

Information security in health care

Evaluation with health professionals

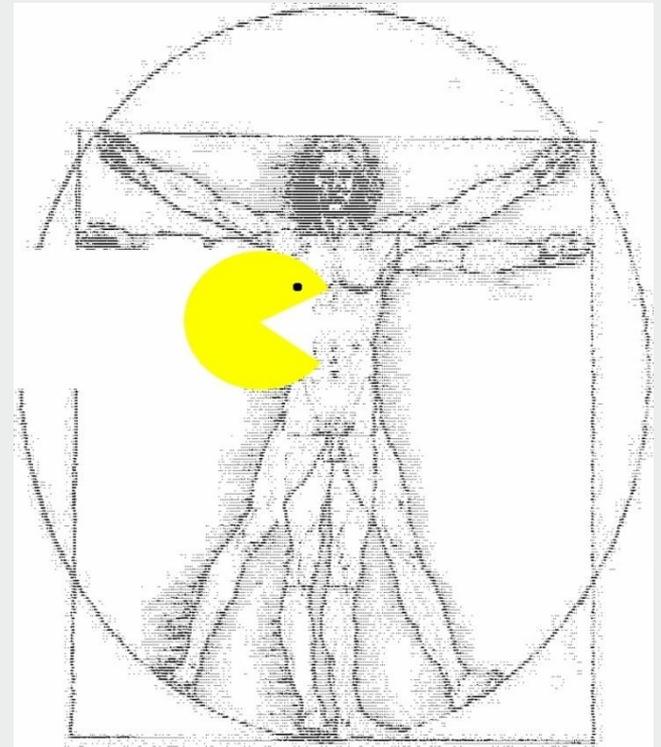
Robin Krens
Marco Spruit
Nathalie Urbanus-van Laar



Universiteit Utrecht

Agenda

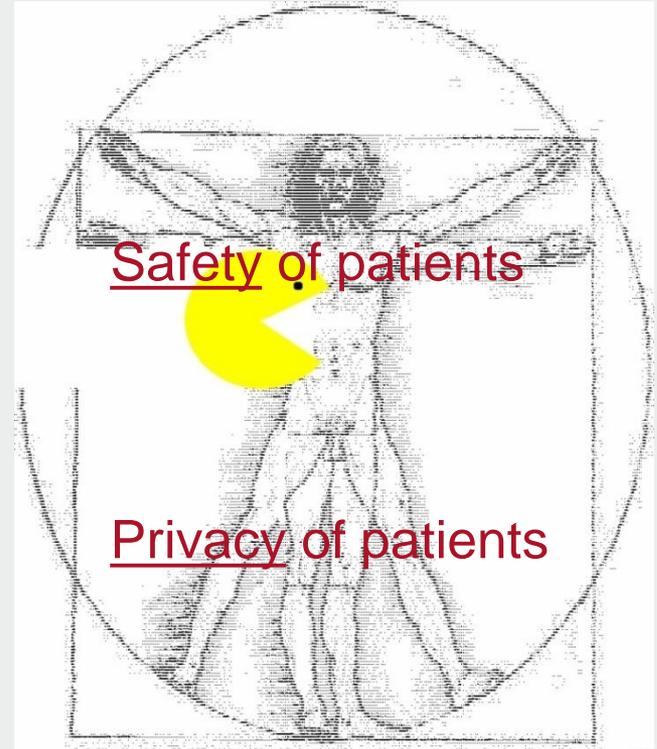
- Introduction to information security
- Research approach
- Evaluation Instrument (ISEE)
- Results
- Summary and discussion



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 Gonorrhoea!



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



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

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	✓		✓	✓

- People *or* perception and awareness



Universiteit Utrecht



* Dhilton & 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**?*



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



Evaluation instrument concepts (2)

Manchester Patient Safety Framework (MaPSaF) – Ambulance

		Increasing maturity				
		A	B	C	D	E
01	Commitment to continuous improvement	There is a sign of an intention to improve and measures are needed to regularly assess or continuously improve. If any safety issues occur, they are treated as a response to what is known.	A continuous improvement framework is developed. Progress is specific, identifiable and measurable. Staff, there are no restrictions or barriers for the safety issues that occur in the hospital and increased staff feedback.	There is a definitive attitude towards the continuous improvement process. Management is involved by an authority or an agency and the patient's views for being taken into account. For example, staff are not engaged in the process and it is seen by them as a management activity.	There is a genuine desire and intention throughout the organisation to provide high quality care and to be the best of our industry. There is a recognition of every level of the organisation that quality is everyone's responsibility and that the quality expectations, including patients and the public, need to be met in developing a quality strategy.	A continuous improvement culture is embedded within the organisation and is integral to all of our work and all staff. The organisation is a centre of excellence, continues to improve and is recognised by the performance agencies both before and outside the health service. Terms and services developed and conducted their own audit processes and participate actively in national accreditation and public involvement. Staff are able to generate quality. This may mean that, over time, the new services and policies are developed and introduced and become secure states and patient safety is everybody's business. Patients are involved in quality as a practice, not only in the way we interact with our patients but also in the way we interact with our staff and our suppliers.
02	Priority given to safety	A low priority is given to patient safety. The few risk management systems that are in place, such as policies and procedures, are inflexible and poorly or not fully delivered.	Patient safety becomes a priority once an incident occurs. The rest of the time only serves to add to the usual work. There is no evidence of any representation of safety management systems. Information is only discussed by the Board or other senior personnel and patient protection is not accepted to contain costs.	Patient safety has a fairly high priority, and there are numerous systems including one designed for the patient and other employees are also involved in risk management systems and not widely disseminated to staff or received. There is also no evidence of any representation of safety management systems. Information is only discussed by the Board or other senior personnel and patient protection is not accepted to contain costs.	There is a recognition that systems contribute to incidents and not just individuals. The organisation sees that an open and fair culture but is not perceived that way by staff.	Patient safety is promoted throughout the organisation and staff are actively involved in all safety issues and processes. Patients, the public and other employees are also involved in risk management systems and their views. Measures taken are aimed at patient protection and not just compliance. Staff are perceived as individuals and not as a group. There are clear lines of accountability and who is responsible to take the responsibility for risk management is understood in a way that is accepted to contain costs.
03	What causes patient safety incidents? How are they identified?	Incidents are seen as 'bad luck' and outside the organisation's control, occurring as a result of staff errors or patient behaviour.	The organisation sees that a variety of circumstances, individuals are seen as the cause and the 'bad' events, mistakes and positive action.	A confidential anonymous reporting system, for both staff and patients, is in place with an emphasis on staff. Reporting systems are made to encourage staff and patients to report incidents and the best to be reported.	There is a recognition that systems contribute to incidents and not just individuals. The organisation sees that an open and fair culture but is not perceived that way by staff.	Incidents are seen as 'bad luck' and outside the organisation's control, occurring as a result of staff errors or patient behaviour.
04	Investigating patient safety incidents	All incidents are superficially investigated to a limited extent and 'blame' any individuals in the system.	Investigations, often by middle management, are designed to identify management failures in the organisation and assign responsibility to individual blame.	Senior managers are involved in the investigation of staff and patients incidents. The investigation of staff and patients incidents is conducted by a team of staff and patients. The investigation of staff and patients incidents is conducted by a team of staff and patients. The investigation of staff and patients incidents is conducted by a team of staff and patients.	There is a recognition that systems contribute to incidents and not just individuals. The organisation sees that an open and fair culture but is not perceived that way by staff.	All incidents are superficially investigated to a limited extent and 'blame' any individuals in the system.
05	Organisational learning following a patient safety incident	No attempts are made to learn from incidents to either improve systems or to learn from public expectations.	Learning is seen as a result of an incident and is not shared with other staff.	Some systems are in place to learn from incidents but they are not shared with other staff.	There is a recognition that systems contribute to incidents and not just individuals. The organisation sees that an open and fair culture but is not perceived that way by staff.	No attempts are made to learn from incidents to either improve systems or to learn from public expectations.
06	Communication	Communication is poor. What there is comes from the bottom up. There is no formal system for staff to speak to the management.	Communication is poor. What there is comes from the bottom up. There is no formal system for staff to speak to the management.	There is a communication system. Policies and procedures are in place and followed. There is a communication system. Policies and procedures are in place and followed.	There is a recognition that systems contribute to incidents and not just individuals. The organisation sees that an open and fair culture but is not perceived that way by staff.	Communication is poor. What there is comes from the bottom up. There is no formal system for staff to speak to the management.
07	Staff and safety issues	Staff are seen as a barrier to safety. There is no formal system for staff to speak to the management.	Staff are seen as a barrier to safety. There is no formal system for staff to speak to the management.	Staff are seen as a barrier to safety. There is no formal system for staff to speak to the management.	There is a recognition that systems contribute to incidents and not just individuals. The organisation sees that an open and fair culture but is not perceived that way by staff.	Staff are seen as a barrier to safety. There is no formal system for staff to speak to the management.
08	Staff education and training issues	Training is a low priority. The only training offered is for the management.	Training is a low priority. The only training offered is for the management.	Training is a low priority. The only training offered is for the management.	There is a recognition that systems contribute to incidents and not just individuals. The organisation sees that an open and fair culture but is not perceived that way by staff.	Training is a low priority. The only training offered is for the management.
09	Team working and safety issues	Individuals mainly work in isolation but, where there are some teams between the team, members and a collection of people brought together with a common goal.	Individuals mainly work in isolation but, where there are some teams between the team, members and a collection of people brought together with a common goal.	Individuals mainly work in isolation but, where there are some teams between the team, members and a collection of people brought together with a common goal.	There is a recognition that systems contribute to incidents and not just individuals. The organisation sees that an open and fair culture but is not perceived that way by staff.	Individuals mainly work in isolation but, where there are some teams between the team, members and a collection of people brought together with a common goal.

How to use MaPSaF

- MaPSaF is best used as a team based self-reflection and educational exercise:
- It should be used by all appropriate members of your team;
- For each of the nine aspects of safety culture, select the description that you think best fits your organisation and/or team.
- Do this individually and privately, without discussion.
- Use a 1 (Team) or 0 (Organisation) on the evaluation sheet to indicate your choices. If you really can't decide between two of the descriptions, tick both. This will give you an indication of the current patient safety culture profile for your organisation.
- Discuss your profiles with the rest of your team. You may notice that there are differences between staff groups. Discuss these differences and identify reasons. Address each dimension in turn and see if you can reach consensus.
- Consider the overall picture of your organisation and/or team. You will almost certainly notice that the emerging profile is not uniform – that there will be areas where your organisation and/or team is doing well and less well.
- Where things are going less well, consider the descriptions of more mature risk management cultures.
- Why is your organisation not more like that? How can you move forward to a higher level?

What we mean by these terms?

- Patient safety incident (PSI):** Any unintended or unexpected incident that could have or did lead to harm to one or more patients receiving funded healthcare.
- Prevented patient safety incident (PPSI):** Any patient safety incident that had the potential to cause harm but was prevented, resulting in no harm to patients receiving NHS-funded healthcare.
- Root cause analysis (RCA):** A technique for undertaking a systematic investigation that looks beyond the individuals concerned and seeks to understand the underlying causes and environmental context in which the incident happened. Retrospective and multidisciplinary in its approach, it is designed to identify the sequence of events, working back from the incident.

Evaluation sheet (sample)

Dimension of patient safety culture	A	B	C	D	E
1. Commitment to continuous improvement					
2. Priority given to safety					
3. What causes patient safety incidents? How are they identified?					
4. Investigating patient safety incidents					
5. Organisational learning following a patient safety incident					
6. Communication					
7. Staff and safety issues					
8. Staff education and training and safety issues					
9. Team working and safety issues					

T = Team O = Organisation



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)



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



Step 1: Building ISEE

Dimension	Level	Pathologic	Reactive	Bureaucratic	Proactive	Generative
Priority						
Incident handling						
Responsibility						
Functionality						
Communication						
Supervision						
Training and education						

■ 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 How important do employees consider the security (availability, integrity and confidentiality) of patient data? What is done to provide adequate security?	<ul style="list-style-type: none"> Risks are not recognized (i.e. System downtime or privacy breaches) . There are no (emergency) plans made to guarantee the security of patient data. There is a lack of protocols to guarantee the availability, integrity and confidentiality of patient data. 	<ul style="list-style-type: none"> After an incident there is an increase in awareness. Solutions are temporarily and planned ad-hoc. Protocols and guidelines are not up to date. 	<ul style="list-style-type: none"> Healthcare professionals are aware of patient data security. Now made in security. Protocols are reviewed and managed known.
Handling of incidents Is the importance of incident reporting...	<ul style="list-style-type: none"> "Reporting incidents with patient data is not part of health care professional's job" . It is not clear where and 	<ul style="list-style-type: none"> There is a reluctance in incident reporting. Health care professionals are not encouraged to report. A variety of reporting 	<ul style="list-style-type: none"> Healthcare professionals are aware of incidents and how to report.



Step 2: Piloting ISEE



Dimension	Pathologic	Reactive	Bureaucratic	Proactive	Generative
Priority		✓			
Incident handling			✓		
Responsibility				✓	
Functionality		✓			
Communication			✓		
Supervision	✓				
Training and education		✓			

- 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



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"



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

