# The Role of Information System Security in Contemporary Health Information Systems

Doctoral Seminar, University of Bern
February 2006

By Martin Lüthi

# Table of Contents

# 1 Introduction

## 1.1 Problem

Health care organizations have been slow adopters of information technology (IT). Albeit the provision of medical services is fundamentally an information intense activity, its adoption has lagged behind other industries.[1] Rationales may be traced to market, institutional, and regulative factors as well as difficulties inherent to health care organizations.[2] Recent increases in hospital IT spending and activities indicate an augmented support of administrative and clinical processes.[3] It can be assumed that these increases were partly triggered by efficiency objectives and are likely to continue. Consequently, exchange and reliance on a multitude of electronic information stored in heterogeneous and decentralized health information systems (IS) is increasing.

At the same time, various reports about IS security breaches, unintended information disclosures, and computer attacks have raised the awareness of organizations, government entities, legislatures, and the general public.[4] Whereas the confidentiality of individual health information has been discussed for many years, additional patient safety concerns regarding the integrity and availability of vital and time-sensitive clinical information have enhanced the debate.[5] Competing interests of easy accessibility of vital

[1] Cf. Garrard (2000), pp.1557-1558. Adoption refers here to the degree of IT use within an organization, and not to the adoption by individuals.

[2] E.g., in Europe, inpatient care organizations tend to be dominated by government and the public sector, in the U.S. a majority is run by private not-for-profit organizations. Furthermore, the industry is highly regulated and localized; entrepreneurial freedom and incentives are limited. Inherent reasons include a unique organizational structure, the diversity and number of interacting professionals, many data sources, little standardization, and complex data sets. Cf. Garrard (2000), p.1558.

[3] Cf. Dorenfest (1997); Dorenfest (2000); Lohr (2005); Nairn (2005).

[4] Cf. Carrns (2000); Flammer (2003); Halbeis (2003); Krim (2005); O'Harrow (2000); Rowland (2005).

[5] Cf. IOM (1997); NRC (1997); Rigby, et al. (2001); Rindfleisch (1996). Several regulations explicitly include the protection of electronic individual health information: in European countries, the protection of personal information, of which health data is a subset thereof, is mostly regulated by strict laws. In the

information versus privacy protection objectives can be interdependent with user acceptance.[6] Even if regulatory compliance requirements mandate the use of IS security safeguards, their effectiveness, practicability, and influence upon publicly accessible health care settings using multi-user and multi-access terminals is largely unknown.[7] Additionally, the capability to implement IS security policy within the tripartite socio-organizational power structure of a hospital with often powerful, divisionally-organized, and semi-autonomous medical departments remains uncertain.

## 1.2 Objective

The paper at hand provides an overview of the role of IS security in health IS at U.S. and Swiss hospital organizations. The term health IS is used from an acute-care hospital perspective since they are the dominant health care provider organizations in many health systems, hold large data repositories of patient data, and often operate under significant resource constraints. On a preliminary basis, this paper summarizes findings from a qualitative empirical research study based on ten semi-structured expert conversations and four in-depth case studies performed in the U.S. and Switzerland with two academic medical centers (referred to as $US_1$ and $CH_1$) and two multi-hospital groups (referred to as $US_2$ and $CH_2$). The study is based on the following research questions:

U.S., privacy laws are less strict and health data is protected by separate regulations. Most regulations include IS security requirements since it has been recognized that without proper security measures privacy and data protection cannot be ensured.

[6] E.g., if personnel are required to authenticate to multiple applications frequently using inconvenient procedures, then applications and systems may potentially be abandoned. Due to user inconvenience, paper-based dual-systems are likely to be introduced in clinical settings. Cf. Lorence/Spink/Richards (2002). Furthermore, procedural security or security tools can be circumvented or not be used after all: cf. Moehr/McDaniel (1998); Whitten/Tygar (1998).

[7] Multi-user terminal refers here to typical situations in medical departments where terminals are repeatedly used by a multitude of different professionals almost concurrently or within a short period of time. Personal is frequently roaming and do not have their assigned workstation. Multi-level refers to the legal need of different access rights. E.g., medical orders need to be signed by a certified physician; this process needs to be reproducible when performed electronically. Therefore, the signing professional has to be uniquely authenticated before performing the signing process.

***Research Questions***

(1) How do context factors such as the health care market environment, regulatory requirements, technology, and institutional aspects affect the adoption of administrative and clinical health IS components in hospital organizations?

(2) What is the state of the organizational and technical IS security capability in these organizations? How are IS adoption and IS security capability related? Are any activity patterns and phases identifiable?

(3) What are socio-organizational and technical characteristics that have a detrimental effect on the IS security capability, its practicability, and effectiveness in hospitals? How can it be improved?

This research pursues a qualitative theory-building approach. For this purpose, the case study method has been applied iteratively, creating theory during the research process.[8] The main objective is a better understanding of the phenomenon (IS security) within its context (health IS) and not its statistical occurrence. The prevalence of phenomena cannot be measured well with case studies because it would require an impractical number of cases.[9] Data was collected through interviews, documents, and observation, which were transcribed, coded, and stored in a research database. Analytically, replication logic was applied instead of statistical sampling logic, which is comparable to

[8] “A case study is an empirical inquiry that: investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident.” Yin (2003), p.13. Deduction starts from a given theory and collects empirical data to prove or disprove the theory. Conversely, induction starts without any given theory and concepts emerge during the data collection and analysis processes.

[9] Cf. Eisenhardt (1989), p.545; Orlikowski/Baroudi (1991); Yin (2003), p.48. It is suggested choosing a number between 4 and 10 cases in order to find a trade-off between building a credible empirical foundation and the complexity of the data produced.

an experiment and predicts similar results or contrasting results for predictable reasons.[10] As contribution – derived from theory and findings – a method based on the three-layer graph-based model is suggested to assess IS security compliance of a heterogeneous and decentralized health IS. The concept was implemented using the Java programming language.[11]

## 1.3 Structure

In chapter 2, characteristics and structure of a health IS are presented and decomposed using three distinct perspectives: the domain, logical, and physical layer. IS in hospitals are grouped by functionality as administrative sub-systems and clinical sub-systems and their security-relevant differences are elaborated. In chapter 3, an overview of contemporary IS security research categories is presented. Further, three common control approaches are discussed: management, technical, and regulatory controls. Differences between U.S. and Swiss regulatory specifications are emphasized and their effect on organizations processing personally identifiable information (PII) and personal health information (PHI). In chapter 4, the conceptual framework and the empirical findings are presented. In chapter 5, a graph-based management model is synthesized that improves control of a health IS. In chapter 6, the paper concludes with a summary and outlook.

[10] Cf. Yin (2003), pp.47-49. The theoretical framework needs to state the condition under which the phenomena can be found. Literal replication is the prediction of similar results, whereas theoretical replication describes the process of finding contrasting results.

[11] The software application is based on Java J2SE 1.4 using the Swing GUI API and the Java Universal Network/Graph Framework (JUNG) developed at the University of California, Irvine. Cf. O'Madadhain, et al. (2005).