# Security and Privacy Practices in Healthcare Information Systems: A Cluster Analysis of European Hospitals

Sylvestre Uwizeyemungu[1] and Placide Poba-Nzaou[2]
[1]*Département des Sciences Comptables, UQTR, 3351, boul. des Forges, Trois-Rivières (Québec), Canada*
[2]*Département d'Organisation et Ressources Humaines, ÉSG UQAM, 315, Ste-Catherine Est, Montréal (Qc), Canada*

Keywords: IT Security, Privacy, Confidentiality, Integrity, Availability, Healthcare Information Technology, Electronic Health Records, e-Health.

Abstract: In the past years, increasing efforts have been made toward the implementation of healthcare information technology with the aim of improving patient care and safety, while lowering healthcare systems' costs. However, the transition from a paper-dominant system toward a fully electronically-based system brings with it major challenges in healthcare systems. It particularly exposes healthcare providers and users to more security and privacy risks which come with the digitization of health records. Drawing on data from 1723 European hospitals, we identified, through a cluster analysis, four distinct patterns of health information technology-related security and privacy practices. We found that most European hospitals fail to implement basic security measures consistent with the use of health information technology (HIT). This study contributes to raise awareness on HIT-related security and privacy issues that can negatively affect healthcare users' trust and impede the effective delivery of healthcare services. An appropriate response to the HIT-related security and privacy concerns will increase the acceptability of the digitization of healthcare services.

## 1 INTRODUCTION

In the last three decades or so, a growing number of healthcare organizations has adopted information and communication technologies (ICT) (Mackintosh and Norris, 1985; Williams et al., 1991) and considerable efforts are still directed toward increasing health information technology (HIT) implementation in different countries (Adler-Milstein et al., 2014). The increasing interest in HIT is motivated by either technological, administrative, clinical, or financial reasons (Poba-Nzaou et al., 2014). Healthcare services delivery is being reformed - and some say revolutionized - through information technology (IT) (Agrawal et al., 2007): IT potential contributes to a substantial reduction in medical errors, and improvements in patient care and safety, while contributing to lower healthcare systems' costs.

HIT offers the opportunity for health information to be portable. As a result, this information becomes readily shareable within and between healthcare units and more accessible to patients. Turning health information into bits is convenient in multiple ways, but it makes health records more vulnerable to security and privacy breaches that plague other digital media (Tejero and de la Torre, 2012). Thus, security and privacy concerns may reduce HIT potential users' trust, leading to lower levels of usage which ultimately translate into ineffective healthcare delivery (Bahtiyar and Çaglayan, 2014).

As well, although multiple HIT contain detailed clinical data from large populations of patients that are readily exploitable for public health surveillance purposes, healthcare providers do not fully share this data due to proprietary, security, and privacy concerns (Vogel et al., 2014).

According to a 2014 survey by Information Security Media Group (ISMG), at least one security breach that affects fewer than 500 individuals has occurred in 75% of surveyed healthcare organizations; at least one incident affecting more than 500 individuals has been reported by 21% of surveyed healthcare providers (ISMG, 2014, p. 6). In the 2015 survey by the Healthcare Information and Management Systems Society (HIMSS), two-thirds (68%) of surveyed healthcare organizations reported to have recently experienced a significant security incident (HIMSS, 2015, p. 15). Reported security incidents came both from external threats (63.6% of healthcare organizations) and insider threats (53.7%) (Ibid, p. 16).

Uwizeyemungu, S. and Poba-Nzaou, P.
Security and Privacy Practices in Healthcare Information Systems: A Cluster Analysis of European Hospitals.
DOI: 10.5220/0005654800370045
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 37-45
ISBN: 978-989-758-167-0

These consistent statistics of security breaches in healthcare settings are disturbing, and even more so when one considers the fact that many security incidents remain undetected or are not properly assessed (ISMG, 2014, p. 11).

Documented incidents show how security breaches in healthcare settings can be expensive. Absolute Software Corporation reports examples of healthcare data breach incidents that costed involved hospitals from US$ 250,000 to US$ 2,5 million in settlement payments; which are but a fraction of the overall cost of the incidents (Absolute Software Corporation, 2015).

Security concerns may prevent healthcare providers from leveraging IT for improving their services. Increasing health IT security and privacy practices in hospitals is then an important step forward for effective healthcare delivery. In this study, we analyze security and privacy measures within European hospitals. We seek to answer the following two questions:

1). What is the state of IT security and privacy practices implementation in European hospitals?

2). Are IT security and privacy practices enhanced as European hospitals move towards fully electronically-based healthcare systems?

Drawing on secondary data from the European Commission 2013 eHealth survey (Joint Research Centre, Institute for Prospective Technological Studies), we derived four clearly distinct clusters of 1723 European hospitals based on their IT security and privacy practices. The results of this study further confirm the alarming conclusions of previous studies that report important weaknesses with regard to IT security and privacy practices in hospitals (Tejero and de la Torre, 2012).

In this study, we also investigated whether the evolution towards electronically-based health information systems is accompanied by required IT security and privacy practices implementation. Indeed, as HIT allows the transition from paper-based health records toward fully electronically-based records, healthcare organizations need to implement security and privacy measures consistent with the level of digital risks. We developed an IT security index for each hospital and we compared it with the self-reported transition level from a paper-based system toward a fully electronic-based system. Our results indicate that the transition of healthcare systems in European hospitals is not sufficiently consistent with the evolution of their IT security and privacy practices. Highlighting health IT security weaknesses, this study contributes to raise awareness among hospitals' managers as to the importance of enhancing their IT security measures so that they can keep up with the security threats inherent in a digital world.

# 2 BACKGROUND

## 2.1 Health Information Technology

The notion of health information technology (HIT) encompasses a wide range of technologies related either to health information gathering, consultation, processing, and sharing, or to healthcare systems management. Currently, they are generally referred to as electronic health record (EHR), a broad term that, according to the Institute of Medicine, encompasses eight core functions related to healthcare delivery and healthcare systems management (Fetter, 2009): health information and data, result management, order management, decision support, electronic communication and connectivity, patient support, administrative processes and reporting, reporting and population health.

Trying to benchmark health IT among OECD countries, Adler-Milstein et al., (2014) underscored the difficulty in comparing countries' systems due to terminology meaning variations across countries: for instance, while in many OECD countries the concept of electronic medical record (EMR) is used interchangeably with electronic health record (EHR), the two terms refer to two different systems in Canada. To overcome this difficulty, the authors have developed a functionality-based approach, and grouped health IT functionalities into four broad categories: provider-centric electronic record, patient-centric electronic record, health information exchange, and tele-health.

In this study we simply use the term "Health Information Technology" or HIT to refer to all IT systems used for storing, sharing, transmitting health information, or for supporting healthcare delivery.

## 2.2 Security and Privacy Issues

Electronic health records (EHR) compile a wide range of highly sensitive information including not only current data related to tests, diagnoses, and treatments, but also past medical history (Häyrinen et al., 2008). In order to obtain the full potential from an EHR, the highly sensitive information it contains need to be readily accessible to healthcare professionals as well as to patients(Tejero and de la Torre, 2012) at any moment and everywhere it is needed.

The ubiquitous access to health data is possible through an open environment like Internet (Bahtiyar and Çaglayan, 2014). Internet also allows for the connection of various health systems from different healthcare providers. While electronic-based systems are undoubtedly convenient for healthcare providers as well as for patients, they raise security and privacy concerns. Thus, healthcare providers that adopt health IT need to put in place an adequate security system. This system is "a set of security mechanisms that are implemented according to a security policy"; which is "a collection of rules that allow or disallow possible actions, events, or something related to security" (Bahtiyar and Çaglayan, 2014, p. 164).

Generally speaking, an IT security policy aims at ensuring that an organization's IT assets (hardware, software, data, people) respond constantly to required levels of confidentiality, integrity and availability (von Solms, 2005). These three basic IT security requirements are generally referred to as the CIA triad (Confidentiality, Integrity, and Availability).

Confidentiality requires that only duly authorized people can get access to data, whether it is stored, being transmitted or being treated. This can be achieved through encryption of data, or through controlled access to the systems. With regard to encryption, the 2014 survey of the Information Security Media Group (ISMG) showed that while encryption is commonly applied for health data transmitted across exposed networks, it is less applied to data stored in mobile devices and other storage media (ISMG, 2014, p. 23). The confidentiality requirement responds to privacy concerns that are of paramount importance in healthcare systems given the sensitivity of information they contain.

With the integrity criterion it is expected "that information is protected against unauthorized modification or deletion as well as irrevocable, accidental, and undesired changes by authorized users" (Dehling and Sunyaev, 2014, p. 92).

As for availability, it requires that a system be accessible and fully operational whenever an authorized user needs to use it. The availability criterion refers to multiple aspects ranging from scalability (adaptability to changing performance needs), to resilience (resistance to software or hardware failures), and to recoverability of data in case of loss for whatever reason (Dehling and Sunyaev, 2014).

# 3 METHODS

## 3.1 Data Source

We used data from the European Commission 2013 eHealth survey (Joint Research Centre, Institute for Prospective Technological Studies). The objective of the survey was "to benchmark the level of eHealth use in acute care hospitals in all 27 European Union Member States, Croatia, Iceland, and Norway" (European Commission, 2014, p. 10).

## 3.2 Sample

Of 1753 initial observations, only 30 (1.7%) were dropped because of missing data ('don't know' response or no answer at all) on key variables, which led us to a final sample of 1723 European hospitals.

We present in Table 1 the characteristics of surveyed hospitals. They are mostly public institutions (70.4%), and only few of them are university hospitals (13.7%). They are mainly independent organizations (72.7%) operating on one site (41.3%) or on multiple sites (31.4%). Smaller hospitals (100 or fewer beds) represent 23.5% of our sample, while large hospitals (more than 750 beds) account for 10.5%. With regard to the IT-enabled transition from a paper-based system to a fully electronically-based system, the majority of surveyed hospitals (61.0%) are in an intermediate phase combining in roughly equal proportions both systems. However, it is worth noting that the portion of hospitals that operate an electronic-dominant system (26.1%) is larger than the portion of hospitals with a paper-dominant system (12.9%). As for IT budget, it represents 3% or less of the total hospital budget for 86.3% of surveyed institutions. Only 4.1% of hospitals devote over 5% of their total budget to IT-related activities. 59.7% of surveyed hospitals report relying on national level regulations for their security practices, 28.3% rely on the regional level, and 69.4% have in place an in-house designed regulation.

## 3.3 Measurement

Three types of measurement were used to collect data on different variables used in this study: dichotomous scale measurements, ordinal/interval scale measurements, and multiple choice questions.

The clustering variables, namely HIT security practices (confidentiality, integrity, and availability), were measured through a dichotomous scale (e.g. 1 if a confidentiality-related practice is implemented, and

0 when it is not implemented). We present in Table 2 the questions used to capture HIT security practices. Dichotomous scales, ordinal or interval scales as well as multiple choice questions were used for contextual variables. The column "characteristic" of Table 1 shows these scales or choices.

Table 1: Characteristics of Surveyed Hospitals.

| Variable | Characteristic | % of the sample |
|---|---|---|
| **Status** | Public | 70.4% |
| | Private | 19.8% |
| | Non for Profit | 9.8% |
| **University Hospital** | Yes | 13.7% |
| | No | 86.3% |
| **Single/ Multiple sites** | Independent/One site | 41.3% |
| | Independent/Multiple sites | 31.4% |
| | Part of a group of hospitals | 19.7% |
| | Part of a group of care institutions | 4.6% |
| | Other | 3.0% |
| **Size (Number of beds)** | Fewer than 101 beds | 23.5% |
| | Between 101 and 250 beds | 31.5% |
| | Between 251 and 750 beds | 34.5% |
| | More than 750 beds | 10.5% |
| **Paper or electronic-based system** | Paper-dominant system | 12.9% |
| | Hybrid Model | 61.0% |
| | Electronic-dominant system | 26.1% |
| **IT Budget (% of Total Hospital Budget)** | Less than 1% | 38.8% |
| | Between 1% and 3% | 47.5% |
| | Between 3.1% and 5% | 9.7% |
| | More than 5% | 4.1% |
| **Security regulation** | National level | 59.7% |
| | Regional level | 28.3% |
| | Hospital level | 69.4% |

Table 2: Security and Privacy Practices Measures.

| Variable | Measure (Yes /No) |
|---|---|
| **1. Confidentiality:** Which of the following security measures are taken to protect the patient data stored and transmitted by the hospital's IT system? | |
| 1.1. Stored Data | Encryption of stored data |
| 1.2. Transmitted Data | Encryption of transmitted data |
| 1.3. Access Control | Workstations with access only through health professional cards or code |
| **2. Integrity** | Is data entry in the hospital's IT system certified with digital signature? |
| **3. Availability** | Are your IT team able to immediately restore critical clinical information system operations if a disaster causes the complete loss of data at your hospital's primary data center? |

## 3.4 Cluster Analysis

For cluster analysis we performed the SPSS agglomerative hierarchical clustering procedure using Ward's minimum variance criterion combined with the squared Euclidian distance. The aim of this procedure was to distribute the sampled hospitals in a number of subgroups (clusters) such as hospitals that fall in the same subgroup are highly homogeneous among themselves while being significantly dissimilar to hospitals in the other subgroups with regard to implemented HIT security practices. In other words, the subgroups or clusters are formed in a way that maximizes both intra-group similarity and inter-group dissimilarity (Jung et al., 2003).

To identify the optimal number of clusters, we first examined the Euclidian distances across the clusters in the dendrogram produced with the clustering procedure. We identified two apparently equally plausible solutions, a 3-cluster, and a 4-cluster solutions. To decide which of these two solutions would be better, we followed Ketchen and Shook's (1996) recommendation: we ascertained the robustness of both by replicating the clustering algorithm on subsamples of about 80%, 60%, and 40% of observations randomly selected using SPSS's random selection functionality. The analysis of the dendrograms produced with all these subsamples indicated that the 4-cluster solution was the most stable, and were then chosen over the 3-cluster solution.

As an additional measure, once the observations were classified into the three clusters, we performed a discriminant analysis to test the validity of the clusters. This test "runs the data back through the minimum-variance method as a discriminant function to see how accurately hospitals are classified" (Kwon and Johnson, 2013, p. 46). The results of this test indicated a perfect classification accuracy (100%) for clusters 1, 2, and 4, and a high level of classification accuracy (84.8%) for cluster 3. Overall, 97.9% of original observations were correctly classified.

# 4 RESULTS AND DISCUSSION

## 4.1 Results of Cluster Analysis

We derived from data on 1723 European hospitals four clearly distinct clusters of hospitals based on IT security and privacy practices implemented. We present the four security patterns resulting from the cluster analysis in Table 3.

Before analyzing cluster differences, it is worth noting the grand mean of HIT security and privacy practices in sampled hospitals. As our security and privacy variables are measured through a dichotomous scale (1 if a practice is implemented, and 0 if not implemented), the grand mean corresponds to the rate of hospitals that have a given practice implemented. This rate is presented in brackets in the column "variable" of Table 3. The most implemented practice is the one intended to ensure the confidentiality of electronically-transmitted data (present in 59% of hospitals), closely followed by the practice aiming at guaranteeing the availability of health data in case of a disaster (57%). The less implemented security practice is the access control or IT workstations that contain sensitive health information (18%).

Based on Tamhane's post hoc test, we can immediately see that the "availability" criteria does not allow for the discrimination between the four clusters: hospitals that have implemented security measures allowing them to immediately recover their electronic health records after a disaster are found in almost the same proportions in the four clusters (54% to 59%). However, there are differences between the four clusters with regard to confidentiality and integrity related practices.

Cluster 1 regroups 30.9% of surveyed hospitals. All hospitals in this cluster (100%) ensure the confidentiality of electronically-transmitted health data through encryption. Less than half of them (47%) encrypt data stored in their health information systems. None of them (0%) reports to have implemented an access control to workstations containing health information through personalized cards or codes. All hospitals in cluster 1 fail with regard to the protection of data integrity.

Table 3: HIT Security and Privacy Patterns Resulting from Cluster Analysis.

| **Variable (Grand Mean)** | **Cluster Number (n) (%)** | | | | **Anova** |
|---|---|---|---|---|---|
| | **1<br>(533)<br>(30.9)<br>Mean** | **2<br>(269)<br>(15.6)<br>Mean** | **3<br>(244)<br>(14.2)<br>Mean** | **4<br>(677)<br>(39.3)<br>Mean** | **F** |
| **Confidentiality** | | | | | |
| -Stored Data (0.37) | $0.47_a$ | $0.56_a$ | $0.50_a$ | $0.18_b$ | 71.7* |
| -Transmitted Data (0.59) | $1.00_a$ | $1.00_a$ | $0.85_b$ | $0.00_c$ | 7059.7* |
| -Access Control (0.18) | $0.00_c$ | $0.00_c$ | $1.00_a$ | $0.10_b$ | 1846.1* |
| **Integrity** (0.31) | $0.00_d$ | $1.00_a$ | $0.54_b$ | $0.20_c$ | 686.0* |
| **Availability** (0.57) | 0.59 | 0.59 | 0.56 | 0.54 | 1.3 |

*: p<0.001 (two-tailed test)
a,b,c,d: Within rows, different subscripts indicate significant (p<0.05) pair-wise differences between means on Tamhane's T2 (post-hoc) test.

Cluster 2 accounts for 15.6% of our sample. With regard to security and privacy practices, hospitals in this cluster present the same patterns as hospitals in cluster 1 in all aspects but one: while none of hospitals in cluster 1 digitally protects data entry in health IT system (data integrity), all hospitals in cluster 2 do. Although none of the hospitals in cluster 2 has implemented the access control measure, adoption levels of other security measures put this cluster in a good position when compared to other clusters.

Hospitals in cluster 3 represent 14.2% of our sample. The implementation rate of each of the four distinctive HIT-related security and privacy practices is higher in this cluster than the average rate for all hospitals in our sample.

Cluster 4 is the largest subgroup (39.3%), and overall, it is the weakest with regard to IT security and privacy practices adopted. None of the 677 hospitals in this group use encryption to protect electronically-transmitted health records, and only 10% of them enforce an access control to health IT systems.

In Figure 1, we alternatively present the results shown in Table 3. Figure 1 shows cluster by cluster the percentages of hospitals in our sample that have implemented IT security and privacy practices. It can be noted that clusters 2 and 3 display the higher levels of IT security implementation. However, cluster 3 appears to be more balanced than cluster 2. Clusters 1 and 4 are the weakest as far as IT security practices implementation are concerned.

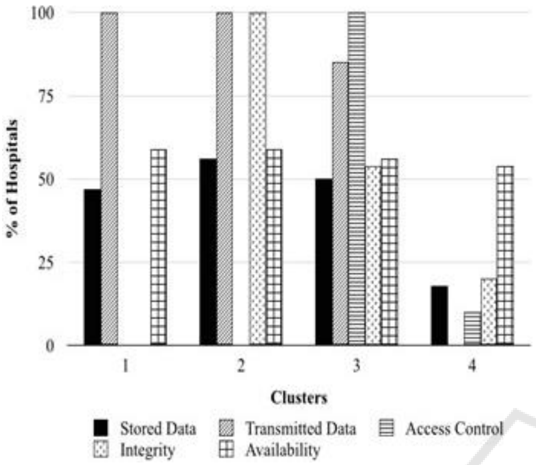

Figure 1: IT Security and Privacy Practices Implemented in Hospitals by Cluster.

## 4.2 Influence of Context Variables

Trying to understand what leads a given hospital to implement or not security and privacy measures, we analyzed the contextual variables. The aim here was to analyze the influence of variables “theoretically related to the clusters, but not used in defining clusters” (Ketchen and Shook, 1996, p. 447). In the appendix we present a breakdown of context variables by cluster.

When comparing distribution percentages of hospitals by characteristic (e.g. public versus private status) in different clusters with corresponding distribution percentages in the whole sample, one can see which type of hospitals are over or under-represented in a given cluster. For most of the contextual variables, the expected distributions did not significantly depart from the observed distributions. This is surprising, as we expected some contextual variables to significantly influence the IT security practices adoption. For example, we expected these practices to be more prevalent in larger hospitals, in hospitals operating on multiple sites or those that are part of a group of hospitals, and in hospitals with electronic-dominant systems. Accordingly, one would expect to find an overwhelming over-representation of these hospitals in clusters 2 and 3, the best clusters with regard to IT security implementation. Although multiple site hospitals are somehow over-represented in clusters 2 and 3 as it can be noted from the appendix, they are also well represented in the worst clusters, namely clusters 1 and 4.

Here it is worth noting that in clusters 2 and 3, there is an over-representation of hospitals that report relying on national level and regional level regulations to ensure the security and privacy of their electronic patient medical data.

Among the contextual variables, we would particularly like to analyze the relationship between the level of transition from a paper-based system to a fully electronically-based system and the implementation of IT security and privacy measures.

## 4.3 Transition Toward an Electronically-based System and IT Security Practices

As more and more hospitals move from a paper-dominant system toward an electronic-dominant system, healthcare providers will be able to electronically exchange health records. In this context, security should not be an afterthought “supported for individual systems for specific providers, but overlooked when one attempts to bring together patient data from multiple electronic sources” (Demurjian et al., 2014, p. 2-3).

As earlier stated, the digitalization of health records exposes health data to IT-related security breaches. Hospitals need to deploy IT security and privacy measures as they move forward in transition from a fully paper-based system to a fully electronically-based system.

In our study, the level attained by a hospital in the transition from a paper-based system to a fully electronically-based system was measured by asking respondents to select the position of their hospital on a 9 points Likert-scale from 1 (totally paper-based) to 9 (totally electronically-based), with point 5 as a hybrid model. The statistics on paper-based or electronic-based system reported in Table 1 were compiled as follows: hospitals that chose positions from 1 to 3 were qualified as having a paper-dominant system; a hybrid system label was given to hospitals that choose positions from 4 to 6; and the remaining hospitals (positions from 7 to 9) were deemed to have an electronic-dominant system.

In order to ascertain whether or not hospitals adopt more IT security and privacy measures consistent with their level in the transition towards a fully-electronically-based system, we developed a security index that we later compared with the self-reported transition level. The security index was developed based on the presence or absence of each of the five IT security and privacy practices used as clustering variables. Each of the three components of security practices (confidentiality, integrity, and availability) accounts for 1 if implemented, and for 0 if not implemented. As our measure of confidentiality is based on three practices, each confidentiality-related practice accounts for one third point. As for integrity and availability, they are measured through a unique practice each, and in each case, when the practice is implemented it accounts for 1, and it accounts for 0 if not implemented. Thus, our security index ranges from 0 (for a hospital with none of the practices implemented) to 3 (for a hospital that has all the 5 practices implemented: 1/3+1/3+1/3+1+1).

In Figure 2 we plotted each hospital's security index (vertical axis) against its level in transition towards a fully electronically-based system (horizontal axis). For facilitating the analysis of the figure, we added a diagonal line. If hospitals were enhancing their IT security and privacy practices as they move forward, points representing hospitals would be scattered around the diagonal line. Rather, we found that points are scattered almost all over the surface of our figure.

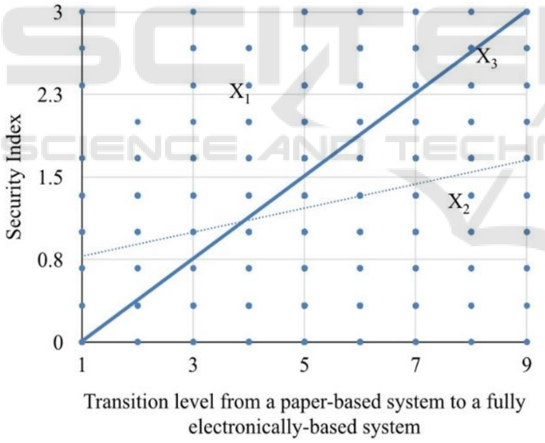

Figure 2: IT Security Index and Transition toward an Electronically-Based System.

Hospitals far above (far below) the diagonal line display a security index that is superior (inferior) to the average level required by their transition level towards a fully electronically-based system. For example, any hospital represented by $X_1$ point has an IT-related security index above the theoretical level required by its progress toward an electronic-dominant system. Conversely, a hospital represented by $X_2$ displays a security index far below the level it should attain considering how far it has progressed toward a fully electronically-based system. The security index of hospital $X_3$ is consistent with its progress in electronic-based system implementation.

The slope of the ascending curve in the figure suggests that there is a trend toward increasing IT security measures when hospitals move from a paper-based system to an electronic-based system. Though this finding is positive, it appears that this trend is not strong enough. Otherwise, the shape of the curve would be closer to the diagonal line.

## 5 IMPLICATIONS AND CONCLUSION

This study highlights a disturbing state in European hospitals with regard to health IT security and privacy practices implemented.

Overall, none of the five basic security and privacy practices investigated in this study is present in more than 60% of surveyed hospitals. Three out of five practices are absent in more than two thirds of surveyed hospitals. These statistics are preoccupying since security and privacy practices studied here are basic practices that should be implemented in almost all hospitals. Encryption for stored data is used in only 37% of hospitals. It is used for transmitted data in only 59% of hospitals. Many hospitals (more than 80%) do not deem it necessary to control the access to workstations containing health data through health professionals cards or codes. There is as few as 18% of hospitals that have implemented this practice. Hospitals in which all these measures are not implemented expose health information to confidentiality breaches.

In this study, the practices related to integrity and availability are measured respectively at 31% and 57% implementation rates in hospitals. These implementation rates are low for systems containing highly sensitive information. They mean that 1) in almost 70% hospitals, health data in IT systems can be modified by non-authorized persons provided they have access to the systems; 2) more than 40% of surveyed European hospitals would not be able to restore critical clinical information in the aftermath of a disaster resulting into a complete loss of data.

There is another way of looking at our results. Our cluster analysis allowed us to identify four patterns of health IT security and privacy practices. The majority of surveyed hospitals fall into the two worst clusters (clusters 1 and 4): these two clusters total 1210 hospitals out of 1723 (70.2%). This means that 7 out of 10 European hospitals are performing poorly in ensuring the security and privacy of their electronic health records.

We expected that hospitals that are well advanced in their transition toward a fully electronic health system would display higher levels of implementation of IT security and privacy practices. Confronting each hospital's security index (a compounded measure of implemented security practices) to its self-rated level of transition toward a fully electronic health system, we have shown our expectation was far from being true. This is a great concern.

Although we had access to an interesting dataset from the European Union, we were limited to the questions asked in the survey. This is the problem of using secondary data. We also acknowledge some limits stemming from our definition of security and privacy practices. One could enlarge this definition or completely choose other security practices. For the transition level toward a fully electronically-based system, we relied on a self-reported level given by each hospital's IT manager in absence of a more objective measure. This can be somehow biased.

Our study contributes to the understanding of IT security practices in healthcare organizations, despite the above mentioned limits. It also contributes to raise awareness on the security and privacy issues that can impede the effective delivery of healthcare services.

## REFERENCES

Absolute Software Corporation. (2015). *The Cost of a Data Breach: Healthcare Settlements Involving Lost or Stolen Devices.* Austin, Texas: Absolute Software Corporation.

Adler-Milstein, J., Ronchi, E., Cohen, G. R., Winn, L. A. P., & Jha, A. K. (2014). Benchmarking Health IT among OECD Countries: Better Data for Better Policy. *Journal of the American Medical Informatics Association, 21*(1), 111-116.

Agrawal, R., Grandison, T., Johnson, C., & Kiernan, J. (2007). Enabling the 21st Century Health Care Information Technology Revolution. *Communications of the ACM, 50*(2), 34-42. doi: http://dx.doi.org/10.1145/1216016.1216018

Bahtiyar, S., & Çaglayan, M. U. (2014). Trust Assessment of Security for e-Health Systems. *Electronic Commerce Research and Applications, 13*(3), 164-177. doi: http://dx.doi.org/10.1016/j.elerap.2013.10.00

Dehling, T., & Sunyaev, A. (2014). Secure Provision of Patient-Centered Health Information Technology Services in Public Networks - Leveraging Security and Privacy Features Provided by the German Nationwide Health Information Technology Infrastructure. *Electronic Markets, 24*(2), 89-99. doi: http://dx.doi.org/10.1007/s12525-013-0150-6

Demurjian, S., Algarín, A., Bi, J., Berhe, S., Agresta, T., Wang, X., & Blechner, M. (2014). A Viewpoint of Security for Digital Health Care in the United States: What's There? What Works? What's Needed? *International Journal of Privacy and Health Information Management, 2(1)*, 1-21.

European Commission. (2014). European Hospital Survey: Benchmarking Deployment of eHealth Services (2012-2013): *JRC Scientific and Policy Reports*.

Fetter, M. S. (2009). The Electronic Health Record. *Issues in Mental Health Nursing, 30*(5), 345-347.

Häyrinen, K., Saranto, K., & Nykänen, P. (2008). Definition, Structure, Content, Use and Impacts of Electronic Health Records: A Review of the Research Literature. *International Journal of Medical Informatics, 77*(5), 291-304.

HIMSS. (2015). 2015 HIMSS Cybersecurity Survey. Chicago, IL: HIMSS.

ISMG. (2014). Healthcare Information Security Today. 2014 Survey Analysis: Update on HIPAA Omnibus Compliance, Protecting Patient Data (pp. 38). Retrieved from http://6dbf9d0f8046b8d5551a-7164cafcaac68bfd3318486ab257f999.r57.cf1.rackcdn.com/2014-healthcare-information-security-today-survey-pdf-5-h-53.pdf

Jung, Y., Park, H., Du, D.-Z., & Drake, B. L. (2003). A Decision Criterion for the Optimal Number of Clusters in Hierarchical Clustering. *Journal of Global Optimization, 25*(1), 91-111.

Ketchen, D. J., & Shook, C. (1996). The Application of Cluster Analysis in Strategic Management Research: An Analysis and Critique. *Strategic Management Journal, 17*(6), 441-458.

Kwon, J., & Johnson, M. E. (2013). Security Practices and Regulatory Compliance in the Healthcare Industry. *Journal of the American Medical Informatics Association, 20*(1), 44-51.

Mackintosh, I. P., & Norris, D. E. (1985). Expanding Role of Information Technology in UK Hospitals. *Information Age, 7*(3), 133-138.

Poba-Nzaou, P., Uwizeyemungu, S., Raymond, L., & Paré, G. (2014). Motivations Underlying the Adoption of ERP Systems in Healthcare Organizations: Insights from Online Stories. *Information Systems Frontiers, 16*(4), 591-605.

Tejero, A., & de la Torre, I. (2012). Advances and Current State of the Security and Privacy in Electronic Health Records: Survey from a Social Perspective. *Journal of Medical Systems, 36*(5), 3019-3027. doi: 10.1007/s10916-011-9779-x

Vogel, J., Brown, J. S., Land, T., Platt, R., & Klompas, M. (2014). MDPHnet: Secure, Distributed Sharing of Electronic Health Record Data for Public Health Surveillance, Evaluation, and Planning. *American Journal of Public Health, 104*(12), 2265-2270.

von Solms, S. H. (2005). Information Security Governance: Compliance Management vs Operational Management. *Computers & Security, 24*(6), 443-447.

Williams, F. G., Netting, F. E., & Engstrom, K. M. (1991). Implementing Computer Information Systems for Hospital-Based Case Management. *Hospital & Health Services Administration, 36*(4), 559-570.

# APPENDIX

Breakdown of Context Variables by Cluster

| **Variable** | **Characteristic** | ***% of the Overall sample*** | **% in Clusters** | | | |
|---|---|---|---|---|---|---|
| | | | **Cluster 1** | **Cluster 2** | **Cluster 3** | **Cluster 4** |
| **Status** | Public | *70.4* | 67.2 | 69.5 | 72.4 | 68.8 |
| | Private | *19.8* | 20.8 | 22.5 | 18.4 | 22.6 |
| | Non for Profit | *9.8* | 11.9 | 8.0 | 9.2 | 8.5 |
| **University Hospital** | Yes | *13.7* | 12.8 | 13.4 | **19.7** | 13.8 |
| | No | *86.3* | 87.2 | 86.6 | **80.3** | 86.2 |
| **Single/ Multiple sites** | Independent/One site | *41.3* | 40.0 | 41.2 | 35.5 | **49.7** |
| | Independent/Multiple sites | *31.4* | 33.9 | **39.0** | **35.5** | 28.4 |
| | Part of a group of hospitals | *19.7* | 21.4 | 16.0 | 21.1 | **13.6** |
| | Part of a group of care institutions | *4.6* | 1.9 | 3.2 | 5.9 | 4.5 |
| | Other | *3.0* | 2.8 | 0.5 | 2.0 | 3.8 |
| **Size (Number of beds)** | Fewer than 101 beds | *23.5* | 23.9 | **16.6** | 26.3 | 26.6 |
| | Between 101 and 250 beds | *31.5* | 28.6 | 34.8 | 29.6 | 28.9 |
| | Between 251 and 750 beds | *34.5* | 36.7 | 35.8 | 31.6 | 32.7 |
| | More than 750 beds | *10.5* | 10.8 | 12.8 | 12.5 | 11.8 |
| **Paper or electronic-based system** | Paper-dominant system | *12.9* | 13.6 | **7.5** | 11.9 | 16.3 |
| | Hybrid Model | *61.0* | 58.3 | 63.1 | 55.9 | 62.3 |
| | Electronic-dominant system | *26.1* | **28.1** | **29.4** | 22.4 | 21.4 |
| **IT Budget (% of Total Hospital Budget)** | Less than 1% | *38.8* | 37.2 | 32.1 | 33.6 | **44.5** |
| | Between 1% and 3% | *47.5* | 47.8 | **55.1** | **52.0** | 43.0 |
| | Between 3.1% and 5% | *9.7* | 10.8 | 10.2 | 8.6 | 8.0 |
| | More than 5% | *4.1* | 4.2 | 2.7 | 5.9 | 4.5 |
| **Security regulation** | National level | *59.7* | 60.8 | **69.0** | **73.7** | 52.5 |
| | Regional level | *28.3* | 31.1 | **40.1** | **33.6** | **17.1** |
| | Hospital level | *69.4* | **79.7** | **77.0** | 68.4 | 61.6 |