Andreas Holzinger

Lecture 11 – Version WS 2013/14
Biomedical Data: Privacy, Safety and Security

VO 444.152 Medical Informatics

a.holzinger@tugraz.at
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 homologies)
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
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 11th Lecture

- Adverse events
- Anonymization
- Context aware patient safety
- Faults
- Human error
- Medical errors
- Personal health records (PHR)
- Privacy
- Pseudonymization
- Safety
- Security
- Swiss-Cheese Model of human error
- Technical dependability
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;
- **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;
- **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;
Cloud solutions
Mobile solutions
In the medical area require strict Privacy, Data Protection, Security and Safety!
Slide 11-2 We start with thinking about safety first ...

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

• **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 from the outside world;

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

• **Safety** = any **protection from harm, injury, or damage**;
  • (let us continue with safety first ...)


One jumbo jet crash every day
The impact of the “To err is human” IOM study

Patient safety publications before and after publication of the IOM report “To Err is Human”.

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.

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

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.


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)
- **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.

Note: Now just definitions, refer to risk management in Lecture 12.
Improving Safety with Information Technology.
Enhancing Patient Safety with ubiquitous devices

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.

Clinical Example: Context-aware patient safety

Bardram & Norskov (2008)
Slide 11-19 Clinical Example: Context aware patient safety 2/2

(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

### Types of adverse events in medicine and care

<table>
<thead>
<tr>
<th>Number</th>
<th>Events</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sentinel event</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>Accident</td>
<td>The person is not intentionally, indiscriminately, or unsuitable behavior that forms un-expect or unfortunate events.</td>
</tr>
<tr>
<td>3</td>
<td>Incident</td>
<td>Manual error or equipment shutdown causes fault of processing sporadically. No matter what, operation of the system was broken.</td>
</tr>
<tr>
<td>4</td>
<td>Critical incident</td>
<td>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</td>
</tr>
<tr>
<td>5</td>
<td>Incident reporting</td>
<td>To record all un-normal processing and treatment different with normal processing in hospital.</td>
</tr>
<tr>
<td>6</td>
<td>Near miss</td>
<td>Due to un-expect or immediately action makes who has not happen accident, harm, or disease about the patient.</td>
</tr>
<tr>
<td>7</td>
<td>Medical adverse event</td>
<td>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.</td>
</tr>
<tr>
<td>8</td>
<td>No harm event</td>
<td>The event had happen on patient, but has not caused anything or a bit harm.</td>
</tr>
<tr>
<td>9</td>
<td>Preventable - avoidable adverse event</td>
<td>The related employee had done use specify processing that can avoid harm for patients, but related employee still mistake to cause adverse event.</td>
</tr>
<tr>
<td>10</td>
<td>High-alert drugs</td>
<td>The event maybe cause critical harm to patient result from un-normal use or manage drugs.</td>
</tr>
<tr>
<td>11</td>
<td>Adverse drug reaction, ADR</td>
<td>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) :</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Do not using any drugs ( drugs were either therapy nor diagnosis )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To change medicine therapy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To adjust dosage ( to adjust a bit dosage)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Go to hospital over night</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Extension in hospital day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Assisted therapy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Causing diagnosis complicated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Producing negative effect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Result in temporary or permanent harm(disabled or death)</td>
</tr>
<tr>
<td>12</td>
<td>Adverse drug event, ADE</td>
<td>Because the patient take medicine or medical employee has not get medicine result in the event.</td>
</tr>
</tbody>
</table>

A Two-Tiered System of Medicine

<table>
<thead>
<tr>
<th>Category</th>
<th>Ultrasafe System</th>
<th>High-Reliability Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example of industry</td>
<td>Nuclear power</td>
<td>Military systems</td>
</tr>
<tr>
<td></td>
<td>Commercial aviation</td>
<td>Chemical production</td>
</tr>
<tr>
<td></td>
<td><strong>Blood transfusion</strong></td>
<td>Intensive care unit</td>
</tr>
<tr>
<td></td>
<td><strong>Anesthesiology</strong></td>
<td>Surgical ward</td>
</tr>
<tr>
<td></td>
<td>Radiotherapy</td>
<td></td>
</tr>
<tr>
<td>Safety goals</td>
<td>Safety first</td>
<td>Production first (imposed)</td>
</tr>
<tr>
<td></td>
<td>Quality of work preserved against unacceptable pressure</td>
<td>Degree of safety as high as possible for the imposed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>level of performance</td>
</tr>
<tr>
<td>Safety level (in terms of risk per exposure)</td>
<td>Better than $1 \times 10^{-5}$, possibly $1 \times 10^{-6}$</td>
<td>Better than $1 \times 10^{-4}$</td>
</tr>
<tr>
<td>Stability of the process</td>
<td>Well-codified and delineated area of expertise</td>
<td>Broad area of expertise</td>
</tr>
<tr>
<td></td>
<td>Ultradominant, rule-based behavior</td>
<td>Frequent knowledge-based behavior</td>
</tr>
<tr>
<td></td>
<td>Consistent recruitment of patients (flow and quality)</td>
<td>Unstable recruitment of patients (flow and quality)</td>
</tr>
<tr>
<td>Complexity of expertise required</td>
<td>Limited complexity</td>
<td>Potential complexity; severe and abnormal cases are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>challenging</td>
</tr>
<tr>
<td></td>
<td>Actors are requested to follow procedure</td>
<td>Reluctance to simplify</td>
</tr>
<tr>
<td></td>
<td>Equivalent actors</td>
<td>Deference to expertise of individual experts</td>
</tr>
<tr>
<td>Situational awareness</td>
<td>Good at the managerial level</td>
<td>Good among all actors, whatever their role and status</td>
</tr>
<tr>
<td>Supervision</td>
<td>Inside (team) and outside supervision and control (black boxes)</td>
<td>Inside supervision and mutual control (team supervision)</td>
</tr>
<tr>
<td>Teamwork</td>
<td>Effective teamwork and communication, resulting in good task</td>
<td>Effective teamwork and communication, with special</td>
</tr>
<tr>
<td></td>
<td>sharing, controls, and collective routines</td>
<td>attention to safe adaptation to the range of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>individual experts</td>
</tr>
</tbody>
</table>

Amalberti et al. (2005)

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!
The personal data is removed and replaced by a "pseudonym", which allows later tracking back to the source data record.

HSM = Hardware Security Module
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.

Example: private personal health record

http://healthbutler.com/
Example: Concept of a Personal Health Record System 1/4

Slide 11-36

Slide 11-37 Example for component relationships 2/4

Fox et al. (2011)
Single composed application

Publishing widget

Sqwelch: Default.html: receiver()

Sqwelch.com

Subscribing widget: receiver()

postMessage(payload) -> Sempo publishpost(payload)

Trusts, payloads

loop

[for each payload]

[widgettrust=false]

Alert("No widget trust")

postMessage(payload, DOM/widgetId)
Collaborating application

- Sqwelch: Default.html: pollsocialsubscriptions()
- Sqwelch.com
- Subscribing widget: receiver()

**Loop**
- [every 10 seconds]
  - getsocialsubscription(user, view)
  - Trusts, payloads

**Loop**
- [for each payload]
  - [widgettrust=false]
    - Alert(“No Widget Trust”)
  - [usertrust=false]
    - Alert(“No user trust”)
  - postMessage(payload, DOM/widgetid)

Fox et al. (2011)
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.
   - 3. Other users.
   - 4. Other users, healthcare professionals and services/programs.
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.
### Overview Personal Health Records (PHR)

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

**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)
Privacy, Security, Safety and Data Protection are of enormous increasing interest in the future. Due to the trend to mobile and cloud computing approaches and the omnipresence of data it is of vital importance. Electronic Health Records (EHR) are the fastest growing example of an application which concern data privacy and patient consent. Increasing amounts of personal health data are being stored in databases for the purpose of maintaining a life-long health record of an individual.

A further big issue is secondary use of data, providing patient data for clinical or medical research. For most secondary data use, it is possible to use deidentified 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.

Another issue is the production of anonymized open data set to support international joint research efforts.
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.ico.gov.uk](http://www.ico.gov.uk) (Information Commissioner’s Office in the UK)
- [http://www.dsk.gv.at/](http://www.dsk.gv.at/) (Österreichische Datenschutz Kommission)
- [http://videolectures.net/kdd09_mohammed_ahdcsbts](http://videolectures.net/kdd09_mohammed_ahdcsbts) (Anonymizing Healthcare Data: A Case Study on the Blood Transfusion Service)
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.

Appendix: Example for a simple warning message

Appendix: Example for trust policies in HIS networks

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!

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 homologies)
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
Thank you!