# Information security in health care

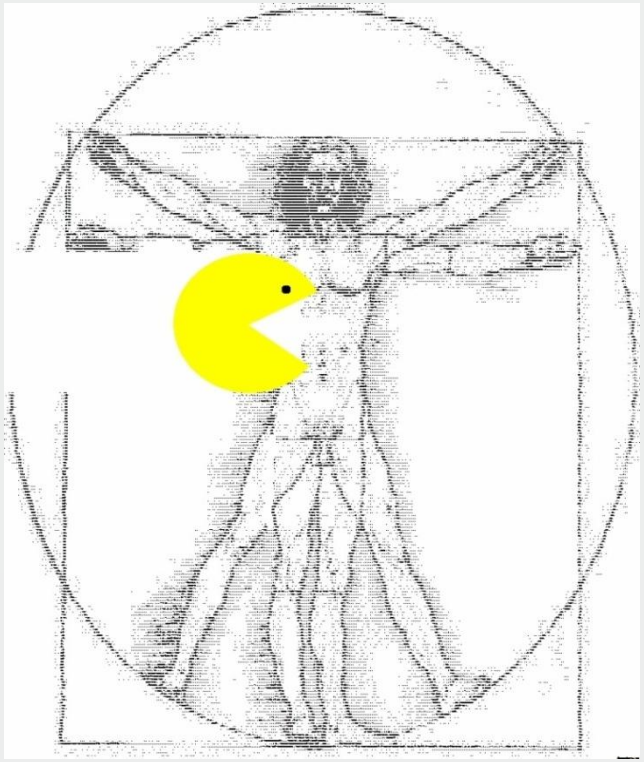
## Evaluation with health professionals

Robin Krens
Marco Spruit
Nathalie Urbanus-van Laar

Universiteit Utrecht

# Agenda

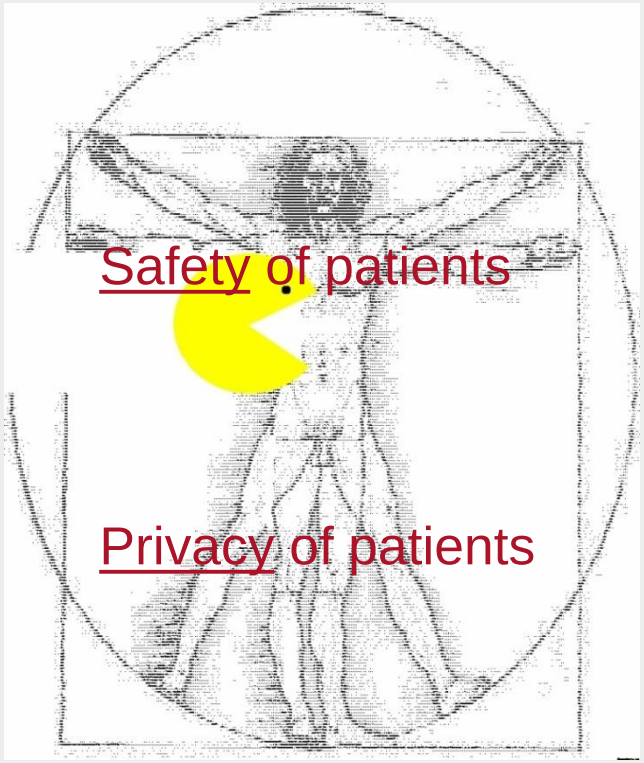
- Introduction to information security
- Research approach
- Evaluation Instrument (ISEE)
- Results
- Summary and discussion



# Introduction

## the scope of information security*

- Availability: Gone?! But I need that information. Now!
- Integrity: But the medical record said blood type B+ …
- Confidentiality: Whoops, now the whole world knows you have Gonorrhea!




Universiteit Utrecht



* Defined as by the Dutch Health Care inspectorate

# Introduction
## research trigger

- Information security in Dutch hospitals is lacking (IGZ & CBP, 2008)
  - Risks for both health care and privacy
  - Staff as weakest link
  - National EMR infrastructure

- New possibilities
- A narrow focus on technical oriented approaches (Siponen, 2005) and the confidentiality aspect (Barber, 2002):

> "the issues of integrity and availability will probably deserve more attention than the issues of confidentiality as medical information systems become more inter-twined with clinical practice"

# Introduction
## approaches*


- Technology *or* solutions
  - i.e. intrusion detection systems

| ISO 27002 Best Practice | NIST | PCI DSS | SOX | HIPAA |
|---|---|---|---|---|
| 4. Risk Assessment and Treatment | ✓ | ✓ | ✓ | ✓ |
| 5. Security Policy | ✓ | ✓ | ✓ | ✓ |
| 6. Organization of Information Security | ✓ | | | ✓ |
| 7. Asset Management | ✓ | | ✓ | ✓ |
| 8. Human Resources Management | ✓ | | | ✓ |
| 9. Physical and Environmental Security | ✓ | ✓ | ✓ | ✓ |
| 10. Communications and Operations Management | ✓ | ✓ | ✓ | ✓ |
| 11. Access Control | ✓ | ✓ | ✓ | ✓ |
| 12. Information Systems Acquisition, Development and Maintenance | ✓ | ✓ | ✓ | ✓ |
| 13. Information Security Incident Management | ✓ | ✓ | ✓ | ✓ |
| 14. Business Continuity Management | ✓ | | ✓ | ✓ |
| 15. Compliance | ✓ | | ✓ | ✓ |

- Processes *or* checklists and standards
  - i.e. ISO27002, CoBIT

- People *or* perception and awareness



* Dhillon & Backhouse (2002) Current directions in IS security research: towards socio-organizational perspectives
* Siponen (2005) An analysis of the traditional IS security approaches: implications for research and practice

# Introduction
## people's perspective

- Hey! Let's evaluate with the day-to-day users:
- Within a hospital department day-to-day users are:
  - Doctors
  - Nurses
  - Management
  - Supporting staff
- *How can we evaluate information security from a health professional's perspective?*

Universiteit Utrecht

# Evaluation instrument

## concepts

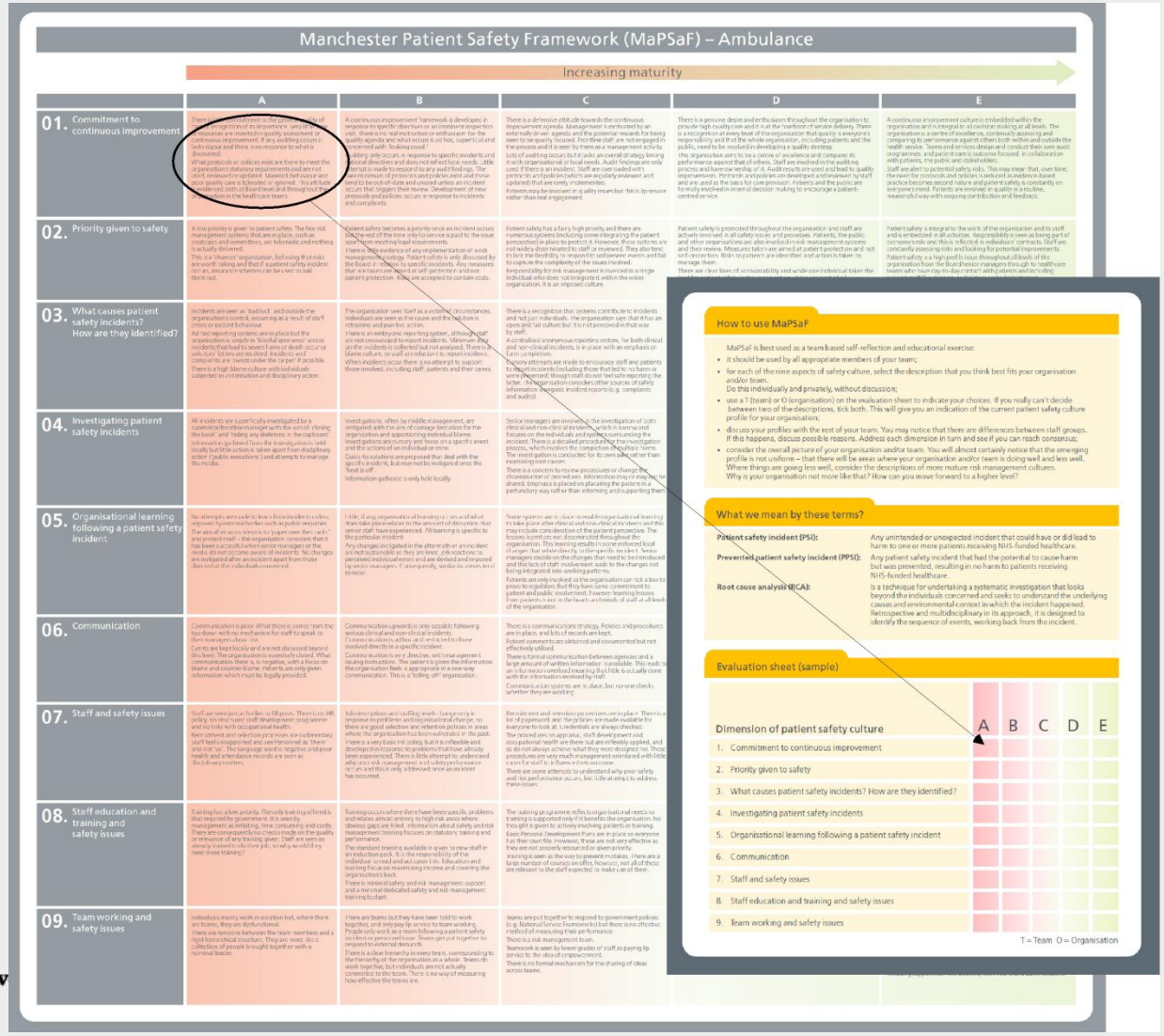
- Not from scratch,
  but usage of an existing instrument MaPSaF*:
  - *How safe is our patient?*
- MaPSaF elements:
  - Evaluation with 6 – 12 health care workers
  - Workshop like evaluation
  - A maturity framework
  - A variety of dimensions

Universiteit Utrecht

* Manchester Patient Safety Framework (NHS and University of Manchester, 2006)

# Evaluation instrument

## concepts (2)



# Research approach*

- Information Security Employee Evaluation (ISEE)
  - Step 1: Building
    - re-use of MaPSaF
    - literature review
    - focus group (delphi-like)
  - Step 2: Piloting ISEE
    - applying the instrument as workshop (5x)

Universiteit Utrecht



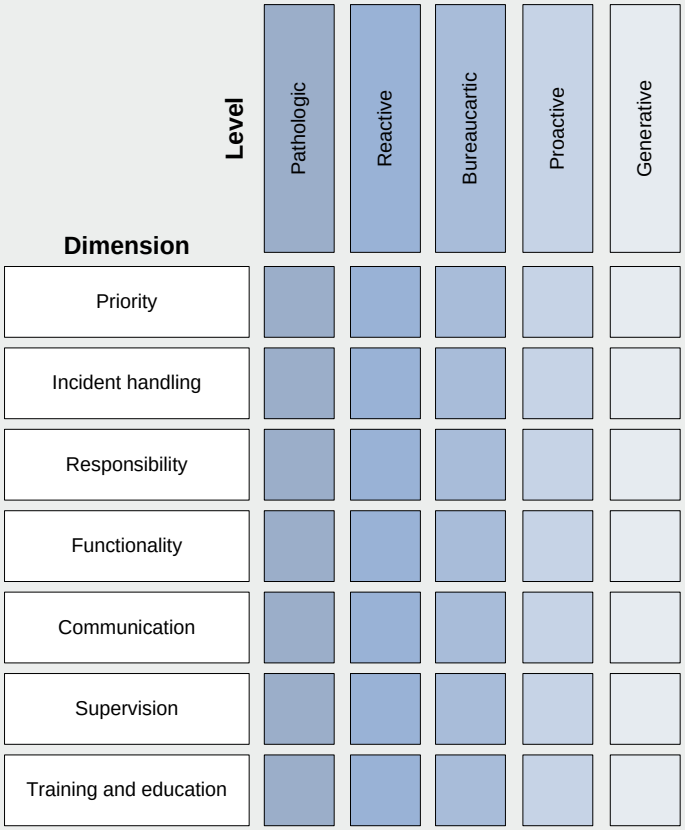
*Design Science as defined by Hevner (2004)

# Step 1: Building ISEE

| Dimension | Description | Examples |
|---|---|---|
| Priority | Priority of security at the department. | budget for security, problem-solving |
| Incident Handling | Handling of security-related incidents. | system downtime and restore |
| Responsibility | Awareness and responsibility. | awareness on privacy |
| Functionality of security | Effective implementation of security mechanism. | inadequate systems |
| Communication | Communication on security related issues. | communication about legislation |
| Supervision | Supervision and control on usage. | unauthorized access to data, logging and audit |
| Training and education | Training and education on security related issues. | usage of mobile devices, usage of encryption |

Universiteit Utrecht

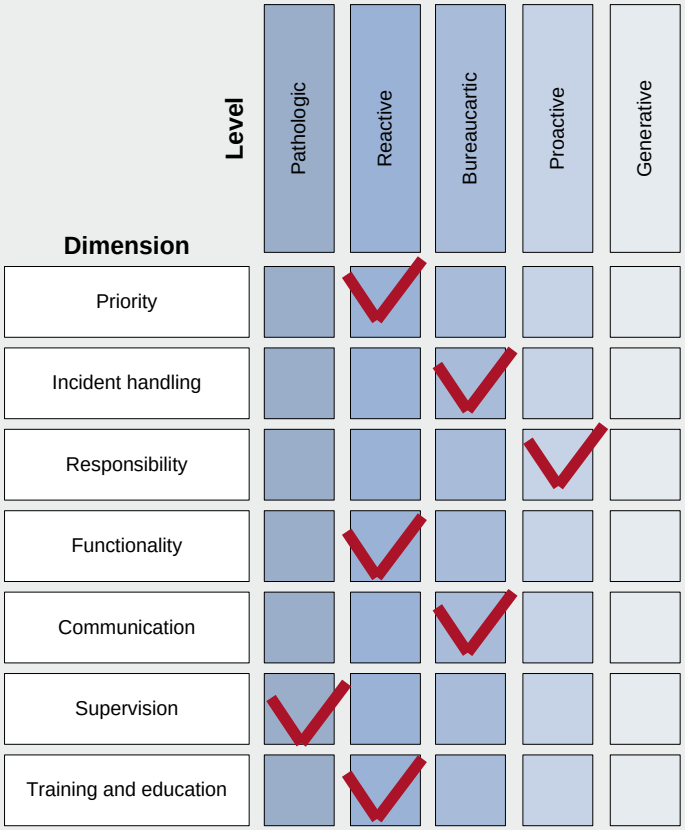
# Step 1: Building ISEE




- Combined with underlying framework of Westrum (1998), Parker & Hudson (2001)
  - How do we rate our department?
- Added examples for each cell

| Dimension / Level | pathologic | reactive | |
|---|---|---|---|
| Priority<br>How important do employees consider the security (availability, integrity and confidentiality) of patient data?<br>What is done to provide adequate security? | • Risks are not recognized (i.e. System downtime or privacy breaches) .<br>• There are no (emergency) plans made to gaurentee the securiy of patient data.<br>• There is a lack of protocols to guarentee the availability, integrity and confidentiality of patient data. | • After an incident there is an increase in awareness.<br>• Solutions are temporarily and planned ad-hoc.<br>• Protocols and guidelines are not up to date. | •Healt<br>are aw<br>patient<br>• Now<br>made<br>securit<br>• Proto<br>are rev<br>manag<br>known |
| Handling of incidents<br>Is the importance of incident reporting | • "Reporting incidents with patient data is not part of health care professional's job" .<br>• It is not clear where and | • There is a reluctance in incident reporting. Health care professionals are not encouraged to report.<br>• A variety of reporting | • Heal<br>are aw<br>of inci<br>are, ho<br>to repo |

# Step 2: Piloting ISEE




- Piloting the instrument as workshops (~1.5 hours)
- A crosscut of a hospital department (6 – 10 persons).

| | |
|---|---|
| Radiology, UMC Utrecht | 7 participants, different disciplines |
| Radiotherapy, UMC Utrecht | 8 participants, different disciplines |
| Skin diseases, LUMC | 10 participants, different disciplines |
| Hematology, LUMC | 7 participants, mostly nursing |
| Urology, UMC Utrecht | 8 participants, different disciplines |

Universiteit Utrecht

# Piloting ISEE as workshops

- Workshop structure:
  - Fill out instrument individually
  - Compare scores
  - Discuss and write down key issues
    - *"I don't know what to do in case of a system failure"*
    - *"The systems are slow and are a threat to the patient!"*
    - *"Am I allowed to mail these files to the general practitioner?"*
  - Make action plan
  - Reflection on workshop and instrument

# Pilot study

## evaluation

| INSTR. Dimensions | Mean (1-5) | Std | Range (1-5) | Floor (x) | Ceiling (x) |
|---|---|---|---|---|---|
| Skin Diseases | | | | | |
| Priority | 2,75 | 0,47 | 2-4 | 0 | 0 |
| Handling of incidents | 3,10 | 0,94 | 1-4,5 | 1 | 0 |
| Responsibility | 3,55 | 0,49 | 3-4 | 0 | 0 |
| Functionality | 2,50 | 1,25 | 1-4 | 3 | 0 |
| Communication | 2,75 | 0,72 | 2-4 | 0 | 0 |
| Supervision | 2,05 | 0,83 | 1-3 | 3 | 0 |
| Training and education | 2,55 | 0,94 | 2-4 | 0 | 0 |

- *Incidents:* "When the allergy EHR is restored, my session is already over"
- *Functionality:* "It's a mess, we have protocols on where to put what data, but this happens rarely"
- *Supervision:* "Supervision is pure ethics"
- *Training:* "I know about the Hippocrates oath, but I have no clue if I'm allowed to mail files to general practitioners"

Universiteit Utrecht

# Discussion and conclusion

- The ISEE instrument
  - Based on MaPSaF
  - Face validated by experts and subject matter experts
  - Feasible and acceptable within the amount of time
  - Practically useful
    - Highlights weak points within departments
- More workshops
  - More data
- Generic dimensions, need for specification
  - Survey-like instrument