# Health Information Exchange and Related IT-security Practices in European Hospitals

Sylvestre Uwizeyemungu[1] and Placide Poba-Nzaou[2]
[1]*Département des Sciences Comptables, Université du Québec à Trois-Rivières (UQTR), 3351, Boul. des Forges, C.P. 500, Trois-Rivières (Québec), Canada*
[2]*Département d'Organisation et Ressources Humaines, ÉSG – Université du Québec à Montréal (UQAM), 315, Ste-Catherine Est, Montréal (Québec), Canada*
*sylvestre.uwizeyemungu@uqtr.ca, poba-nzaou.placide@uqam.ca*

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

Abstract: Alongside other health information technologies (HIT), several projects aimed at implementing electronic health information exchange (HIE) have been initiated in European countries, with the hope of improving the coordination, safety, and efficiency in healthcare systems. However, the electronic exchange exposes health data to information technology (IT)-related vulnerabilities and threats, raising concerns among patients, health care providers, and policy-makers. Drawing on data from a sample of 1123 European hospitals, we conducted a cluster analysis to determine to what extent hospitals do live up to the IT security and privacy challenges of electronic HIE. We produced two sets of clusters, one related to HIE usage and another related to the implementation of IT-security practices. Through a cross-comparison, we proceeded to a match/mis-match analysis. The results of this study depict a mixed situation: even though most of surveyed hospitals (79.2%) have implemented IT-security practices consistent with their HIE usage levels, hospitals that have failed to do so (20.8%) pose a threat to the entire healthcare system which is becoming more and more interconnected.



## 1 INTRODUCTION

Developed countries have undertaken the reform of their healthcare systems in the quest to achieve what has been called the "triple aim", that is (1) improving individual care experience, (2) improving population health, and (3) reducing per-capita cost of healthcare (Berwick et al., 2008). The adoption of health information technologies (HIT) is at the heart of the healthcare reform.

The use of Health IT is now widely accepted as a cornerstone of modern healthcare delivery, and the question has shifted from whether IT should be used in health care to which models of care delivery should HIT support (Bitton et al., 2012). It then makes sense to analyze the challenges that would impede the unleashing of the full potential of IT in healthcare settings in order to alleviate their effects. Among these challenges, security and privacy concerns are of utmost importance for at least three reasons.

First, health IT systems in general, and electronic health records (EHR) in particular 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). Concerns of patients as well as health professionals with regard to ensuring security and privacy of highly-sensitive records might fuel their resistance to trust and embrace HIT (Ancker et al., 2012; O'Donnell et al., 2011; Vogel et al., 2014).

Second, by turning health information into bits, a HIT increases health records' portability, which is convenient in multiple ways, but in so doing, it increases their vulnerability to security and privacy breaches that are paramount in other digital media (Tejero et al., 2012).

Third, in order to obtain the full potential from any HIT, the highly sensitive information it contains has to be readily accessible to healthcare professionals as well as to patients (Tejero et al., 2012) at any moment and everywhere it is justifiably needed. Therefore, an effective HIT goes hand in hand with electronic health information exchange (HIE). However, security and privacy concerns stem from the fact that an electronic HIE multiplies parties that have access to health information and increases patients' feeling



Uwizeyemungu, S. and Poba-Nzaou, P.
Health Information Exchange and Related IT-security Practices in European Hospitals.
DOI: 10.5220/0006263305380545
In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, pages 538-545
ISBN: 978-989-758-209-7

of limited control over health care providers' use of that information (O'Donnell et al., 2011). In a survey of patients (Ancker et al., 2012), 68% respondents expressed privacy and security concerns. These concerns are especially about who will have access to the health information including the risks of unauthorized access and the nature of sensitive information that would be shared (Simon et al., 2009).

In this study, we measure the implementation levels of electronic HIE against the IT-security related practices in European hospitals. Our main research question is: are European hospitals living up to the IT security and privacy challenges of electronic Health Information Exchange?

Drawing on data collected by the European Commission through 2013 eHealth survey (European Commission, 2014), we first proceeded to a cluster analysis of European hospitals with regards 1) to their HIE usage levels and 2) to their IT-security practices implementation levels. We then compared the two sets of clusters. Secondly, after developing an electronic HIE implementation Index (referred to as « HIE Index » from now on) as well as an IT-security index for each surveyed hospital, we compared each hospital's HIE Index to its IT-security Index to assess whether the implementation of electronic HIE is accompanied by the enforcement of required IT-security and privacy practices.

Our results depict a mixed situation: even though most of surveyed hospitals (79.2%) have implemented IT-security practices consistent with their HIE usage levels, hospitals that have failed to do so (20.8%) pose a threat to the entire healthcare system which is becoming more and more interconnected. In addition, a fine analysis of our results shows a more complex situation that led us to call for more IT-security practices implementation in hospitals given the sensitive nature of health information. Indeed, over 60% hospitals that are well advanced in using health information exchange do not adopt IT-security practices that are consistent with the associated IT-security risks.

# 2 BACKGROUND

## 2.1 IT Security Concerns About HIE

Various stakeholders in healthcare systems have concerns over the security and privacy of health information stored in, or transmitted across, different health IT systems. Patients have concerns related to the risk of their sensitive health information falling into unauthorized hands or being exploited by third parties without their informed consent (Hwang et al., 2012). Healthcare providers, health IT suppliers, as well as health policy-makers are preoccupied by the adverse effects of IT security and privacy breaches. Healthcare providers may loose patients' trust and confidence that are necessary for the laters' willingness to consent to the usage of their information in HIE. Consequently, HIE would not meet the "meaningful use" requirement, a failing that will undermine the efficiency and effectiveness of healthcare delivery and public health surveillance. Healthcare providers are also preoccupied by healthcare professional responsibilities and liabilities (Zwaanswijk et al., 2013). Reports from the USA (Absolute Software Corporation, 2015) mention data breaches that cost hospitals up to US$ 2.5 million in settlement payments.

Concerns of patients, healthcare providers, and policy-makers over health information exposure to IT security and privacy breaches are justified if one considers the results of recent surveys in healthcare organizations (HIMSS, 2015; ISMG, 2014; Ponemon Institute, 2016). In the 2014 survey of Information Security Media Group (ISMG), three quarters (75%) of surveyed healthcare providers reported to have experienced at least one IT security related breach affecting under 500 individuals; and 21% reported at least one security incident affecting over 500 individuals (ISMG, 2014, p. 6). A Healthcare Information and Management Systems Society (HIMSS) survey conducted in 2015 found that at least one major security incident recently occurred in 68% of respondent healthcare organizations (HIMSS, 2015, p. 15). In a survey by Ponemon Institute (Ponemon Institute, 2016, p. 19), 89% of surveyed healthcare organizations reported to have suffered a data breach leading to the loss or theft of patient data during the 24 months preceding the survey.

## 2.2 IT Security Reference for HIE

Considering HIE-related concerns over data breaches, the implementation of HIE should be accompanied with an appropriate IT security policy, which is "a collection of rules that allow or disallow possible actions, events, or something related to security" (Bahtiyar et al., 2014, p. 164).

IT-security requirements are generally determined with reference to the so-called CIA triad: confidentiality, integrity, and availability (Dehling et al., 2014; von Solms, 2005). The confidentiality requirement is met if only people with valid authorization can have access to data obtained from, or transmitted through HIE. This can be achieved

through encryption of data in storage or being transmitted, as well as through access control of workstations.

The integrity requirement aims at guaranteeing specific and authorized ways health data can be modified (White, 2004). It is meant to avoid any undue alteration or effacement of health data, whether it is intentional and malicious or unintentional, and whether it comes from authorized or unauthorized users (Dehling et al., 2014).

A HIE that is accessible and operates at its full capacity whenever an authorized user needs it meets the availability requirement. In order to meet this requirement, a HIE has to respond adequately even in peak periods (scalability), to resist to hardware and/or software failures (resilience), and to be designed in a fashion that allows to immediately or very quickly recuperate data after any kind of disaster (recoverability) (Dehling et al., 2014).

# 3 METHODS

## 3.1 Data Source

For the purposes of this study, we used data collected by the European Commission through the 2013 eHealth survey (Joint Research Centre, Institute for Prospective Technological Studies). The survey targeted acute care hospitals across the European Union (27 member states, plus Croatia, Iceland, and Norway), with the objective of benchmarking the level of eHealth use (European Commission, 2014).

## 3.2 Sample

The European Commission survey collected data from a total of 1753 acute care hospitals. But as our aim was to study the HIE usage and related IT-security practices, we dropped all hospitals that declared to not use any form of HIE. This led us to a sample of 1293 hospitals, which represent 73.8% of all surveyed hospitals. From this sample, we dropped 170 cases (13.2%) due to missing values on HIE-related measuring variables (no answer or 'don't know' response). This led us to a final sample of 1123 hospitals. The statistical tests for non-response bias analysis were non significant.

Seven out of 10 hospitals in our sample are public hospitals. They are mostly non-university hospitals (84.6%). Independent hospitals make up almost three quarters (73.4%) of the sample. Medium hospitals (between 101 and 750 beds) make up two thirds (67.1%) of the sample. 6 out of 10 hospitals (60.2%) rated themselves to being in an intermediate phase on their way in transition from a paper-based system towards a fully electronic-based system. For slightly more than half of hospitals (51.3%), the IT budget represents between 1 to 3% of the total hospital budget. As for IT-security regulation reference, 71.9% of sampled hospitals reported to have developed an in-house regulation, 65.5% and 33.6% reported to rely respectively on national-level and regional-level regulations.

## 3.3 Measurement

For this study, our contextual variables were measured through either multiple choice questions (e.g. status), dichotomous questions (e.g. hospital university), interval scales (e.g. size), or ordinal scales (e.g. transition level from paper to electronic-based system).

As for the clustering variables, namely HIE-related variables as well as IT-security related variables, they were all but one measured through dichotomous questions: yes (1) for the presence of a practice related to either information exchange (Table 1) or to IT-security (Table 2), and no (0) if the practice was not implemented. The sole exception is for the second availability-related question: hospitals were asked how much time it would take them to restore their critical clinical systems in the wake of a disaster causing a complete loss of data. Hospitals were asked to choose only one response among the following: immediately, less than 24 hours, less than 2 days, less than 1 week, less than 1 month, and more than 1 month. A hospital that would be able to immediately restore data was given the full score on this point (1) while a hospital that would need more than a month was given a null score (0). Hospitals in between these two extremes were given scores of 0.8 (less than 24 hours), 0.6 (less than 2 days), 0.4 (less than 1 week), and 0.2 (less than 1 month).

The HIE index with which we measure to what extent a given hospital electronically exchanges health information was developed based on the "yes" answers to questions in Table 1. These questions allow to know which information (4 types of information) a hospital electronically exchanges and with whom the exchange is done (5 types of partners).

As 1 point is attributed to a "yes" answer to any type of exchange with any type of partner, and zero to a "no" answer, the score obtained is theoretically comprised between 0 (there is no electronic exchange at all) and 20 (exchange of all 4 types of information with all 5 categories of partners). For convenience, the score was calibrated to a 10-scale measure.

Table 1: HIE Usage Levels.

| **Does your hospital exchange electronically:**<br>A. Clinical care information<br>B. Laboratory results information<br>C. Medication lists information<br>D. Radiology images and reports | **Measure (Yes: 1 / No: 0)** | | | |
|---|---|---|---|---|
| | **A** | **B** | **C** | **D** |
| a). With other hospitals | | | | |
| b). With external general practitioners | | | | |
| c). With external specialists | | | | |
| d). With health care providers in other EU countries | | | | |
| e). With health care providers outside the EU countries | | | | |

We also developed an IT-security index taking into account the IT-security practices implemented (Table 2). Consistent with our definition of IT-security, the IT-security index allows to assess the level of IT security practices implementation alongside three dimensions: confidentiality, integrity, and availability. The confidentiality component of IT security was captured through five (5) questions related to data encryption and data access control; each of the integrity and availability components was measured through two (2) questions. Before calibrating the overall IT-security index on a 10-scale measure, all its three dimensions were equivalently weighted (2 points for each one); this step allowed us to avoid that an over-weight be put on the confidentiality component due to its being captured through more questions (5) than the other components (2 questions each).

## 3.4 Cluster Analysis

We performed two cluster analyses, one on HIE usage dimensions and another on IT-security practices. We used SPSS's agglomerative hierarchical clustering algorithm, with Ward's minimum variance and squared Euclidian distance as grouping criterions. To decide the optimal number of clusters, we inspected the Euclidian distances across dendrograms produced by the algorithm. From this inspection a 3-cluster solution emerged as a probable optimal solution for HIE usage, while two solutions (a 3-cluster and a 4-cluster solutions) appeared to be plausible for IT-security practices. To confirm the HIE-related cluster and to decide which solution among the two related to IT security would be better, we applied Ketchen and Shook's (1996) recommendation: using SPSS's random selection functionality, we constituted subsamples of about successively 70% and 40%, on which we performed the already described clustering procedure, after which we analyzed the resulting dendrograms. The results of this analysis confirmed the robustness of the 3-cluster solutions for both HIE usage and IT-security practices. Once the clusters were formed, we performed the Tamhane's T2 (post-hoc) test to ascertain pair-wise differences between clusters' means.

Table 2: IT-ecurity Practices Measures.

| **Practice** | **Measure** |
|---|---|
| **1. Confidentiality** | |
| 1.1. Encryption of stored data | Yes / No |
| 1.2. Encryption of transmitted data | Yes / No |
| 1.3. Access control through cards | Yes / No |
| 1.4. Access control through fingerprint information | Yes / No |
| 1.5. Access control through a password | Yes / No |
| **2. Integrity** | |
| 2.1. Data entry in the hospital's IT system certified with digital signature | Yes / No |
| 2.2. Clear structured rules on reading-writing patients' electronic medical data | Yes / No |
| **3. Availability** | |
| 3.1. Hospital archive strategy for long-term storage and disaster recovery | Yes / No |
| 3.2. Time laps to restore critical clinical information system operations after a disaster causes the complete loss of data | Hours / Days / Weeks / Months |

# 4 RESULTS AND DISCUSSION

## 4.1 Results of Cluster Analysis

We present in Table 3 the HIE usage patterns resulting from our cluster analysis. But, before scrutinizing the differences between clusters, we can note from the grand means in Table 3 that overall, clinical care information is the most electronically exchanged information (with an average of 1.68 types of partners), followed by laboratory results information (1.46), while radiology images and reports (1.03) as well as medication lists information

(0.72) are the least exchanged.

Table 3: HIE Usage Patterns Resulting from Cluster Analysis.

| Variable (Grand Mean) | Cluster Label (n; %) | | | Anova (F Test) |
|---|---|---|---|---|
| | Advanced (240; 21.4%) Mean | Average (348; 31.0%) Mean | Laggards (535; 47.6%) Mean | |
| Clinical Care (1.68) | **H** $2.74_a$ | **H** $2.64_a$ | **L** $0.58_b$ | 1026.89* |
| Laboratory Results (1.46) | **H** $2.64_a$ | **M** $1.90_b$ | **L** $0.65_c$ | 377.79* |
| Medication Lists (0.72) | **H** $2.65_a$ | **L** $0.13_c$ | **M** $0.24_b$ | 1309.17* |
| Radiology Images and Reports (1.03) | **M** $1.88_b$ | **L** $0.72_c$ | **H** $2.52_a$ | 150.01* |

Legend:
- *: p<0.001 (two-tailed test);
- a,b,c: Within rows, different subscripts indicate significant (p<0.05) pair-wise differences between means on Tamhane's T2 (post-hoc) test;
- H (High), M (Medium), and L (Low) indicate relative magnitude of the group means on each variable across the three clusters

Three clearly distinct clusters emerged from our analysis. We labelled these clusters according to the intensity of HIE usage given by the means calculated based on how many different types of health information are electronically exchanged with how many types of healthcare partners (cf. Table 1). The first cluster we labelled "Advanced HIE users" is the smallest group (21.4%) and exhibits the highest levels of exchanges in 3 out of 4 types of exchanged health information (clinical care, laboratory results, medication lists), and in the fourth (radiology images and reports), it comes in the second position. The second and third clusters account respectively for 31% and 47.6% of hospitals in our sample, and they both score « high » in one type of health information exchanged, they both come in the middle position once, and they both score « low » twice. At this point they seem quite similar, but they are distinct in that their respective high, medium and low scores are realized on different types of health information.

Besides, the third cluster is markedly more unipolar than the second cluster: hospitals in the third group exchange almost exclusively one type of health information (radiology images and reports), while hospitals in the second cluster, in addition to remarkably exchanging clinical care information, also exchange laboratory results to a certain extent. Thus, we labelled the second cluster « Average HIE Users » and the third cluster « Laggard HIE Users ».

We present in Table 4 the results of our cluster analysis, based this time on IT-security practices. For this analysis, we used data on 1068 hospitals (instead of 1123 - loss of 55 observations) due to missing data on key IT-security variables for the 55 dropped observations.

Table 4: IT-Security Practices Patterns Resulting from Cluster Analysis.

| Variable (Grand Mean) | Cluster Label (n; %) | | | Anova (F Test) |
|---|---|---|---|---|
| | Strong (281; 26.3%) Mean | Moderate (520; 48.7%) Mean | Weak (267; 25.0%) Mean | |
| Confidentiality (0.99) | **H** $1.18_a$ | **M** $0.96_b$ | **L** $0.85_c$ | 28.12* |
| Integrity (1.23) | **H** $2.00_a$ | **L** $0.90_c$ | **M** $1.08_b$ | 847.18* |
| Availability (1.49) | **H** $1.77_a$ | **H** $1.75_a$ | **L** $0.68_b$ | 2223.44* |

Legend:
- *: p<0.001 (two-tailed test);
- a,b,c: Within rows, different subscripts indicate significant (p<0.05) pair-wise differences between means on Tamhane's T2 (post-hoc) test;
- H (High), M (Medium), and L (Low) indicate relative magnitude of the group means on each variable across the three clusters

Generally speaking, it appears that the "availability" component of IT-security is the most implemented practice (grand mean of 1.49), followed by the "integrity" dimension (1.23), while the "confidentiality" dimension comes in the last position (0.99).

Based on levels of IT-security practices implemented, we labelled the derived three clusters "Strong IT-Security", "Moderate IT-Security", and "Weak IT-Security". The cluster labelled "Strong IT-Security" is comprised of 26.3% of surveyed hospitals and exhibits the highest levels on all the three dimensions of our IT-security index. On the other end of the spectrum one finds the cluster with low levels of IT-security practices implemented. This cluster labelled "Weak IT-Security" accounts for 25% of our sample. The largest group (48.7%) is the

"Moderate IT-Security" cluster which exhibits high levels on the availability component of IT-security, while exhibiting relatively moderate levels on the confidentiality component, and low levels on the integrity dimension.

## 4.2 HIE Usage and IT-security Practices: Cross-comparison

Hospitals that electronically exchange health information are more exposed to IT-security breaches than hospitals that do not. It was then expected that higher levels of HIE usage would be associated with higher levels of IT-security practices implemented. To test this hypothesis, we present in Table 5 a cross-tabulation of HIE patterns and IT-security practices patterns.

Table 5: Cross-Tabulation of the Two Sets of Clusters.

| HIE Patterns* | | IT-Security Practices Patterns | | | |
|---|---|---|---|---|---|
| | | Strong (26.3%) | Moderate (48.7%) | Weak (25.0%) | **TOTAL** |
| Advanced (21.3%) | n | 87 | 103 | 38 | **228** |
| | % | 38.2% | 45.2% | 16.7% | **100.0%** |
| Average (31.4%) | n | 94 | 160 | 81 | **335** |
| | % | 28.1% | 47.8% | 24.2% | **100.0%** |
| Laggards (47.3%) | n | 100 | 257 | 148 | **505** |
| | % | 19.8% | 50.9% | 29.3% | **100.0%** |
| **TOTAL** | **n** | **281** | **520** | **267** | **1068** |

*The percentages are here **slightly** different from the percentages in Table 3 because of 55 dropped observations for the clustering analysis on IT-security practices.

The "perfect match" between HIE usage levels and IT-security practices implementation occurs for only 395 (= 87 + 160 + 148) hospitals (37.0% of all the sample).

More precisely, it is worth noting, from Table 5, that only 38.2% of "advanced HIE users" are at the same time "strong IT-security practices" implementers. This means that over 60% hospitals that are well advanced in using health information exchange do not adopt IT-security practices that are consistent with the associated IT-security risks. More preoccupying are the 16.7% of hospitals that are extensively using HIE while exhibiting weak IT-security practices implementation. On the positive note, one can emphasize that 70.7% (19.8% + 50.9%) of hospitals that are far behind with regard to HIE usage (laggards) have already in place IT-security practices that would allow them to securely step up their HIE usage should the need arises.

We pushed further our analysis by comparing each hospital's level of HIE usage with its implementation level of IT-security practices. To do so, we used the HIE Index and the IT-security Index described in section 3.3. In Figure 1, we plotted each hospital's HIE index (horizontal axis) against its IT-security index (vertical axis). Both indices are on a 10-scale measure.

From the median lines (M1 and M2), one can note that half of the sampled hospitals:

– are very weakly involved in health information exchange (the median is 2.5 on a 0 to 10 scale);
– have already made over the half path in implementing IT-security practices (median of 6.24 on a 0 to 10 scale).

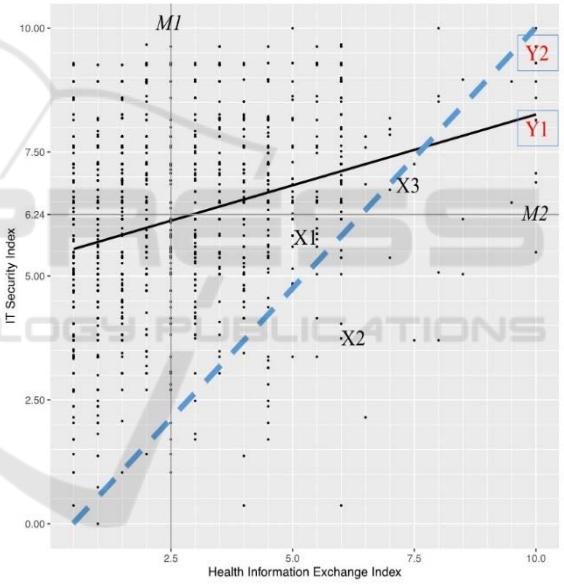


Figure 1: HIE Index and IT-Security Index.

The ascending slope of the regression line (Y1) suggests that overall, there is a trend toward enhancing IT-security measures as hospitals intensify their electronic HIE usage. This is a rather positive result, but upon close scrutiny, one has to moderate the positive impression. Indeed, the points are scattered all over a large part of the surface of the figure, instead of being roughly grouped along the regression line, which suggests a lack of a consistent trend: the variability within hospitals is too high. Even though there are many hospitals that have implemented IT-security practices at a high level while using HIE at lower levels, there are other many

hospitals in the opposite situation (weak IT-security practices implemented and higher levels of HIE usage).

As we hypothesized that hospitals would have to adopt IT-security measures consistent with their electronic HIE levels, the diagonal line in Figure 1 reflects the theoretical "perfect" alignment between IT-security practices and HIE usage. Stating this, we are aware of the fact that the health information exchange is not the only determinant of IT-security measures. It is possible that a hospital weakly or not at all involved in electronic HIE would feel the need to stage up its IT-security practices due to its being well advanced in the transition towards a fully electronic-based hospital management system (which does not yet include HIE). Thus, in our view, the diagonal line defines the coordinates (HIE Index, IT-Security Index) that indicate the minimum threshold of IT-security practices any hospital using electronic HIE at some extent must implement. More precisely, any hospital above the diagonal line (like the hospital represented by the coordinate X1) displays an IT-security index above the minimum it is required to attain considering its level of electronic HIE usage. Conversely, a hospital represented by the coordinate X2 below the diagonal line should step up its IT-security practices to meet the minimal security requirements of its level of HIE usage. The IT-security index of hospital X3 right on the diagonal line is consistent with its HIE usage level.

The analysis of the dispersion of points in Figure 1 leads to conclusions that are consistent with the results stemming from our cluster analysis, and specifically from the cross-comparison of HIE usage clusters and IT-security practices clusters (Table 5). From the Figure 1, we note that there are many points above than below the diagonal line, which means that most hospitals have already in place IT-security measures that would allow them to securely go further with electronic HIE. Hospitals in this position are mainly "HIE laggards" that are either "moderate IT-security" practices implementers (50.9% of HIE laggards - Table 5) or "strong IT-security" practices implementers (19.8%); they also include "average HIE users" that are "strong IT-security" practices implementers (28.1%).

# 5 IMPLICATIONS AND CONCLUSION

Our study allows to shed light on the state of HIE in European hospitals. First of all, we found that 73.8% of surveyed hospitals are engaged in one form or another of electronic HIE. A higher rate of hospitals that have already adopted electronic HIE is rather a good news. Indeed, previous studies have proven that an electronic HIE can be instrumental not only in improving patient care and safety (Cochran et al., 2015; Kaelber et al., 2007), but also in alleviating the health system's financial burden through significant reduction of laboratory tests and radiology examinations (Yaraghi, 2015). However, the mere adoption in itself is not enough to yield the potential benefits expected from HIE. Hospitals have to reach the "meaningful use". As HIE usage levels vary from one hospital to another, we grouped hospitals according to their HIE usage patterns. Hospitals that emerged as "advanced HIE users" represent only 21.4% of surveyed hospitals. A relatively important proportion of hospitals (47.6%) exhibit HIE usage patterns that put them in the category of "laggard HIE users". From these results, it is clear that there is still a long way to go in order to achieve the "meaningful use" of HIE in European hospitals.

With regard to IT-security practices, only 26.3% of surveyed hospitals display a strong position. In absolute terms, this rate is very low considering the highly sensitive nature of health information. However, back to our research question, our main objective was to ascertain whether European hospitals do live up to the IT security and privacy challenges of HIE. In this regards, our results are rather mixed: we found that most of surveyed hospitals have in place an IT-security apparatus that is either consistent with their HIE usage (37.0%) or more ambitious than what would be required of them considering their HIE usage level (42.2%). These two groups make up 79.2% of surveyed European hospitals. The remaining hospitals (20.8%) would need to step up their IT-security practices in order to keep up with their electronic HIE usage levels.

This global picture seems positive, but it hides some preoccupying situations that appear when one scrutinizes the HIE clusters. The group of "Advanced HIE users" is composed of 228 hospitals, among which 141 (=103 + 38) do not live up to the security challenges that their HIE usage entails. This represents 63.7% of the group that needs the most to implement IT-security practices. The same analysis can be done with the group labelled "Average HIE users": this group comprises 335 hospitals, among which 81 (24.2%) do not meet the threshold of IT-security practices implementation that would be in line with their HIE usage level.

In spite of some limitations (usage of secondary data, assumption of a linear relationship between HIE

usage and IT-security practices), this study addresses one of the major concerns surrounding the electronic HIE usage: the IT-security practices that are required to ensure the trust of both patients and healthcare providers. In future works, it would be worthwhile to pursue and deepen the analysis of factors that determine the levels of HIE usage and IT-security practices implementation.

## REFERENCES


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

Ancker, J. S., Edwards, A. M., Miller, M. C., & Kaushal, R., 2012. Consumer perceptions of electronic health information exchange. *American Journal of Preventive Medicine, 43*(1), 76-80.

Bahtiyar, S., & Çaglayan, M. U., 2014. Trust Assessment of Security for e-Health Systems. *Electronic Commerce Research and Applications, 13*(3), 164-177.

Berwick, D.M., Nolan, T. W., & Whittington, J., 2008. The Triple Aim: Care, health, and cost. *Health Affairs, 27*(3), 759-769.

Bitton, A., Flier, L. A., & Jha, A. K., 2012. Health information technology in the era of care delivery reform: To what end? The Journal of the American Medical Association, 307(24), 2593-2594.

Cochran, G. L., Lander, L., Morien, M., Lomelin, D. E., Sayles, H., & Klepser, D. G., 2015. Health care provider perceptions of a query-based health information exchange: barriers and benefits. *Journal of Innovation in Health Informatics, 22*(2), 302-308.

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.

European Commission, 2014. *European hospital survey: Benchmarking deployment of eHealth services (2012-2013).* Luxembourg: JRC Scientific and Policy Reports - Institute for Prospective Technological Studies.

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.

Hwang, H.-G., Han, H.-E., Kuo, K.-M., & Liu, C.-F., 2012. The differing privacy concerns regarding exchanging electronic medical records of Internet users in Taiwan. *Journal of Medical Systems, 36*(6), 3783-3793.

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.

Kaelber, D. C., & Bates, D. W., 2007. Health information exchange and patient safety. *Journal of Biomedical Informatics, 40*(6 SUPPL), S40-S45.

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.

O'Donnell, H. C., Patel, V., Kern, L. M., Barrón, Y., Teixeira, P., Dhopeshwarkar, R., & Kaushal, R., 2011. Healthcare consumers' attitudes towards physician and personal use of health information exchange. *Journal of General Internal Medicine, 26*(9), 1019-1026.

Ponemon Institute, 2016. *Sixth annual benchmark study on privacy & security of healthcare data*. Traverse City, MI, USA: Ponemon Institute.

Simon, S. R., Benjamin, A., Delano, D., & Bates, D. W., 2009. Patients' attitudes toward electronic health information exchange: Qualitative study. *Journal of Medical Internet Research, 11*(3), e30.

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.

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.

White, P., 2004. Privacy and security issues in teleradiology. *Seminars in Ultrasound, CT and MRI, 25*(5), 391-395.

Yaraghi, N., 2015. An empirical analysis of the financial benefits of health information exchange in emergency departments. *Journal of the American Medical Informatics Association, 22*(6), 1169-1172.

Zwaanswijk, M., Ploem, M. C., Wiesman, F. J., Verheij, R. A., Friele, R. D., & Gevers, J. K., 2013. Understanding health care providers' reluctance to adopt a national electronic patient record: an empirical and legal analysis. *Medicine And Law, 32*(1), 13-31.