

---

# Standardisation as a Mean to Improve Information Security in Process-Oriented Distributed Healthcare

---

Eva Söderström, Rose-Mharie Åhlfeldt  
and Nomie Eriksson

University of Skövde

EURAS 2008, 16-17 June, 2008

---

# Structure of presentation

- ◆ Introduction
- ◆ Aim
- ◆ Distributed Healthcare
- ◆ Information Security
- ◆ Mapping info sec standards to process oriented distributed healthcare
- ◆ Discussion and concluding remarks

# Introduction

- ◆ The healthcare professionals need access to all relevant information about a patient.
- ◆ Patients visit several caregivers during an illness.
- ◆ There is a lack of a process-oriented view.
- ◆ Standards are needed to ensure security in healthcare.



---

# The aim

- ◆ ... is to investigate how current standards map against the concept of information security, and how process-orientation can be used in conjunction with standards to create secure information flows in healthcare.

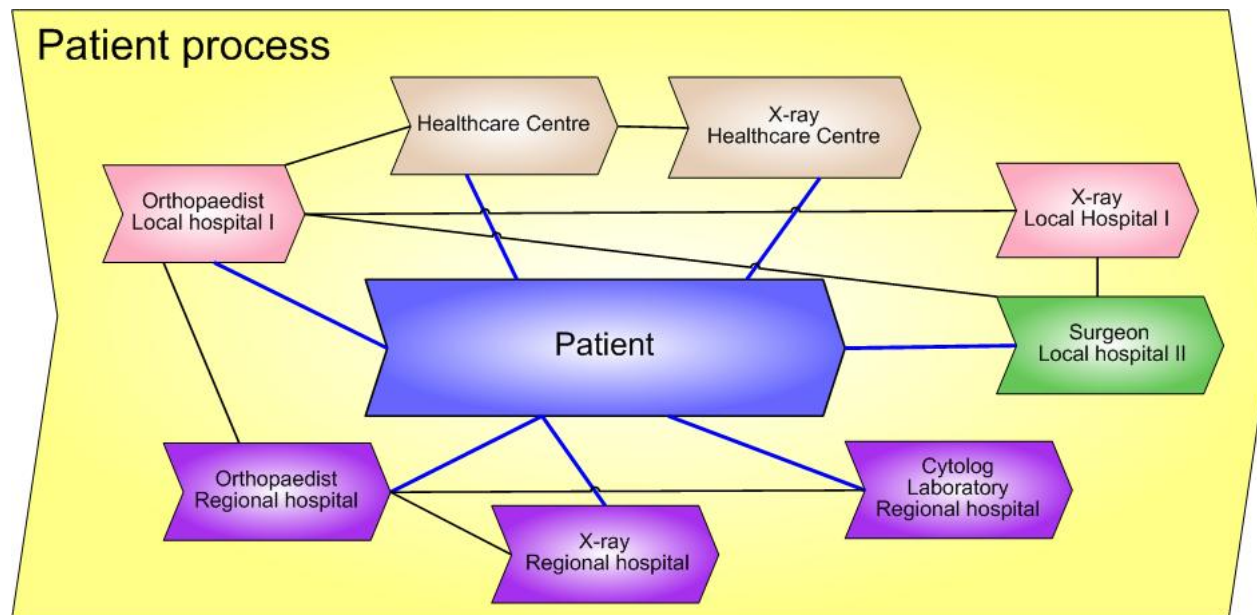
---

# Healthcare

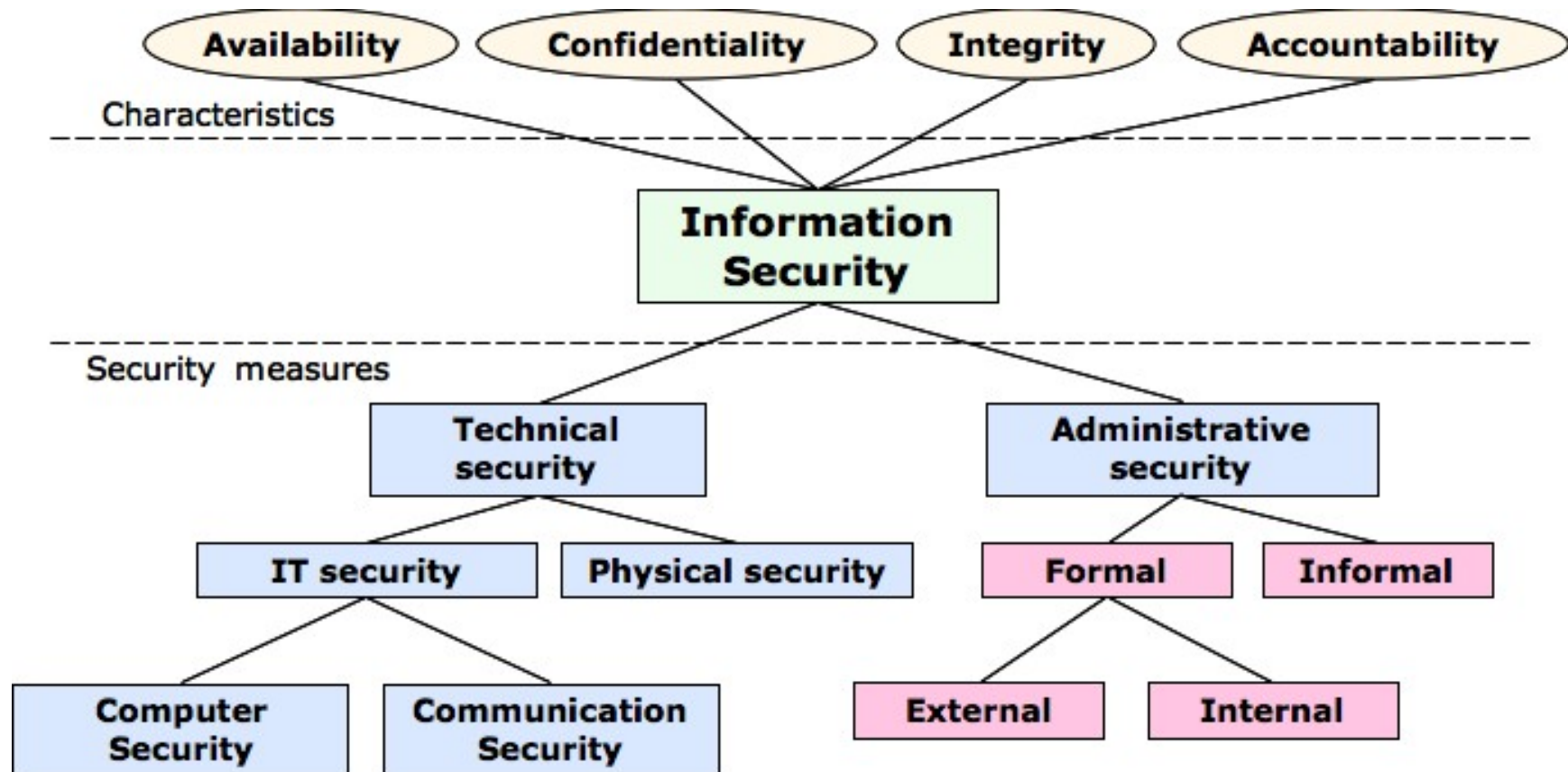
- ◆ Slow implementation of IT in Healthcare.
- ◆ EHR – Electronic Healthcare Record.
- ◆ EHR bodes well for improved healthcare.
- ◆ New solutions must achieve interoperability between the different caregivers.
- ◆ This is one area where standards can help.

# Healthcare cont.

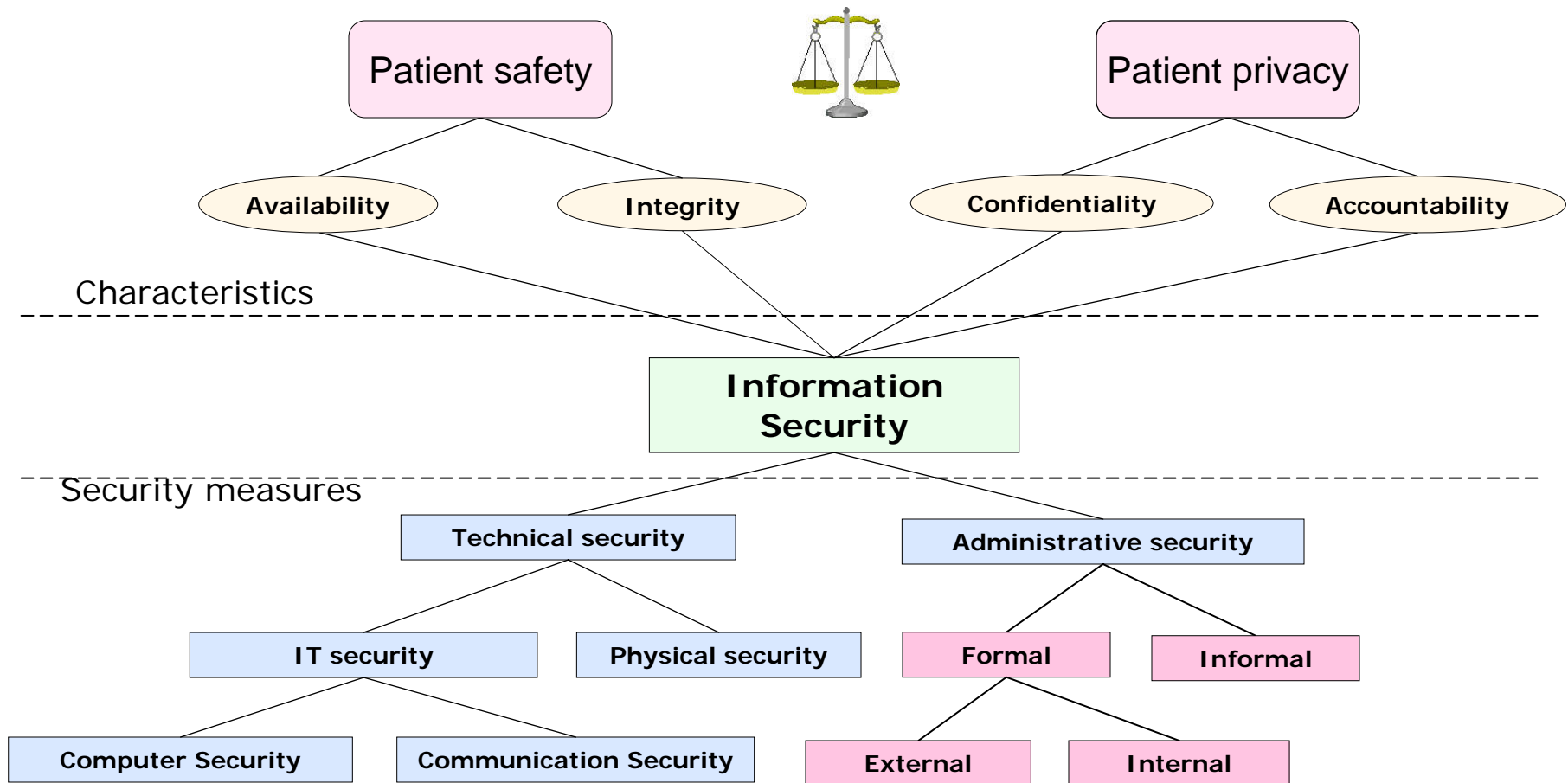
- ◆ Process-orientation in healthcare
- ◆ Communicating across borders



# Information Security



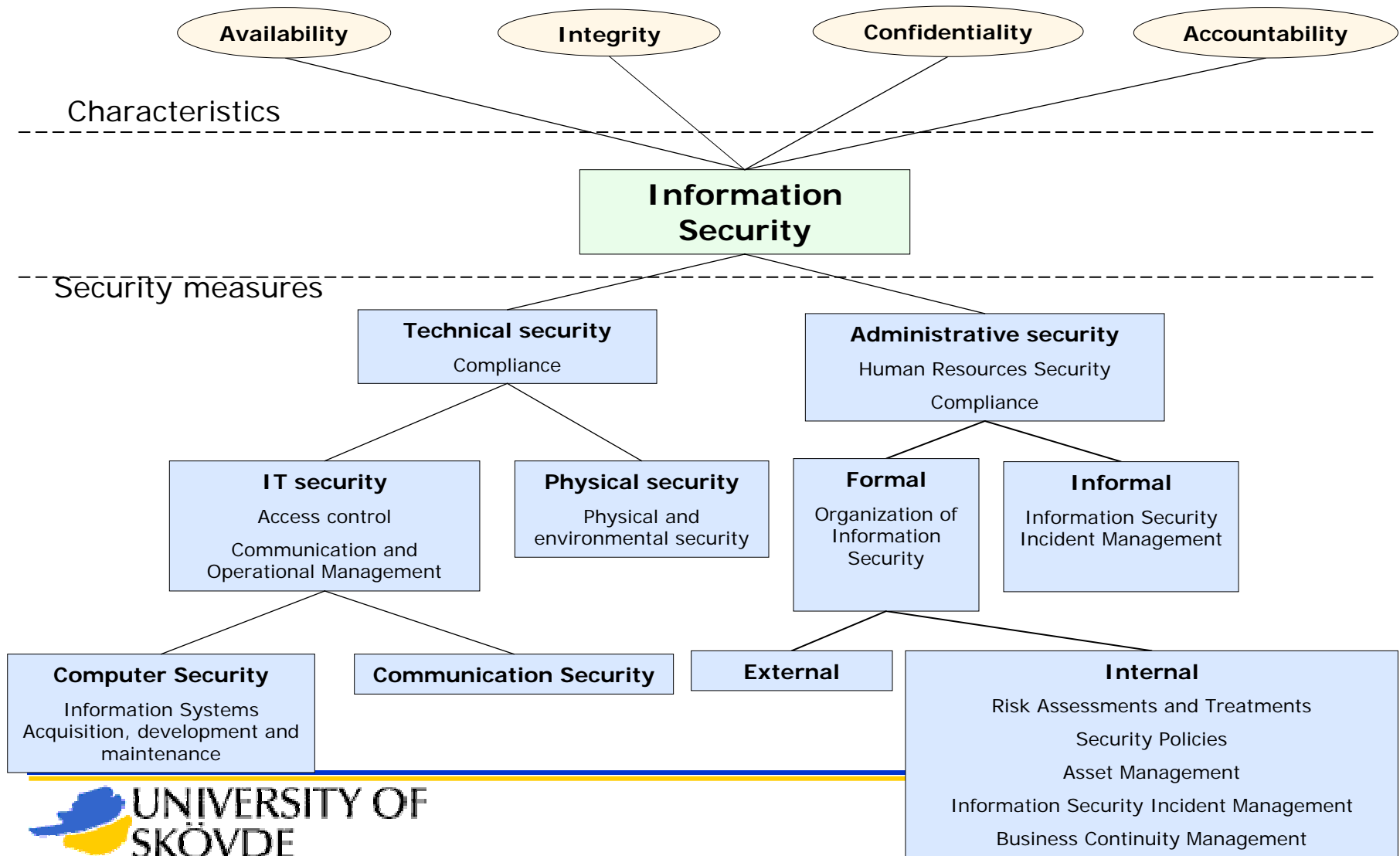
# The Need for Information security in Healthcare



# ISO/IEC 27000-family

- ◆ ISO 27001: a specification for an information security management system (ISMS)
  - ◆ **ISO 27002: Code of best practice of Information Security Management**
  - ◆ ISO 27003: will include guidance for implementing an ISMS
  - ◆ ISO 27004: will include ISMS measures and metrics
  - ◆ ISO 27005: will cover information security risk management
  - ◆ ISO 27006: will include guidelines for the accreditation of organisations offering ISMS certification
1. Risk Assessment and Treatments
  2. Security Policies
  3. Organisation of information security
  4. Asset Management
  5. Human Resources Security
  6. Physical and environmental security
  7. Communication and Operational Management
  8. Access Control Management
  9. Information System Acquisition, Development and Maintenance
  10. Information Security Incident Management
  11. Business Continuity Management
  12. Compliance

# Mapping info sec standards to process-oriented distributed healthcare



---

# Process-orientation is standardization of activities

- ◆ Process-orientation *is* standardization the healthcare personnel has implemented since it is a form of control and coordination.
- ◆ The increasing power of standardization goes together with a high legitimacy for those who know better.
- ◆ The professions have taken it as their right to know how healthcare is best to be conducted.
- ◆ Well-developed standardization may therefore be considered as a threat against professional expertise, a problem since the standardisation bodies set the standards for other organisations.
- ◆ There is a need to clearly define the ownership of health information assets.
- ◆ There is a lack of unique standards for health information classification as well as procedures for information labelling and handling in accordance with the classification scheme.

---

# Conclusion

- ◆ Standardisation of the healthcare chain, i.e. the patient process, is not about either the documents *or* the processes. It is about both.
- ◆ It is a matter of incorporating the ISO standards into management, the administrative side of healthcare activities, and plan for their use in the everyday activities.
- ◆ Information security work should be based on established and well-known standards for information security management and these standards should explicitly cater better for the administrative information security part.
- ◆ The best way to reach a sufficient level of information security is to use a structured way of working, and hence, the use of a well-known standard