Patient Records:
Challenges for and Approaches to Safety and Security

Klaus Pommerening

IMBEI, Universitätsmedizin Mainz

eHealth Workshop, London, 16 June 2011

5 Challenges of eHealth for the Next Years

1. Electronic Patient Records and Health Telematics
2. Personalised Medicine, genetic data, and Biobanking
3. Assistive Technology (Ambient Assisted Living, AAL)
4. Using data for medical research
5. Dependable IT systems

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Electronic Patient Records

The patient record of today (or the near future) is an EPR

- Shared between health care institutions, online
- Transparent and accessible for the patient
- Lifelong for the patient

Expectations:

- Better documentation, better quality control, more safety
- Availability of information
- Enhancement of healthcare processes
- Better communication
- Support of eHealth and telemedicine
- Cost reduction in health care

JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Challenges for Safety and Security of EPR

- The EPR is sensitive and will become even more sensitive
  - by inclusion of genetic, AAL, and research data (see below)
  - by new use cases
- Strong requirements for safety and security:
  - Availability, integrity, confidentiality
- Safety (EPR as source of trouble): Can the EPR harm the patient? → Availability, system stability, reliability, integrity, correctness
  - What about a misdiagnosis in the EPR?
  - May a physician rely on an EPR when the patient has the right to delete or hide Items?
- Security (EPR as target): Can someone misuse the EPR?
  - Security of EPR at service provider, in the network, in the Health Cloud?
  - Data once leaked out will remain public forever.

JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Technical Approaches to Safety and Security

- Network component architecture with trusted service providers, independent TTPs*
- Implementation and enforcement of policies and access rights and access restrictions
- Consideration of standards and certification offerings
- Use of cryptography (encryption, digital signature, strong authentication), encrypted communication, PKI**
- Encrypted or pseudonymised storage
- Hardware and network security
- Advantage of EPR over paper record:
  - Non-repudiation and integrity by digital signature
  - Better access control
  - Logging of accesses

[* Trusted Third Parties
** Public Key Infrastructure]

JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Example: Health Telematics in Germany

- Encrypted storage of EPR (central or distributed)
- Access implies decryption
  - Needs health professional's and patient's keys (from smartcards)
  - Access control enforced by cryptographic means (access password = cryptographic key)
- However: Access by a priori unknown health professionals only possible, when there is a master key (hybrid encryption)
  - Who knows the master key?
  - Emergency access by physician's key alone (with extended logging)
- Distributed architecture with many trusted third parties and trusted services
  - Is there a weak link in the chain?
- Elegant and convincing in White Papers, stumbling in pilot projects, not yet rolled out ☹

JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Problems with the Technical Approach to IT Security

- Technical approach alone is insufficient
  - Stable framework of mandatory legal and organisational regulations required
  - Technical and organisational measures should derive from comprehensive policy.
- Existing security technology adequate for Health Telematics, but security is fragile and requires extreme care.
  - Sometimes failures are irreparable (patient dies, information leaks out), current IT doesn't adapt well to such an environment.
- Security measures tend to be complex.
  - How complex should eHealth infrastructure be?
  - Complexity is the main enemy of security.
  - KISS = Keep it Small and Simple.

JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Example: Smartcards – the Key to Security?

- Smartcards for patient and health professionals as secure devices for access control
- Access to EPR needs both of them (except in emergency situations).
- Use of smartcard OK for patient (except when card missing)
- Cumbersome for doctors in hospitals
- Vision: “RFID* bracelets” and “Login/ logout on the fly”
- *Complexity for users reduced (hidden from users by system)*

[* Radio Frequency IDentification]

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Pharmacogenomics and Pharmacogenetics

- Enzymes may influence the effect of drugs.
  - = proteins produced by genetic activity
- Personalised medicine tries to adapt diagnosis and therapy to the individual genetic constellation of the patient.
  - Identify “responders”, avoid ineffective therapies
  - Adjust doses
  - Reduce unwanted secondary effects
- For the moment mostly in a research context
- Growing relevance for routine care

$\Rightarrow$ The EPR will contain genetic data (maybe the complete genome?).

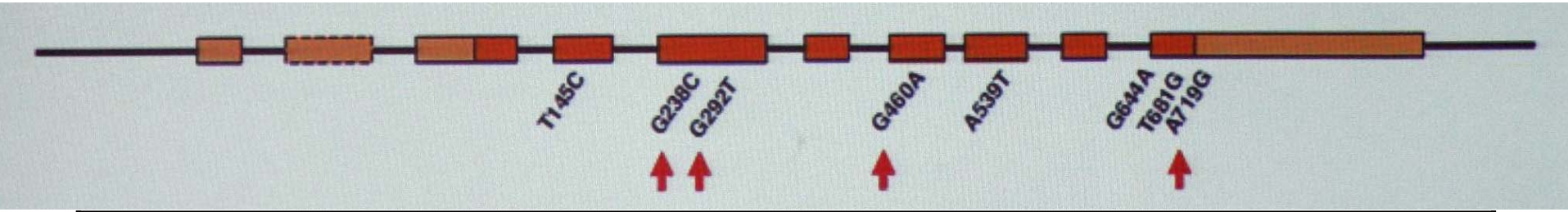
UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Example of Therapeutic Success

Enzyme activity of TPMT* affects toxicity of drug AZA**.
Dose recommendations established.

[* Thiopurine methyltransferase]
[** Azathioprine (immunosuppr.)]

Polymorphisms in TPMT

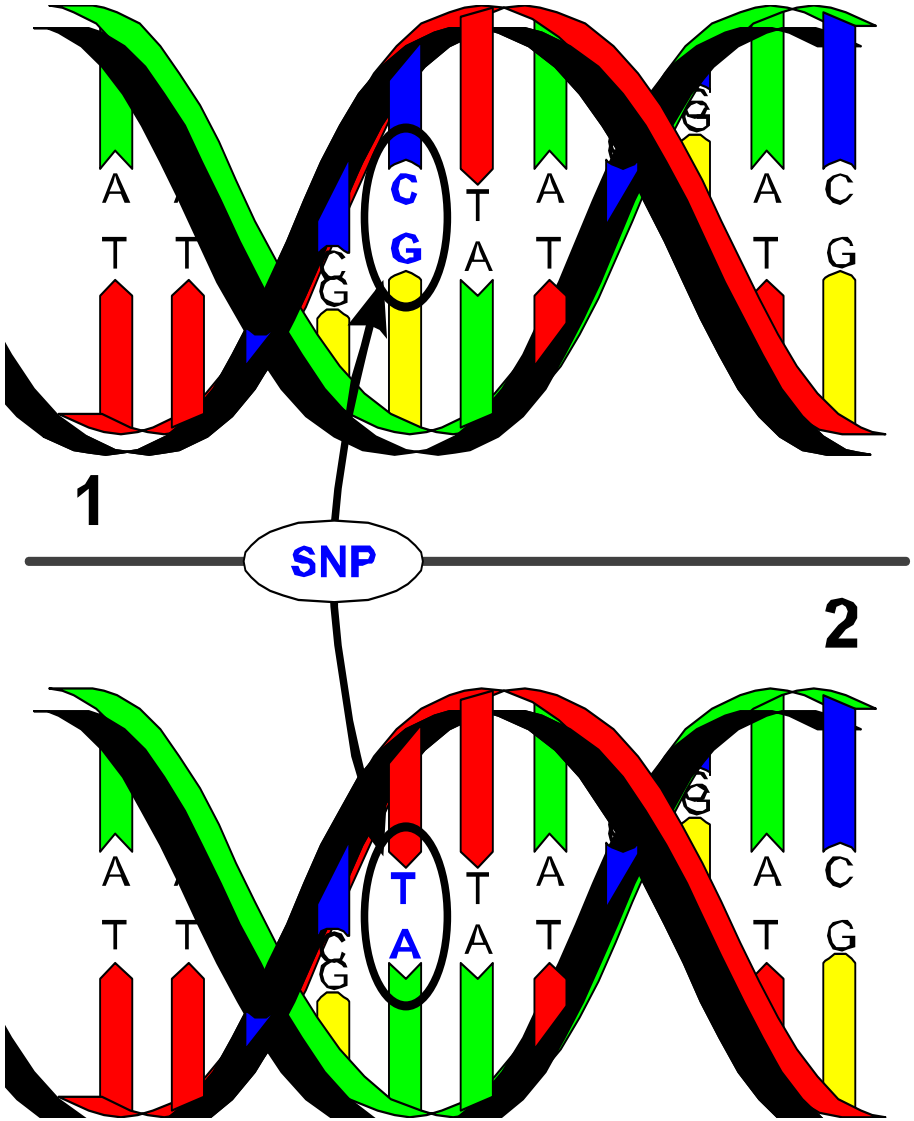


TPMT*1		Normal enzyme activity
TPMT*2	G238C	Reduced enzyme activity
TPMT*3A	G460A, A719G	Reduced enzyme activity
TPMT*3B	G460A	Reduced enzyme activity
TPMT*3C	A719G	Reduced enzyme activity
TPMT*3D	G292T	No enzyme activity

[Source: W. Siffert]

2. Personalised Medicine, genetic data, Biobanking

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

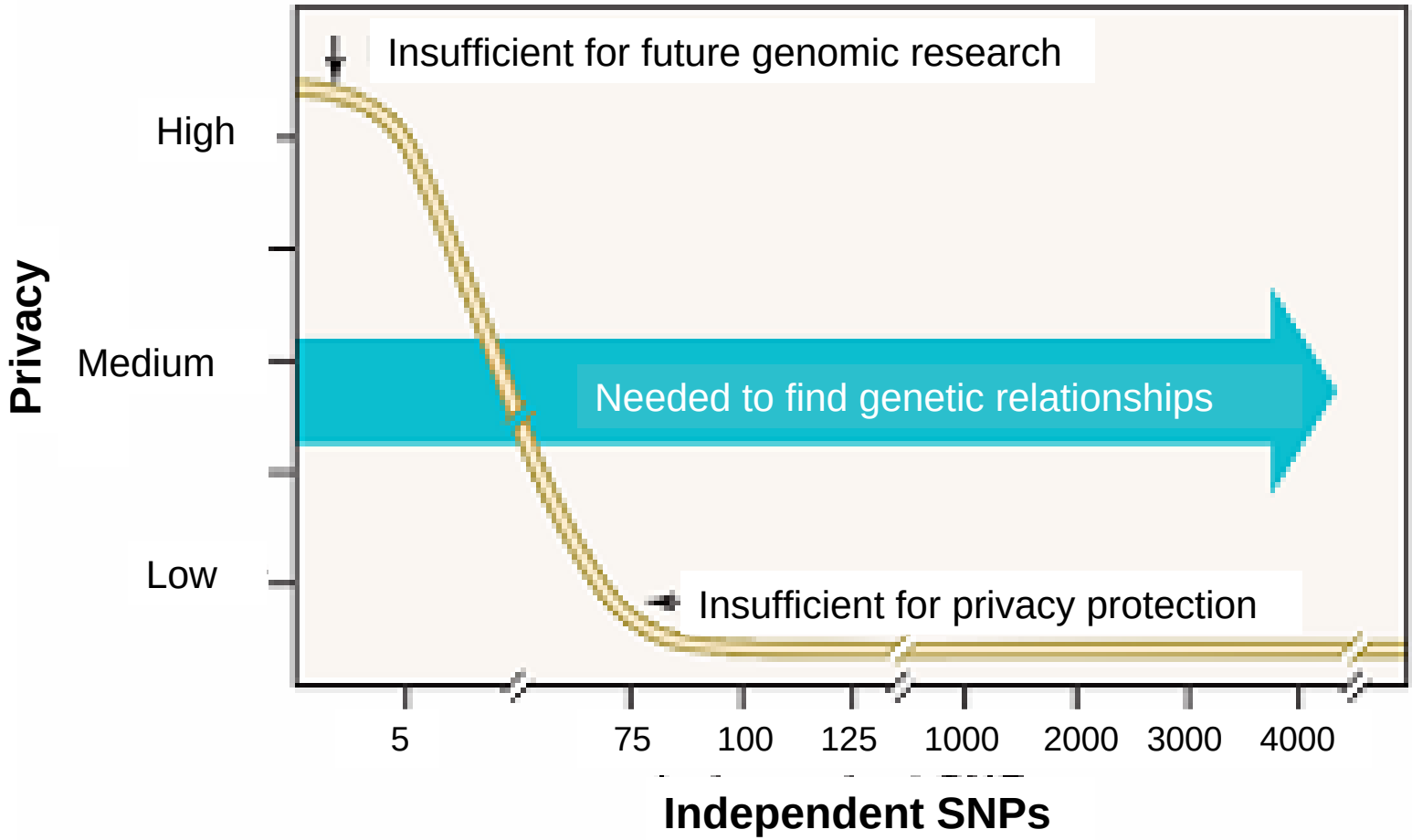


Most variants in a gene consist of only 1 SNP*, a different base pair somewhere in the double helix.

[* Single Nucleotid Polymorphism]
[Source: Wikipedia]

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

70 SNPs suffice for identification.



[Source: Lin/Owen/Altman Science 305 (2004)]

JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Challenges for Privacy by Genetic Information

- Special features of genetic data: availability, indivisibility (in samples), identifiability
- *Genetic data are no secrets*: Easy to get reference samples.
- *Genetic data are identifiers*: 70 SNPs suffice.
  - A single prognostic or therapeutic application typically involves 5 – 20 SNPs.
- Perspective: “The Race for the 1000 $ Genome”:
  - ➢ complete sequencing of the individual genome

- However: Genetic data alone are not as informative as first believed.
  - Predispositions, not evolution of individual, not actual diagnoses

JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Biobank

- Collection of samples and derived material (DNA, RNA, …)
  - Useful only with clinical annotation.
- Valuable basis for genetic, translational, clinical, and epidemiological research.
- Long term storage intended for future research.
- *Biomaterial (samples, extracts) contains comprehensive information and may serve as identifier*.
- The inherent identification risk of genetic data may expose the corresponding clinical data.
- … and also associated sociodemographic or lifestyle data
  - in projects of genetic epidemiology.

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Approaches to Safety and Security

- Genetic data as part of EPR OK as long as used in a treatment context only
  - and subject to the strong access restrictions of the EPR
- Unsuitable for data export or “anonymous” access
  - Data warehouses, biobanks, economic evaluations, …
- Scientific Use of EPR containing genetic data only in restricted setting
  - “Approved projects”, see below
- Recommendations for data warehouses and biobanks:
  - Store genetic data separately from clinical data, combine them only as necessary.
  - Restrict public use
  - and check query results for re-identification potential.

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

AAL Data in the EPR

- With emerging assistive technologies the EPR will contain
  - large collections of body and environmental parameters from sensors,
  - socioeconomic data,
  - lifestyle and behavioural data.
- This makes the EPR a high-dimensional individual data record with high re-identification risk
  - Significant overlap with “external knowledge” from social networks and other internet activities
    (movement profiles, daily activities, ordering of drugs, search queries, …).
  - Date and time of a single consultation may suffice for identification.
- AAL settings comprise a mixture of medical care and social services.
  - Delineation of medical treatment context legally relevant but difficult.
  - Requires sophisticated access rules.

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Further Challenges for AAL data

- How to ensure rights of individuals?
  - Informational self-determination for data collection difficult
  - Voluntariness and consequences of consent questionable
  - Automated decisions dangerous (e.g. adjust drug dose?)
- IT security for mobile IT,
  - Vulnerable technology: sensor networks, mobile devices.
  - Manipulation may endanger lives (“Pacemaker online”).
  - Embedded chips with low performance make cryptographic algorithms inefficient.
  - How to handle software updates for medical devices? (that run versions of standard operating systems)

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

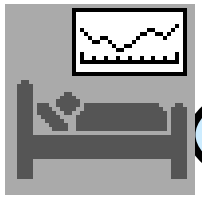
Approaches to Safety and Security of AAL data

- PKI for sensor networks
  - needs special efficient algorithms
  - *There is no communication security without a working PKI*.
  - PKI provides strong mutual authentication, encrypted communication, protection against manipulations.
- Approach for respecting patients' rights: the gateway
  - Patient may configure, even switch off, data transfer.
  - Patient can see what data leave his home.
- Strong detailed access restrictions to AAL data in EPR
  - many different user roles involved
- No intransparent enforced automatisms (decisions, data transfers)

JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Using data for medical research

- "Research": Each kind of (secondary) use of EPR data outside the treatment context: evaluations, statistics, benchmarks, …
- Large long term data pools and biobanks crucial for medical progress
  - Example: rare diseases, sole chance for finding new diagnostic and therapeutic approaches
  - Research requires that EPR data should be kept, not deleted.
- Healthcare and research are tightly connected.
  - Same data needed in both domains.
  - Main investigators in clinical trials and experts participate in treatment.
- Data from clinical trials in the EPR → even more dimensions
- Interregional or international cooperation necessary, in particular for rare diseases



Patient-Physician Relationship

[Primary use/ treatment context]

Barrier: Professional Discretion

[Secondary use/ research context]

Clinical research
health care research

direct
data capture

Export allowed, if
- anonymous data,
- informed consent,
- law

Registries/ Biobanks,
epidemiological research

JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Ethical Aspects of Secondary Use

- Privacy of patient-physician relationship essential for success of treatment
- Use of EPR data for research ethically OK as long as useful for the patient and restricted to the medical domain
- Patient profiles by insurance companies or employers not OK, because against the interests of the patients.
- Deletion vs permanency of EPR data for future research?
- Patients' rights: Self-determination, transparency, revocation
- Informed consent and its limitations
- Who has the benefit from research?
  - Research may be useful for the actual patients themselves, but maybe only for future patients.
  - Patients are highly motivated for participation in research projects.

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Challenges for medical research

- Transferring data from health care into a research context
  - (in most cases) allowed only with informed consent
  - In Germany high legal obstacles
- No efficient anonymisation of EPR data possible:
  - High dimensional data records
  - Re-identification risk (genetic data, social and behavioural data, medical images, unique combinations of innocuous data)
  - External (in particular future) knowledge unknown, e.g. data from social networks
- Protecting data over long time periods
- Increasing trend to cooperation and networking

  also internationally (data collection and evaluation, genetic analyses)
- Balance between public transparency of research and privacy of medical data?

JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

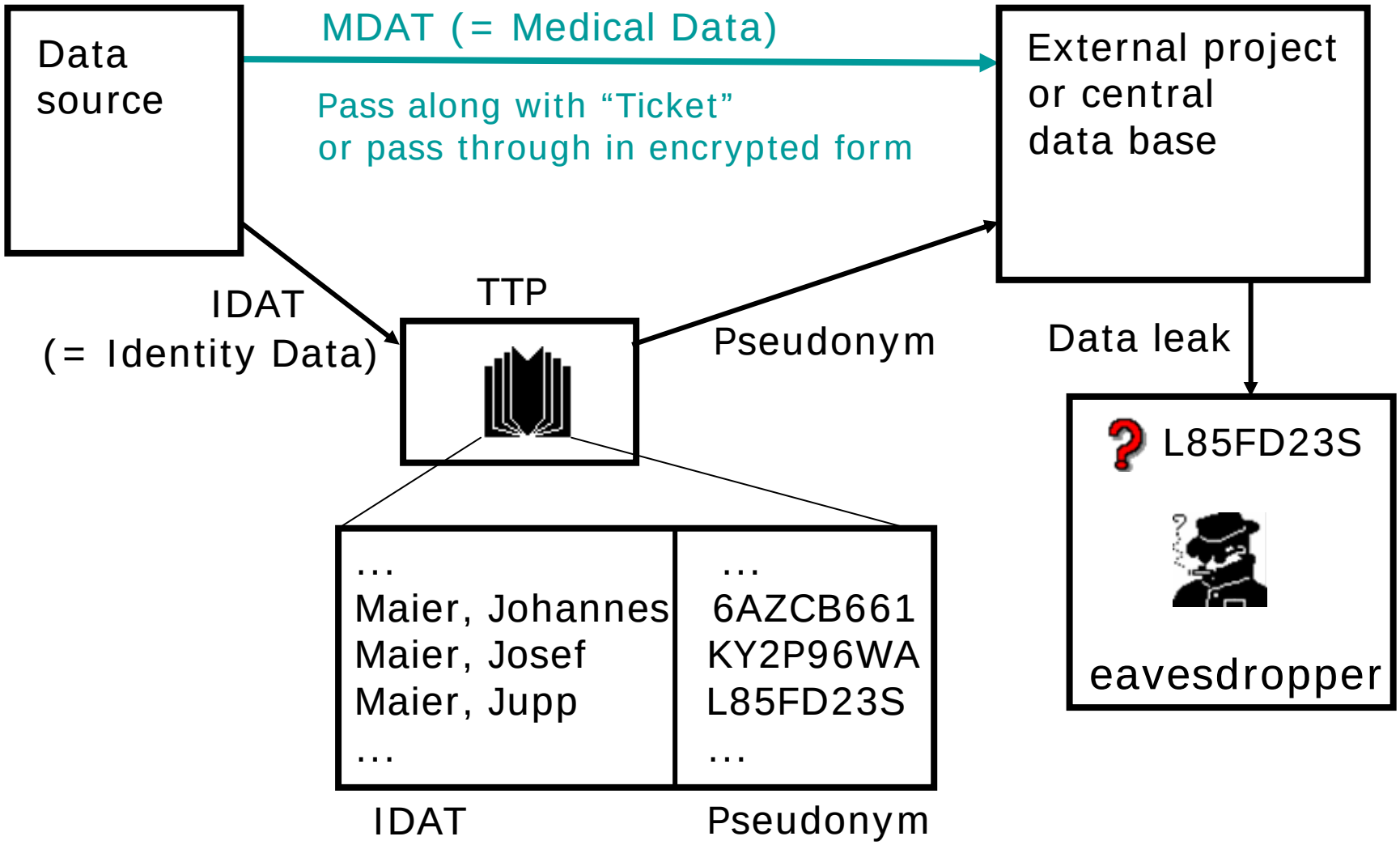
Approaches to Security

- (Anonymisation and) pseudonymisation
  - Pseudonymisation offers far better usability of data
  - but requires considerable organisational effort.
- Strong organisational framework
  - with transparent responsibilities
  - and depseudonymisation rules
  - Approval procedure for projects that need EPR data, genetic data, biomaterial involving steering committee, data protection officer, ethics committee
- Strong IT security also for research projects
- In Germany: TMF* Data Protection Schemes**
  - Tries to balance freedom of research and individuals' rights

* Technologie- und Methodenplattform für die vernetzte medizinische Forschung, www.tmf-ev.de

** KP et al. Integrating eHealth and medical research: The TMF data protection scheme.
In: B. Blobel et. al (Eds): eHealth: Combining Health Telematics, Telemedicine, Biomedical Engineering and Bioinformatics to the Edge. Aka, Berlin 2008, 5–10

How to Pseudonymise Data: The Trusted Third Party (TTP) scheme



JG|U UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Dependable IT systems

- Trustworthy (dependable) IT systems and networks
  - General situation: challenge since >30 years, situation becomes worse
  - What can go wrong will go wrong (see Peter Neumann‘s Risks Digest*).
  - Computer related risks and vulnerabilities ubiquitous
- Dimensions: Availability, integrity, non-repudiation, confidentiality.
- How far can we trust our standard IT systems – hardware, operating systems, software?
- How far can we trust external service providers? Will they get the security right?
  - Privacy of EPR is not a question of shifting liabilities, but of fundamental rights.
  - Comparing security of eHealth with home banking inadequate

* www.risks.org

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Challenges for dependable IT

- The EPR uses a highly vulnerable technology
  - PCs and network infrastructure not trustworthy
  - Intransparent operating systems
  - Software, that permanently phones home
  - “Trusted Computing” (TC) technology used for the profit of “content industry”, against the user
  - Active content (macros) in files of every kind as vehicles for malware
  - Tunnel techniques to evade firewalls

  $\Rightarrow$ Hundreds of targets for hackers.
- Implementation of IT security technology (TC, PKI, Smartcards, ...) missing or inadequate.
  - Techniques exist since at least 20 years, but rarely used
  - Example: Smartcards in health care, Struif ca 1992 working prototype

UNIVERSITÄTSmedizin. MAINZ
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Example: New Communication Technology

- Hospitals and general practitioners are “online”:
  - Mobile technology
  - Wireless networks
  - Use of internet services
  - Medical devices online
  - Remote services
  - Telemedicine
- Cloud computing, social networks:
  - Naive use by employees of hospitals or practitioners
  - Naive use by patients

This causes many security problems and gaps.

No mix of private and professional use! (Beware the scientists!)

Approaches to Safety and Security

We have the means – technology and schemes – to make the EPR safe and secure
in a world where know-how is adequately distributed and applied,
where errors and bugs are a rare exception.

Dear Developers: Devote a small percentage of the resources that go into the development of cool new features to know-how in security.
Consult Ross Anderson's book *Security Engineering*.
Rent a hacker as consultant.

Dear CIOs: Don't run for the latest cool new features only, also acquire security know-how and ask for security.

Layers of EPR Safety and Security

- Ethical layer: Values, principles, laws
- Management (governance) layer: Policies, access rules, trust relations, responsibilities, awareness
- Application layer: Policy enforcement, access control, trustworthy services
- Methodological layer: Network architecture and services, cryptography, pseudonymisation
- Technical layer: Secure hardware, secure OSs, network security

Summary

- The EPR is a highly sensitive object and needs as much protection as possible.
  - By including genetic, AAL, and research data it will become even more sensitive.
  - Protect Patient-Physician relationship as strongly as possible.
  - For secondary use: Anonymisation is illusory, high re-identification risk is unavoidable,
    instead use pseudonyms, rely on transparency and control,
    engage ethic committees, scientific societies, patient communities.
  - Strive for standards and certification.
- The protection of the EPR by current IT is insufficient.
  - It will become even more insufficient by running for the newest innovations and by adding more complexity.
  - Beware the next bug!
- There remain conflicts and even contradictions in requirements that are not easily solved.
  → Balance sought between conflicting goals.