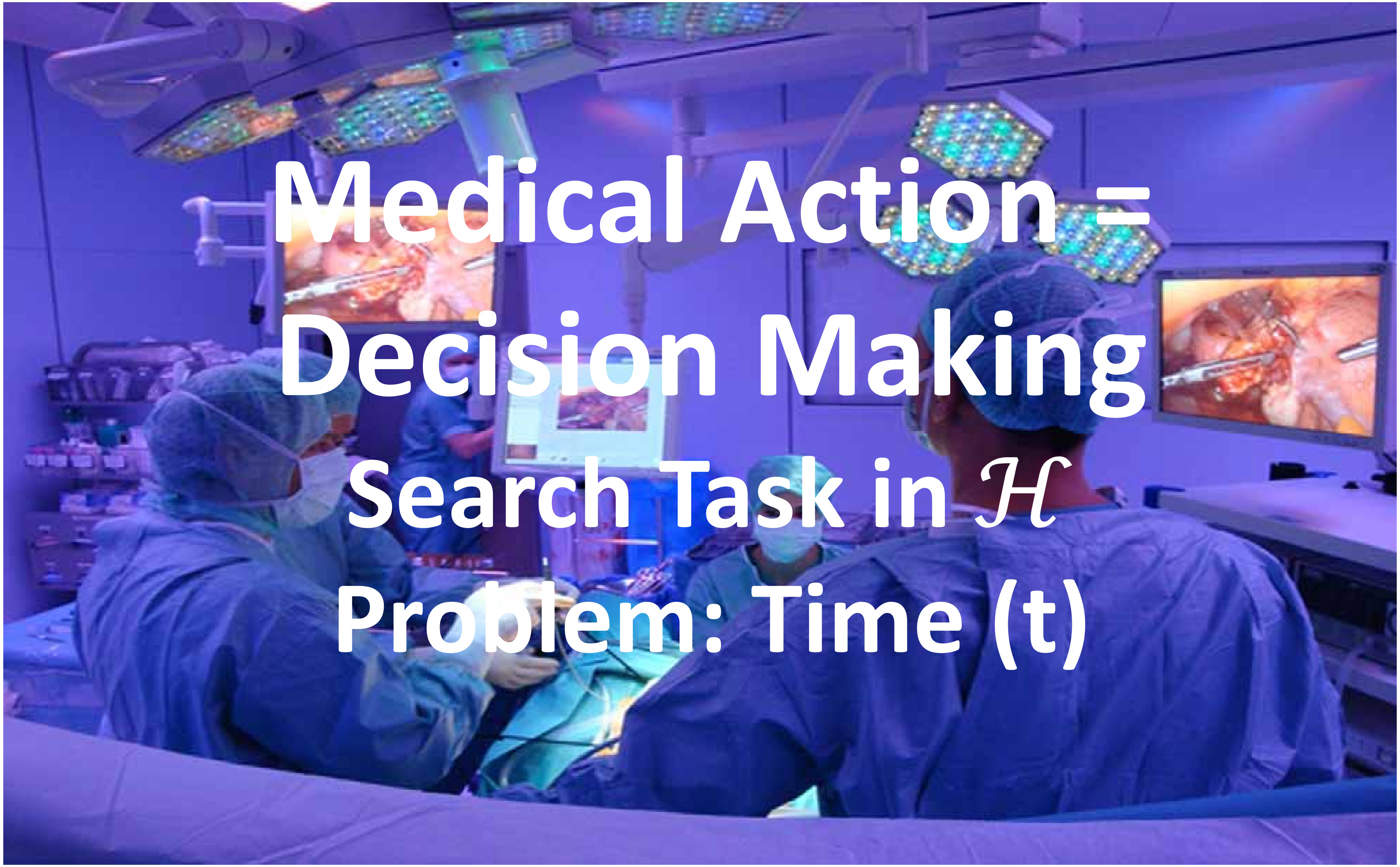
Sample Questions (2)

- 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?
- Ubiqutious 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 healt 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?

Appendix

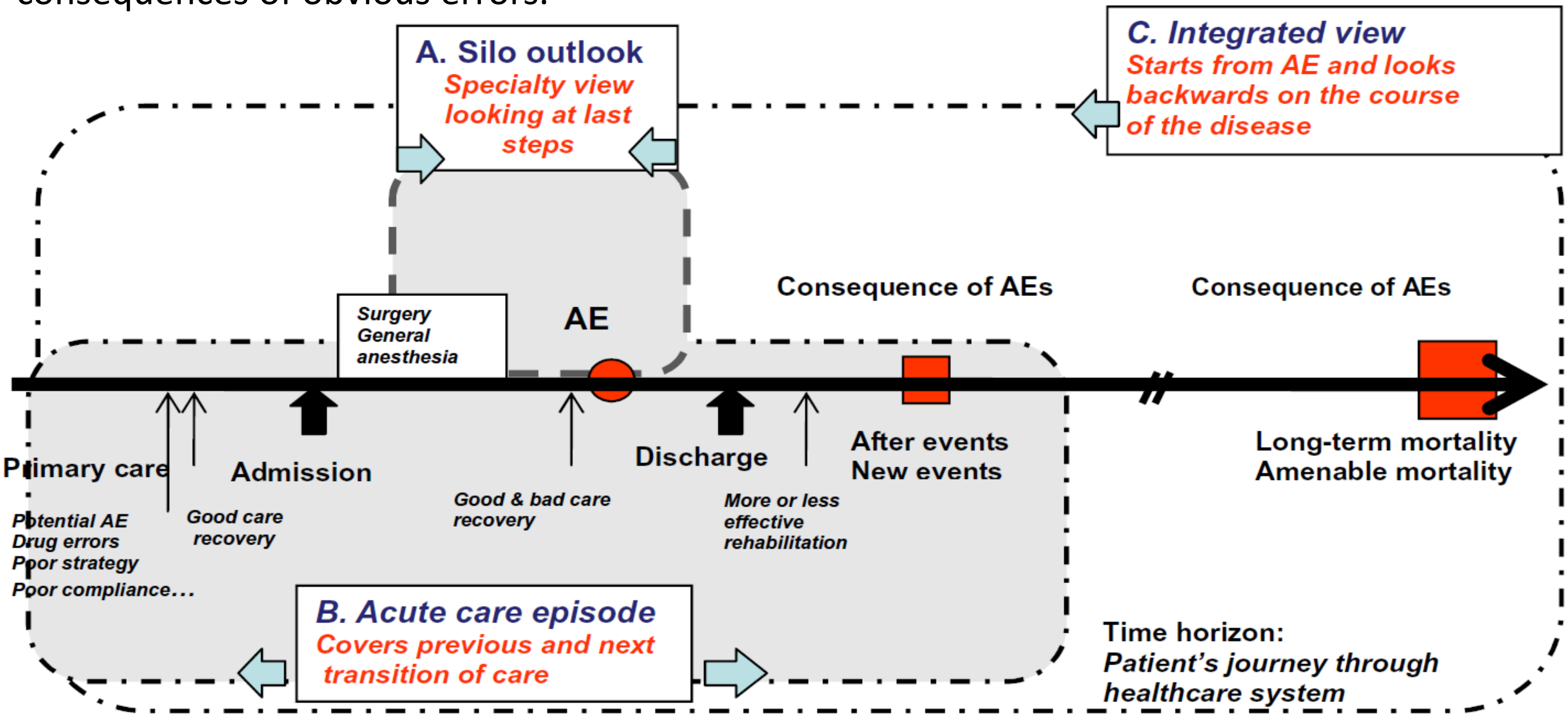

Medical Action =
Decision Making
Search Task in $\mathcal{H}$
Problem: Time (t)

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 (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 (Department of Health: Patient confidentiality and Access to Health Records)
- http://videolectures.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?)

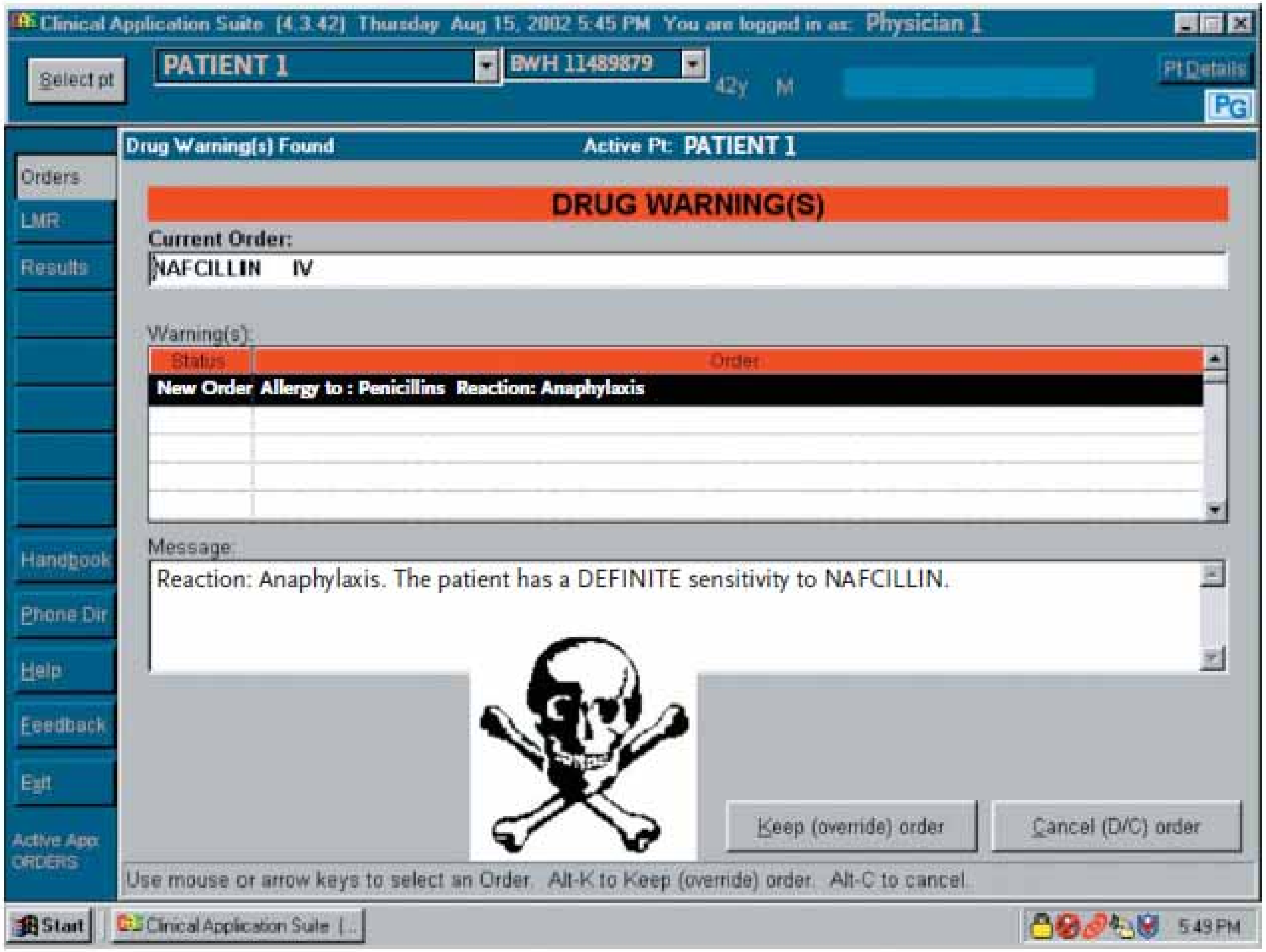
Appendix: Advances in patient safety are hampered by …

… the silo andinsurance-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.



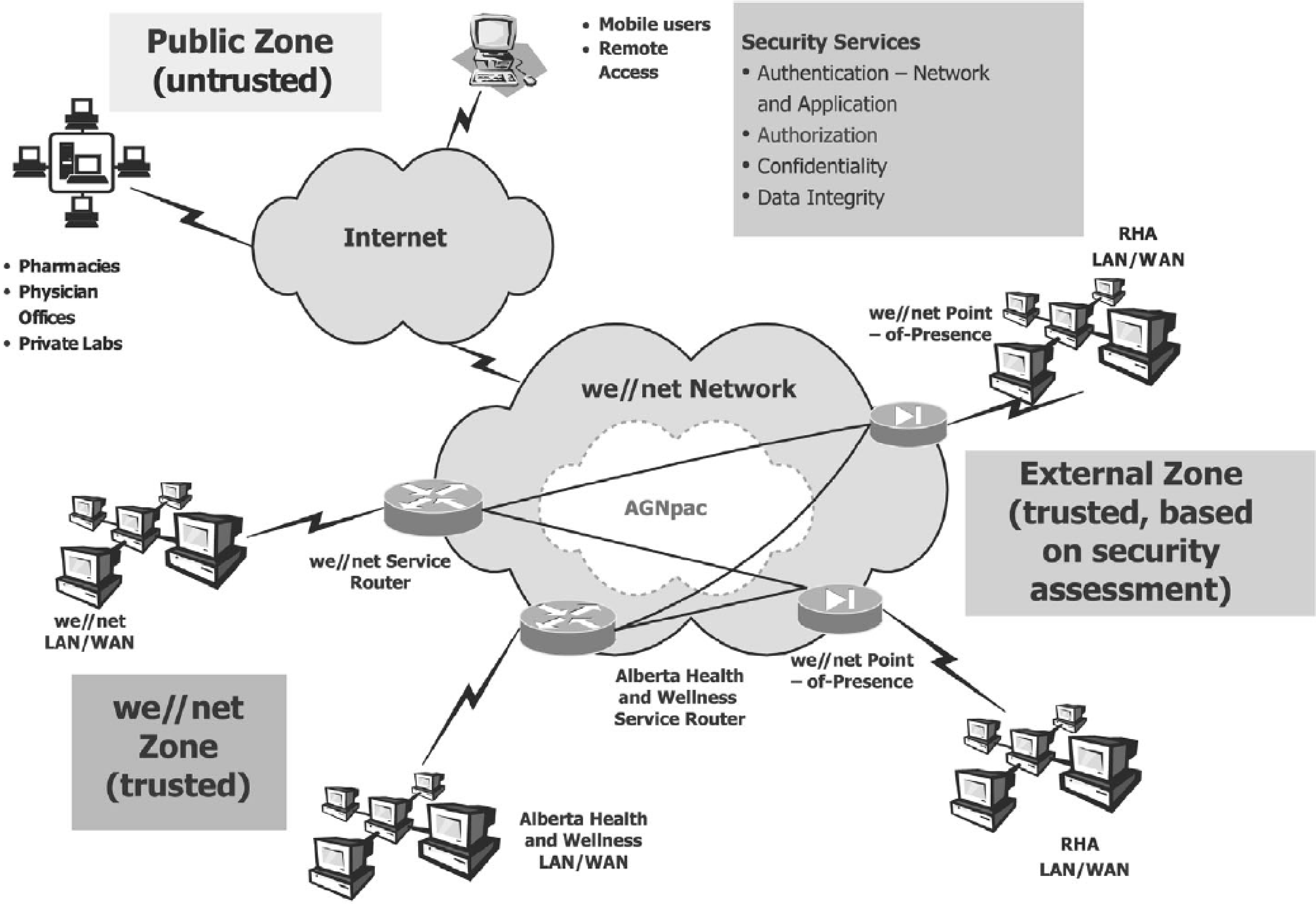
Amalberti, R., Benhamou, D., Auroy, Y. & Degos, L. (2011) Adverse events in medicine: Easy to count, complicated to understand, and complex to prevent. Journal of Biomedical Informatics, 44, 3, 390-394.

Appendix: Example for a simple warning message



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

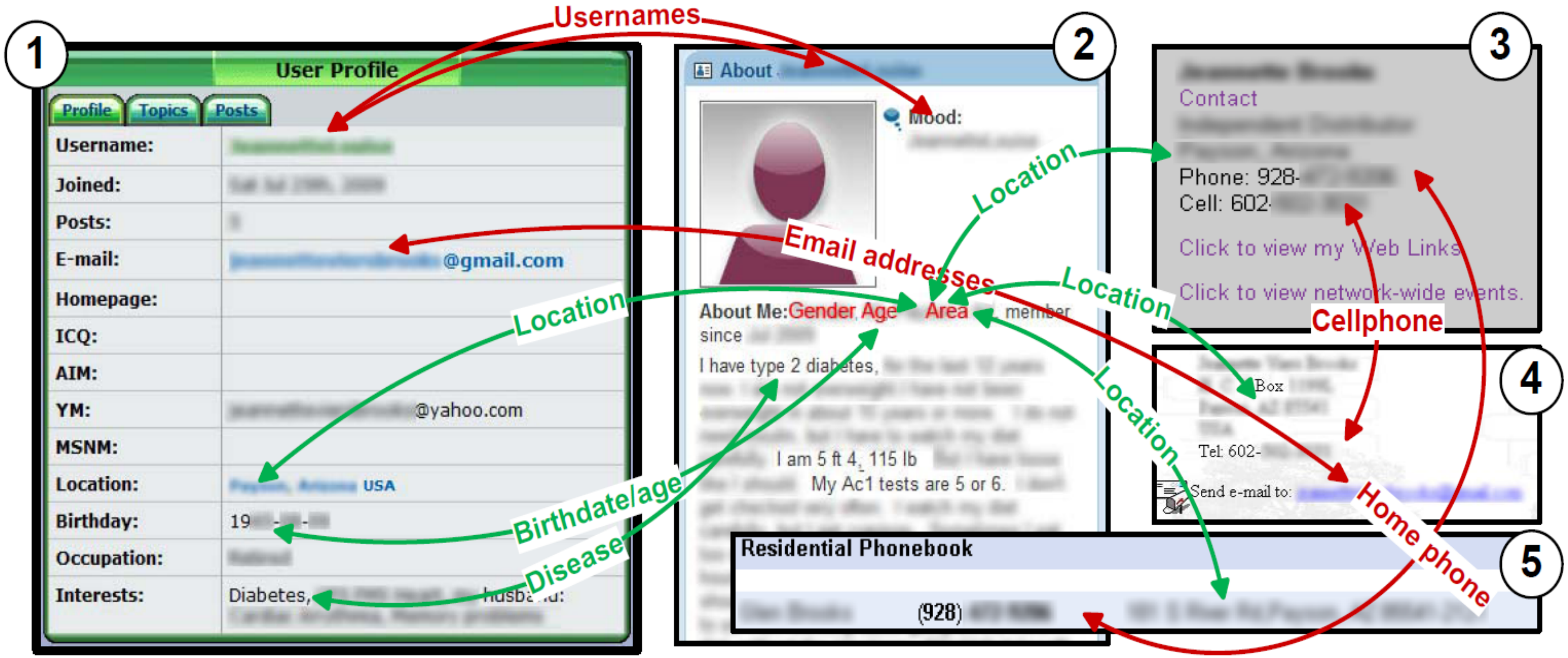
Appendix: Example for trust policies in HIS networks



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.*

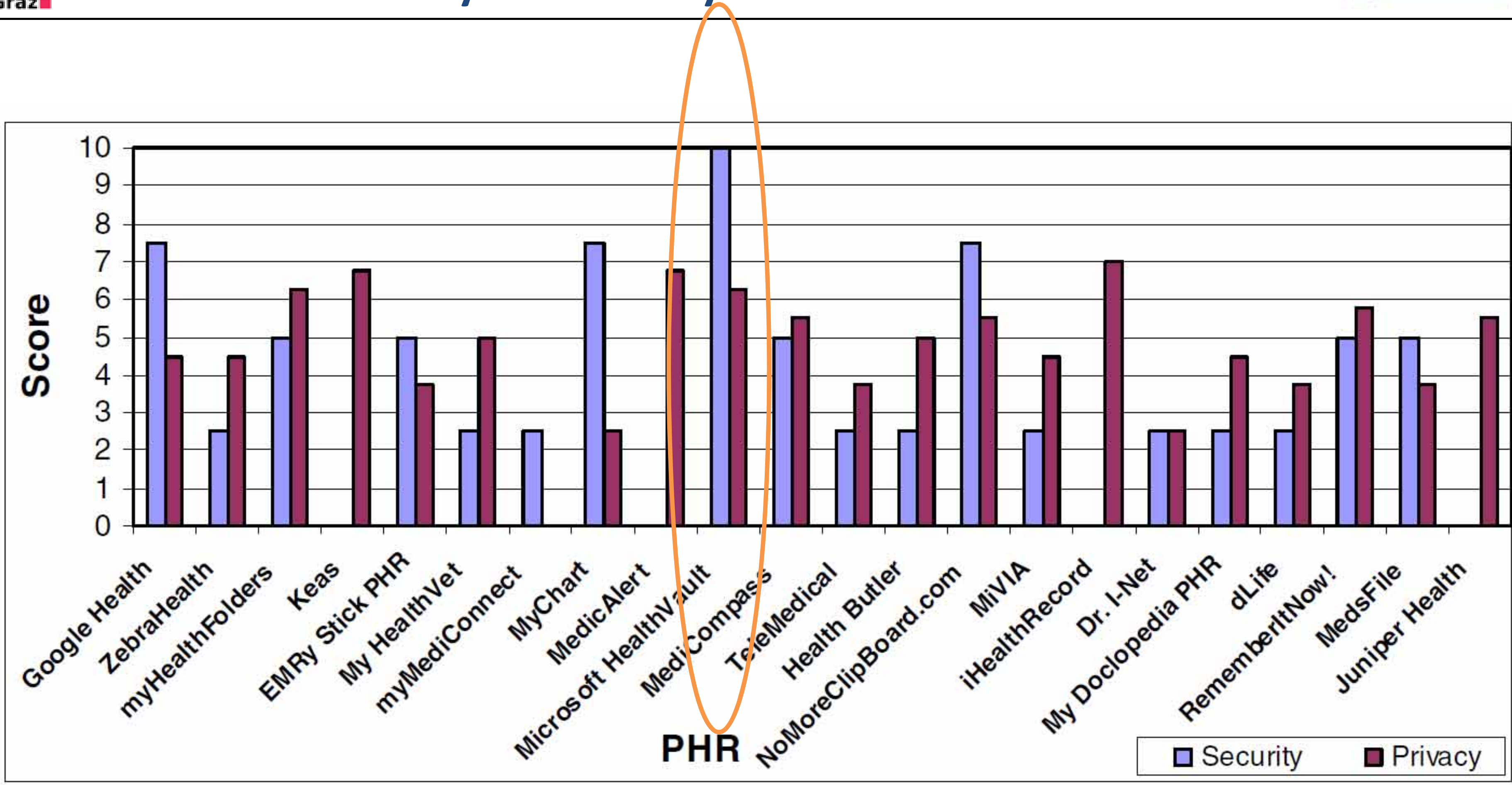
Appendix: Example of new threats to health data privacy

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



Carrión, I., Fernández-Alemán, J. & Toval, A. (2011) Usable Privacy and Security in Personal Health Records. In: *INTERACT 2011, Lecture Notes in Computer Science LNCS 6949. Berlin, Heidelberg, Springer, 36-43.*

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

- **1) Privacy Policy**
  - 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.
- **2) Data Source**
  - 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.
- **3) Data Management**
  - 0. Not indicated.
  - 1. Data user.
  - 2. Data user and his/her family data.
- **4) Access management**
  - 0. Not indicated.
  - 1. Other users and services/programs.
  - 2. Healthcare professionals.
  - 3. Other users.
  - 4. Other users, healthcare professionals and services/programs.

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

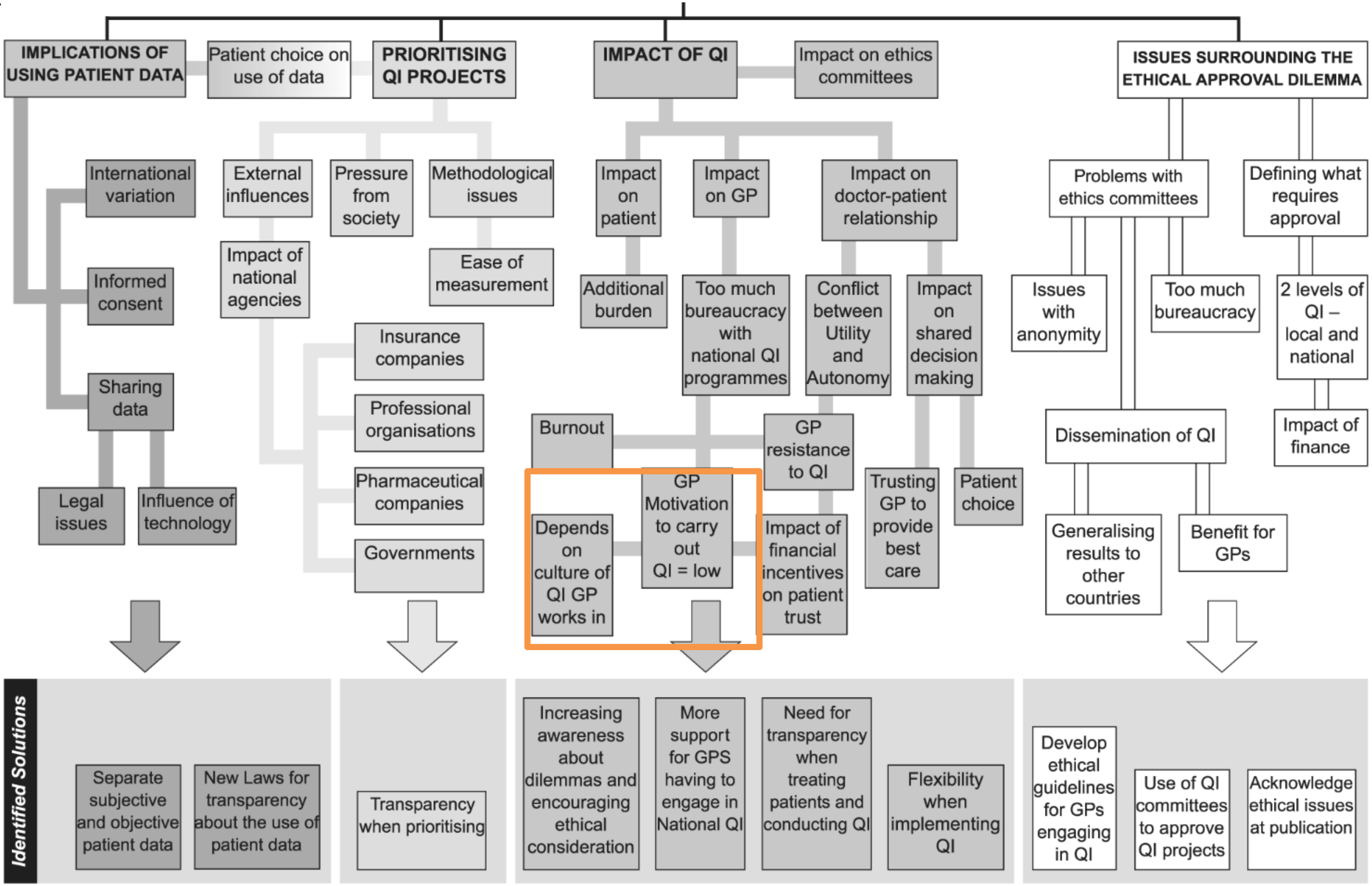
- **5) Access audit**
  - 0. No.
  - 1. Yes.
- **6) Data access without the end user's permission**
  - 0. Not indicated.
  - 1. Information related to the accesses.
  - 2. De-identified user information.
  - 3. Information related to the accesses and de-identified user information.
  - 4. Information related to the accesses and identified user information.
- **7) Security measures**
  - 0. Not indicated.
  - 1. Physical security measures.
  - 2. Electronic security measures.
  - 3. Physical security measures and electronic security measures.
- **8) Changes in Privacy Policy**
  - 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.
- **9) Standards**
  - 0. Not indicated.
  - 1. HIPAA is mentioned.
  - 2. System is covered by HONcode (HON = Health on the Net).
  - 3. HIPAA is mentioned and system is covered by HONcode.

Slide 11-43 Overview Personal Health Records (PHR)

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

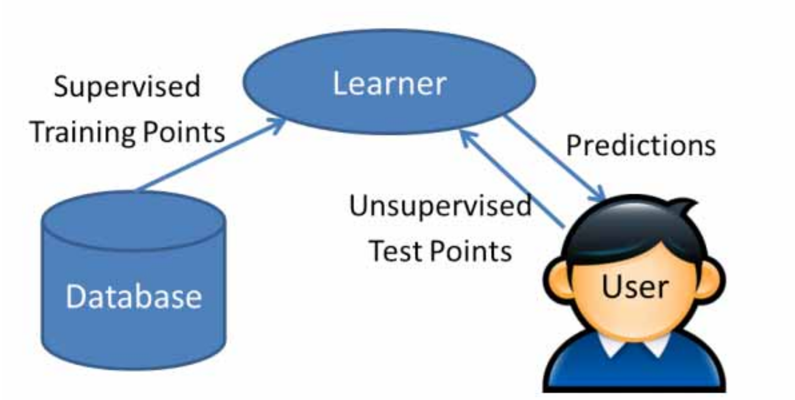
Legend: PL = Privacy policy location; DS = Data source; DM = Data managed; AM = Access management; AA = Access audit; DA = Data accessed without the user's permission; SM = Security measures; CP = Changes in privacy policy; S = Standards

Carrión et al. (2011)

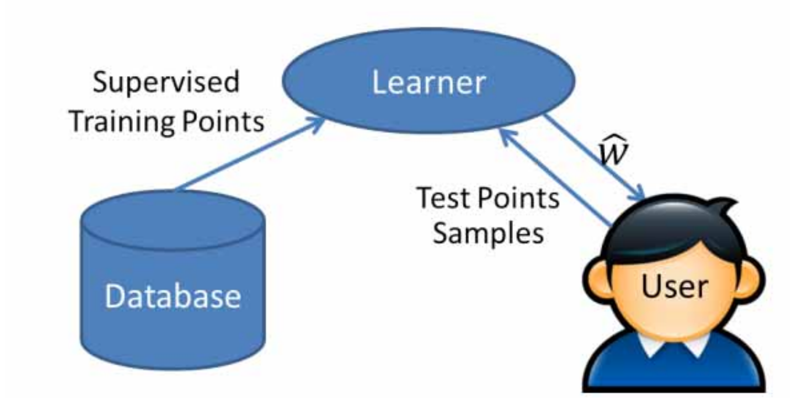


Tapp et al. (2009) Quality improvement in primary care: ethical issues explored. *International Journal of Health Care Quality Assurance, 22, 1, 8-29.*

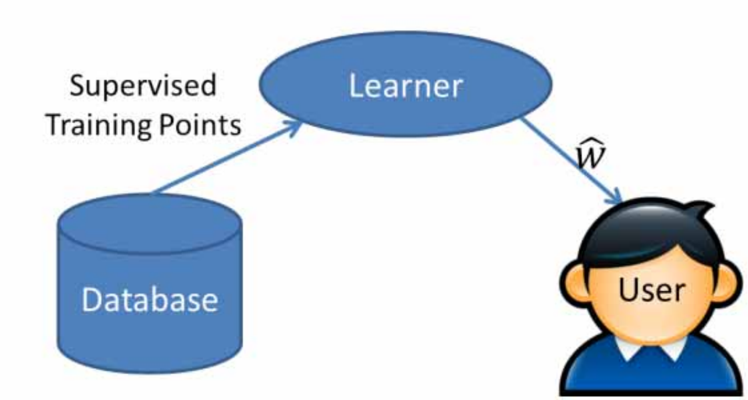
Example: Differentially Private Kernel Learning



(a) Interactive Model



(b) Semi-interactive model

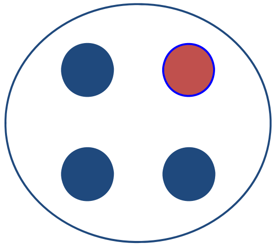


(c) Non-interactive Model

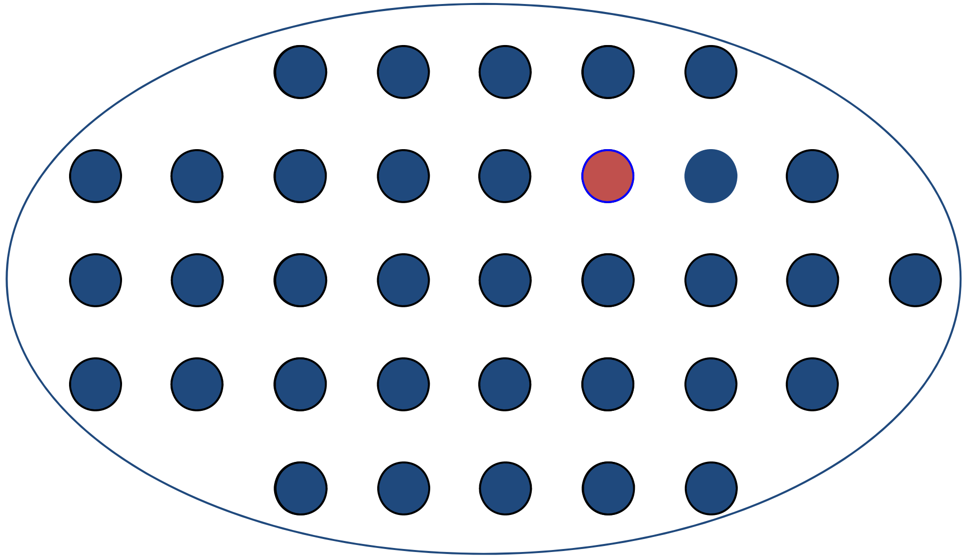
Simplest Privacy Metric

- 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

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

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

- 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

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

- Remember: Entropy measures the randomness (uncertainty) – here private data
- The attacker 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:

$$D(A,t) = H^*(A) - H(A,t)$$

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

$H^*(A)$ – the maximum entropy

Computed when probability distribution of p_i's is uniform

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

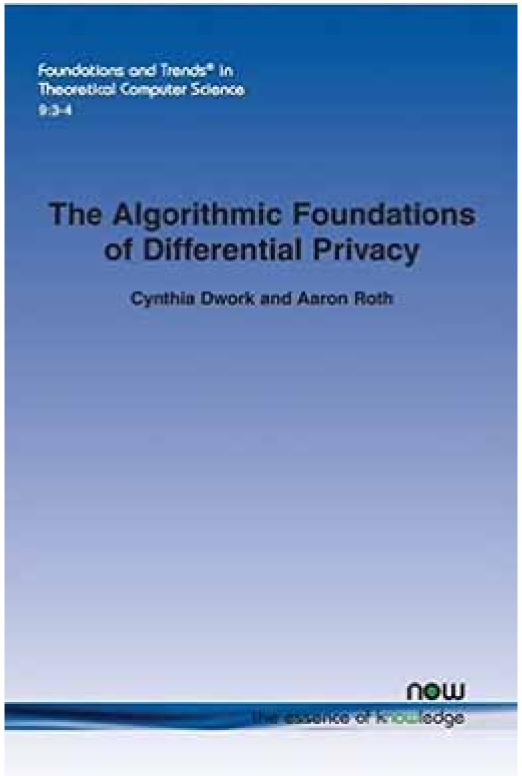
w_j – weights capturing relative privacy "value" of attributes

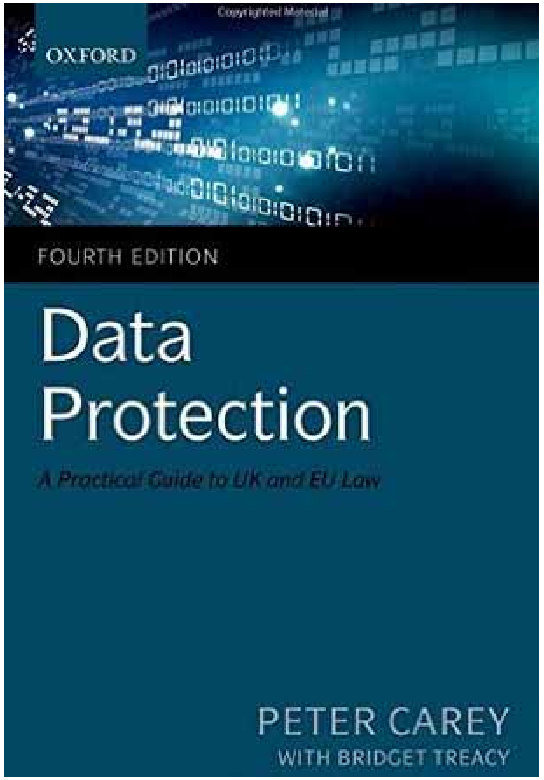
Privacy Aware Machine Learning for Health Data Science

- – 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

Additional Reading

Additional Reading





Dwork, C. & Roth, A. 2014. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9, (3–4), 211-407, doi:http://dx.doi.org/10.1561/0400000042.

Blackmer, W. 2016. GDPR: Getting Ready for the New EU General Data Protection Regulation. Information Law Group, InfoLawGroup LLP

Carey, P. 2009. Data protection: a practical guide to UK and EU law, Oxford University Press