Trust in a Cloud-Based Healthcare Environment

Teresa Piliouras; Pui Lam (Raymond) Yu; Yang Su;
and Vijay Kumar Ajjampur Siddaramaiah
Center for Advanced Research
on Emerging Healthcare Technologies
Technical Consulting & Research, Inc.
Weston, CT, 06883

Nadia Sultana; Edward Meyer; and
Rodney Harrington
New York University College of Nursing
New York, NY USA 10003

***Abstract*—The authors are engaged in on-going research on the functionality of Electronic Health Records (EHR) software, and challenges doctors face as they migrate from paper to electronic-based record keeping. Our goal is to assist healthcare providers in the adoption of EHR software and in the optimization of their clinical and practice management functions.**

Healthcare providers face increasing pressure to adopt an EHR, if they haven't already done so. Providers should temper their response to this pressure and avoid blind faith selection. In this paper, we review the meaning of trust, and introduce a measure of *trustworthiness.* This measure is used to rank cloud-based EHR solutions. The trustworthiness measure quantifies how well an EHR satisfies the provider needs and critical operational requirements. The trustworthiness measure uses a certainty factor to weigh the quality of evidence used to evaluate the EHR. The trustworthiness model provides a framework for contextualizing and prioritizing important selection considerations, and can be used with risk mitigation strategies to improve decision making when selecting an EHR.

Keywords-electronic health records; cloud-computing; trust; EHR policies; privacy; security, safety; confidentiality; risk mitigation

I. INTRODUCTION

The health care industry is being transformed by numerous legislative, insurance, legal, and government initiatives aimed at promoting wide-scale adoption of health information technology (HIT). To cite a few examples:

- The ARRA (American Recovery and Reinvestment Act) of 2009 earmarked over $17 billion to reimburse eligible healthcare providers and hospitals for expenses related to adoption of electronic health records systems (EHRs). These reimbursement incentives are offered through 2016. After this, the incentives will be replaced by penalties -- in the form of decreased Medicare reimbursement rates [1, 2, 3].
- The Patient Protection and Affordable Care Act (PPACA) of 2010 amends the False Claims Act (FCA) with new provisions for penalties, criminal fines, and imprisonment to deter abuse and fraud amongst providers participating in Medicare, Medicaid, and the Children's Health Insurance Program (CHIP) [4]. EHRs collect documentation needed to support claims submitted to federal health care programs, and provide proof that patient care meets or exceeds accepted standards.
- Increasingly stringent HIPAA privacy, security and breach notification rules are expected in coming months, and "privacy and security are included in all the hot federal health policies of today, including meaningful use, value-based purchasing, bundled payments, quality measurements, accountable care organizations, and auditing" [5]. Compliance with meaningful use and other accountability standards necessitates the use of EHRs.
- Providers are incentivized to use government certified EHRs by receiving the best rates on malpractice insurance, and on patient care insurance reimbursements.

These initiatives are encouraging growing numbers of healthcare providers to reconsider their reliance on paper-based clinical and practice management record keeping systems. To-date, providers have eschewed EHRs by a 9-to-1 margin. The reasons are manifold, and include [3, 5]:

- EHRs are perceived as ephemeral and vulnerable to technology failures and security breaches;
- EHRs, used improperly, expose the practice to legal liabilities and exposures;
- EHRs are subject to more onerous Health Insurance Portability and Accountability Act (HIPPA) provisions than paper-based recordkeeping;
- EHRs are costly -- with acquisition costs that can range from $10,000 to $100,000 per eligible provider;
- EHRs often require a long learning curve. Typically, physician productivity declines 30% or more when EHRs are first installed, and does not increase until the system has been used six to twelve months;
- EHR selection, implementation and maintenance are technically challenging. The failure rate of EHR implementation efforts is estimated to between 40-60%.

EHRs come in two flavors: on-site or cloud-based. An on-site EHR is maintained locally, on the premise of the practice office(s). This approach requires considerable investment in computer equipment, software, and technical support staff. With a cloud-based solution, software and data files are maintained and backed-up by a third-party hosting service,

978-1-4577-1591-4/11/$26.00 ©2011 IEEE

relieving providers of these responsibilities. Providers must maintain end-user computers and network connectivity to access the cloud via the Internet using a web-enabled browser, but this is significantly easier and less costly than a full on-site EHR installation.

Providers are generally skeptical of cloud-based EHRs, perceiving them as higher risk and less trustworthy than on-site EHRs. Physicians have legitimate concerns about safeguarding patient privacy and confidentiality, and the need to comply with HIPAA and other government regulations when relying upon a third-party to collect, maintain, and secure clinical and practice management data [16]. Nonetheless, many medical organizations, especially small ambulatory practices, lack the resources and expertise to maintain a secure in-house EHR. Without the requisite systems, processes and procedures in place, they may actually be more at risk than if these responsibilities were outsourced to a reliable, professional third-party [3]. One of the goals of the authors' research is to provide healthcare professionals with tools to make informed decisions on health information technology, so the adoption of EHRs is not rejected out of hand based on fear nor accepted without appropriate due diligence.

Ultimately, a practitioner's decision to adopt an EHR comes down to trust that the benefits will outweigh the risks and costs. A key to establishing trust is to choose a solution well matched to the providers' capabilities and technical, functional, governance, and compliance needs.

II. TRUST – BLIND OR NOT?

The notion of trust has been widely examined in the literature, from a multitude of perspectives and disciplines -- including psychology, sociology, economics, computer science, and decision theory. The concept of trust is complex, multi-faceted, and context-dependent. Trust may be based on objective knowledge, subjective opinion, and prior experience [6, 7, 8, 9]. No universal definition of trust exists, and no definition can adequately encompass all its dimensions.

According to [11], "trust revolves around 'assurance' and confidence that people, data, entities, information or processes will function or behave in expected ways. Trust may be human to human, machine to machine (e.g., handshake protocols negotiated within certain protocols), human to machine (e.g., when a consumer reviews a digital signature advisory notice on a web site) or machine to human (e.g., when a system relies on user input and instructions without extensive verification). At a deeper level, trust might be regarded as a consequence of progress towards security or privacy objectives."

As depicted in Figure 1, both known and unknown risks exist within the universe. Ideally, trust should be based on explicit knowledge of known knowns and known unknowns. Otherwise, trust is blind. Unknown unknowns cause unexpected problems, precluding preemptive corrective action. Unknown unknowns arise when providers fail to understand their own needs and the limitations of HIT.

For example, providers who acquire EHR solutions on the basis of recommendations from colleagues or other third-parties, without further examination, do so at their own peril. Anecdotal stories abound of providers locking into long term contracts and then finding the system selected does not meet their needs.

Industry certifications and ratings of EHR offerings, while helpful, do not paint a complete picture. For example, the Office of the National Coordinator - Authorized Testing and Certification Body (ONC-ATCB) has established standards that EHRs must meet to qualify for Meaningful Use certification. Using an ONC-ATCB certified EHR system helps physicians serving Medicare and Medicaid patients to qualify for government ARRA (American Recovery and Reinvestment Act) Meaningful Use (MU) incentives. However, the EHR's support of MU requirements does not address the larger issue of whether it is suitable for the practice or implements industry best practices for online security and privacy.

ICSA Labs, an independent division of Verizon Business, provides reliable "independent, 3rd party product assurance for end users and enterprises for the last 20 years. ICSA Labs has provided vendor-neutral testing and certification for hundreds of security products and solutions for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance" [6]. ICSA Labs posts its certification results on EHR packages for free on its website. Notably, many well-known EHRs with significant market share are missing from the reports.

There are hundreds of EHR solutions on the market. Many details needed to make an informed decision about their functionality, safety, privacy, and robustness are difficult to obtain or unavailable in a form that invites easy comparison. Cloud-based EHRs are vulnerable to a diverse array of internal and external threats, and are deceptively hard to secure. Providers considering a cloud-based EHR must confront a multitude of unknown unknowns. In the next section, a multi-criteria decision model is presented to help to quantify these uncertainties.

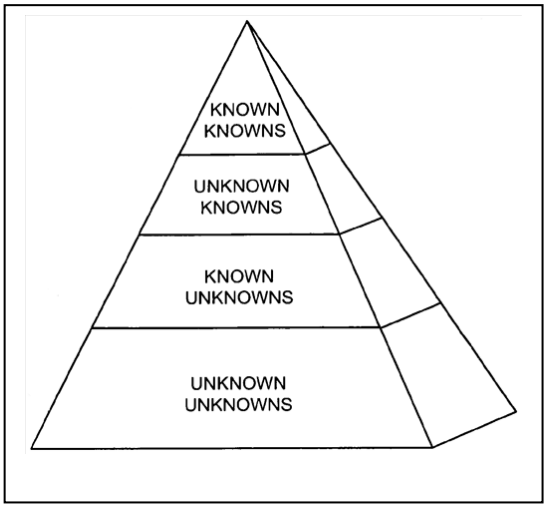

Figure 1: Universe of Unknowns and Knowns

III. A Multiple-Criteria Decision Model of Trustworthiness

Application of the multiple-criteria decision model of trustworthiness involves the following steps:

1. Define relevant decision factors.
2. Collect data related to the decision factors.
3. Assign a certainty value to the perceived credibility of collected data.
4. Use collected data and associated certainty value as inputs to mathematical model shown in (1), and compute a trustworthiness score for EHR.
5. Sort all EHR candidates based on their trustworthiness score, from high to low. The ranking indicates the preference order of one EHR over another (Note: it does not indicate how much one EHR is preferred over another).
6. Examine potential weaknesses in decision factor hierarchy and identify risk mitigation strategies.

The trustworthiness model is based on a mathematical equation of the following general form:

$$F(X) = \text{Operator}\ (D_1^{C_1}, D_2^{C_2}, \ldots, D_n^{C_n}) \quad (1)$$

Where:

- D_j represents a decision factor associated with trustworthiness;
- C_j represents a weighting or certainty factor associated with D_j;
- "Operator" represents a generic mathematical aggregation procedure for computing a Trustworthiness score based on the weighted decision factors;
- F(X) represents an overall Trustworthiness score.

Key features of the model include:

- **Objective and/or subjective criteria are used in evaluation process.** An example of an objective decision factor is "System Availability." This metric is generally expressed as a percentage (e.g., if system availability is 99.999 %, this implies it is not available .001 % of the time). An example of a subjective decision factor is "Reputation." The standard of measurement for this decision factor is not universal and may be based on the personal preferences and opinions of the decision maker.
- **Multiple decision factors (D_j) are used to assess EHR trustworthiness**. Fig. 2 is a pictorial representation of the building blocks for a trustworthy EHR (depicted as a fortress). The building blocks are arranged in a hierarchy. The most fundamental level – security – represents the foundation of EHR trustworthiness. If this decision critierion is not met, then there will be a critical weakness in the EHR trustworthiness that cannot be overcome by satisfaction of higher level critiera – such as vendor and end-user characteristics. Each hierarchical building block reinforces the others, and when all are satisfied, the EHR is deemed trustworthy. The decision factors include:
  - *Security*. Possible dimensions to represent this criterion include: business recovery and continuity; confidentiality; data location and segregation; privacy; and transparency (allowing provider to monitor and observe behaviors and events on the vendor side of the cloud).
  - *Governance and regulatory compliance*. Possible dimensions to represent this criterion include: auditability; contractual compliance with HIPAA and guarantees; data integrity, retention and ownership; and policies and procedures.
  - *Functionality*. Possible dimensions to represent this criterion include: scope of features and functions supported.
  - *System performance*. Possible dimensions to represent this criterion include: system availability; accessibility; reliability; mean time between failures; response time; and quality of services (service level agreements).
  - *Vendor characteristics*. Possible dimensions to represent this criterion include: competence; honesty; professionalism; integrity; qualifications; expertise; responsiveness; reputation; and viability.
  - *User Characteristics:* Possible dimensions to represent this criterion include: training received; qualifications; expertise; and technical background.
- **Decision factors (D_j) are expressed on a scale between one (indicating complete trustworthiness) and zero** (indicating completely untrustworthy). Partial trustworthiness is indicated by a proportionate value between zero (0) and one (1).
- **Each decision factor is associated with a certainty (C_j)** weighting factor that expresses the level of confidence in the evidence used to assess (D_j). C_j may be expressed by a single dimension of certainty, or as an aggregate of multiple dimensions of certainty.
  - Suggested dimensions of certainty include: accuracy; completeness; objectivity; measurability; simplicity, and verifiability.
  - Certainty is expressed on a scale between zero (indicating complete uncertainty) and one (indicating complete certainty). Partial certainty is indicated by a value between 0 and 1. The closer the value is to one (1), the closer the criterion achieves complete certainty. The certainty measure is used to reduce the weight given to the decision factor if it is not wholly satisfied (i.e., equal to 1).
  - One or more certainty dimensions may be combined into a single (C_j) certainty score. As shown in Table 1, there are several ways to create an aggregate (C_j):

- The preferred method is to calculate a simple average or mean score. This method is demonstrated in Fig. 3, where C_j is computed as the average of two certainty dimensions (Accuracy and Completeness): $C_j = ((C_1 + C_2)/2)$.
- Alternatively, C_j may be based on the minimum certainty value. This method implies it is especially important to satisfy all the certainty dimensions in the evaluation process.
- A third option is to compute an aggregate (C_j) certainty score based on the maximum certainty value. This option implies it is especially important to maximize consideration of the best certainty feature.
- The method used to determine an aggregate certainty (C_j) may vary depending on the decision factor. For example, the minimum operator might be used to determine the aggregate (C_j) value for the security decision factor. Similarly, the maximum operator might be appropriate for weighting a subjective vendor decision factor. Any combination of aggregation methods can be used, as long as they are used consistently in the same manner for all EHR evaluated.

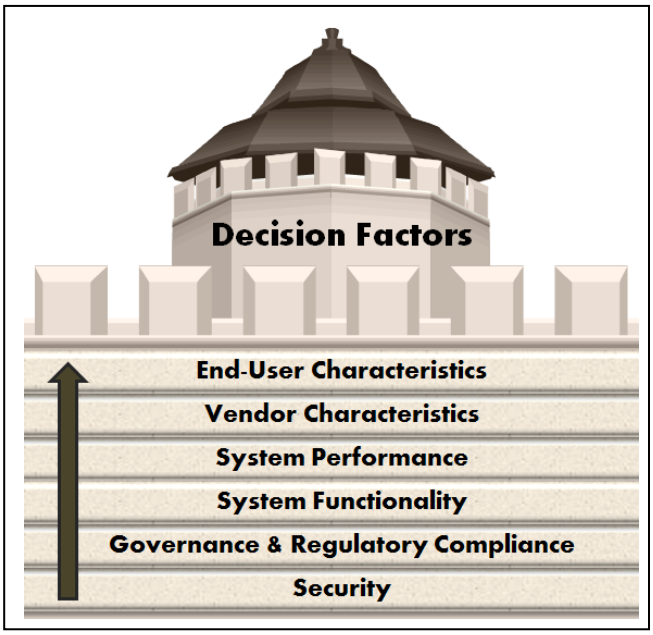

Figure 2: Decision Factor Hierarchies

TABLE 1: OPTIONS FOR CALCULATING AGGREGATE CERTAINTY SCORE (C_j)

Aggregation Method	*Linguistic Interpretation*	*Features*	*Calculation Example*
MINIMUM	**"AND"**: Goal is to satisfy certainty factor 1, AND certainty factor 2, AND certainty factor 3, etc.	Overall score is determined by the worst individual certainty factor, no matter what it is.	MIN (0.7, 0.8, 0.9) = 0.7
MAXIMUM	**"OR":** Goal is to satisfy certainty factor 1, OR certainty factor 2, OR certainty factor 3, etc.	Overall score is determined by the best individual certainty factor, no matter what it is.	MAX (0.7, 0.8, 0.9) = 0.9
MEAN	**ALL":** Goal is to satisfy all options to some extent	Overall score represents a balanced representation of all certainty factors	MEAN (0.7,0 .8, 0.9) = 0.8

An example is now provided in to demonstrate application of the model. As shown in (2), *Trustworthiness* is calculated as the sum over all decision factor hierarchies, (D_j), raised to the power ($1/c_j$) – where C_j is defined as the certainty associated with D_j.

$$\sum (D_j)^{1/Cj} = \text{Trustworthiness} \qquad (2)$$

The decision factor (D_j) values correspond to: user characteristics; vendor characteristics; performance; functionality; governance/regulatory compliance; and security. Each decision factor is raised to the power ($1/C_j$). In this example, (C_j) represents the *accuracy* and *completeness* of the evaluation data. An overall Trustworthiness score for the EHR is computed by adding all the weighted $(D)^{1/Cj}$ values. Trustworthy scores are sorted high to low to obtain a preferred ranking order. Since EHR #1 has a higher score (4.552573) than EHR #2 (3.6797665), it is the preferred solution.

Decision Factor	Decision Facor Score (Dj)	Accuracy (C_1)	Completeness (C_2)	Cj = (C_1+C_2)/2	$Dj^{(Cj)}$
User Characteristics	1	1	0.8	0.9	1
Vendor Characteristics	0.8	1	1	1	0.8
Performance	0.9	1	0.4	0.7	0.86026481
Functionality	0.6	0.9	0.5	0.7	0.48202905
Governance/Regulatory Compliance	1	0.8	0.4	0.6	1
Security	0.7	0.3	0.5	0.4	0.40996341
			Trustworthy Score for EHR #1:		**4.5522573**
User Characteristics	1	1	0.8	0.9	1
Vendor Characteristics	0.7	0.1	0.2	0.15	0.09275136
Performance	0.9	0.6	0.9	0.75	0.86894045
Functionality	1	0.9	0.9	0.9	1
Governance/Regulatory Compliance	0.7	1	1	1	0.7
Security	0.3	0.4	0.2	0.3	0.01807469
			Trustworthy Score for EHR #2:		**3.6797665**

Figure 3: Trustworthiness Calculations for Two EHRs

In a real-life due diligence evaluation, it is important to include all the relevant decision factors in the trustworthiness calculation. According to the CloudSecurity Alliance, the top seven (7) threats to cloud computing are [13]:

1. Abuse and nefarious use of cloud computing;
2. Insecure application programming interfaces (APIs);
3. Malicious insiders;
4. Shared technology vulnerabilities;
5. Data loss or leakages;
6. Account, service and traffic hijacking;
7. Unknown risk profile.

Prevention of these threats implies corresponding security requirements must be satisfied by the EHR to ensure trustworthiness (such as improved programming design of APIs; risk profiling to prevent unknown users from accessing system functions; etc.). An overall Trustworthiness score for security may be calculated in the same manner illustrated above. This discussion is intended to demonstrate the flexibility of the model and how it can be modified to incorporate any number of relevant decision factors.

IV. RISK MITIGATION STRATEGIES

Risk mitigation strategies may be useful in compensating for shortcomings identified in EHRs during the evaluation process. There are three principal ways to manage risk: through risk reduction, risk control, and risk transfer. Risk reduction and risk control might involve, for example, the adoption of a disaster recovery and data continuance strategy. Risk transfer involves shifting the burden of exposure to a third party, often through insurance or outsourcing.

When a cloud-based EHR solution is used, system data are stored at the hosting service, at what is likely to be an undisclosed location. While Physicians are transferring the responsibility of data maintenance to a third-party, they are still liable under HIPAA regulations if protected data is breeched by unauthorized individuals. Providers must maintain secure end-user computers and network connectivity to prevent unauthorized persons from viewing protected, confidential, or sensitive heath records and practice management data.

A thorough due-diligence evaluation, as described here, is a form of risk reduction. It decreases the risk that a poor EHR selection will be made. The model proposed herein provides a framework for contextualizing and prioritizing important considerations. This tool is best used in conjunction with advice and support from expert Information Technology professionals and legal counsel, and after careful analysis of the practice's requirements.

After computing the Trustworthiness scores described in the last section, a simple graphical analysis is recommended. A bar chart plot of the weighted $D_{j.}$ components of the top ranked EHRS makes it easier to compare and visualize the respective strengths and weaknesses of each EHR. As shown in Fig. 5, EHR #1 dominates EHR #2 in every respect except functionality. If a provider were to base a selection decision solely on functionality, EHR #2 would be the likely winner, despite significant trustworthy concerns with the vendor and the system security. If the functionality provided by EHR #2 is critical to the success of the EHR implementation, and it is not supported in EHR #1, then neither solution should be selected. The search for a suitable EHR should be continued.

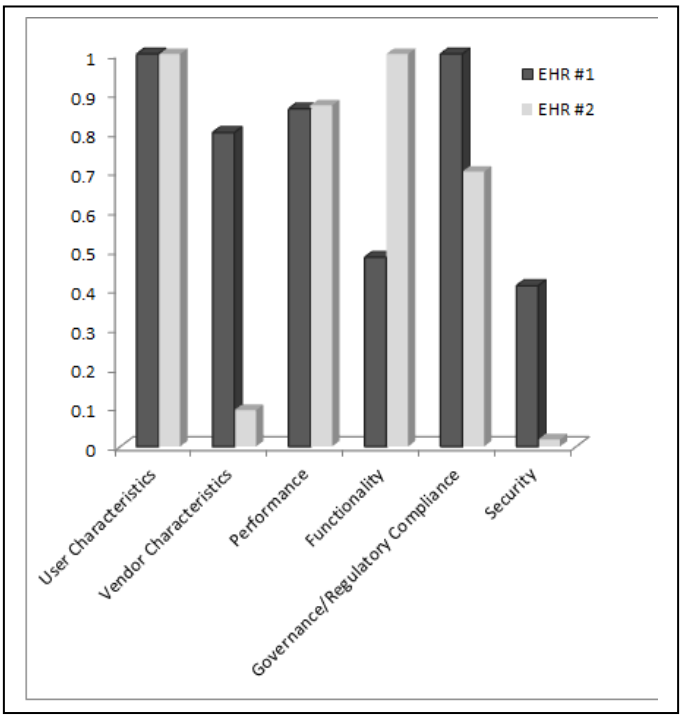

Figure 4: Comparison of Decision Factors in Top Ranked EHRs

V. SUMMARY AND SUGGESTIONS FOR FUTURE RESEARCH

In this paper, the meaning of trust is examined. A multiple-criteria model is presented to characterize trustworthiness for the purpose of evaluating and ranking cloud-based EHR solutions.

Even in best cloud-based EHRs, system integrity is at risk if users fail to observe required safeguards (e.g., by failing to protect system passwords and log-in identifiers, employing inadequate physical security of system computers and networking infrastructure, etc.). Unfortunately, from an end-user perspective, security is inversely proportional to convenience. User education, training, and policies and procedures to enforce best practices are critical in assuring a trustworthy EHR environment in spite of the inconvenience they may impose.

Vendors, for the part, should provide users with monitoring, auditing, and reporting tools to allow on-going verification of the EHR's compliance with user expectations and contractual arrangements. This transparency provides a basis for informed trust and confidence in the cloud-based EHR. Security is inversely proportional to convenience. Paradoxically, improvements in transparency and mutual communication

introduce potential points of system vulnerability that must be carefully managed.

Even with a very high level of trust between parties, security can never be guaranteed with complete certainty. Calculated risks should be carefully weighed against potential exposures and liabilities. From this analysis, one can develop a mix of risk reduction, risk control, and risk transfer strategies suited to the provider needs and setting.

Selecting an appropriate and trustworthy EHR solution requires careful consideration of many decision factors. Collecting information on the decision factors is the most time consuming aspect of applying the multiple-criteria decision model presented here. There is no accepted standard for measuring and reporting data pertinent to relevant decision factors, and information obtained from one vendor may be difficult to compare with information obtained from another. More independent third-party sources of information and industry certification programs are needed so decision makers have access to reliable information required for a thorough due diligence evaluation of trustworthiness. The authors are engaged in on-going research in this area.

REFERENCES

[1] The American Recovery and Reinvestment Act of 2009 (ARRA), p. 115, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname= 111_cong_bills&docid=f:h1enr.pdf.

[2] Centers for Medicare and Medicaid Services, "MEDICARE AND MEDICAID HEALTH INFORMATION TECHNOLOGY: TITLE IV OF THE AMERICAN RECOVERY AND REINVESTMENT ACT,", http://www.cms.hhs.gov/apps/media/press/factsheet.asp?Counter=3466.

[3] Piliouras, T., A Guided Tour of: SOAPware Clinical Suite Electronic Health Records & Practice Management Software, Technical Consulting & Research, Inc., October 2011.

[4] Federal False Claims Act, 31 USC 3729-3733, text available at: http://www.taf.org/federalfca.htm.

[5] Goedert, J., "In Health Care, Privacy & Security Emphasis Will Only Increase," *Health Data Management*, October 6, 2011, http://www.healthdatamanagement.com/news/hipaa-privacy-security-rule-ahima-43354-1.html?ET=healthdatamanagement:e2033:156345a:&st=email&utm_source=editorial&utm_medium=email&utm_campaign=HDM_Daily_100611

[6] ICSA Labs, https://www.icsalabs.com/about-icsa-labs.

[7] Mohammad Momani and Subhash Challa, "Survey of Trust Models in Different Network Domains," *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)*, vol. 1, no. 3, pp. 1-19, September 2010.

[8] Tzu Yu Chuang, "Trust with Social Network Learning in E-Commerce," in *IEEE International Conference on Communications Workshops (ICC)*, Capetown, South Africa, 2010, pp. 1-6.

[9] Firdhous, M., Ghazali, O., Hassan, S., "Trust and Trust Management in Cloud Computing – A Survey," InterNetWorks Research Group, Universiti Utara Malaysia, Technical Report No: UUM/CAS/InterNetWorks/TR2011-01, http://www.internetworks.my/pubs/techrep/TR2011-01.pdf.

[10] Qing Zhang, Ting Yu, and Keith Irwin, "A Classification Scheme for Trust Functions in Reputation-Based Trust Management," in International Workshop on Trust, Security, and Reputation on the Semantic Web, Hiroshima, Japan, 2004.

[11] Ko, Ryan K L; Jagadpramana, Peter; Mowbray, Miranda; Pearson, Siani; Kirchberg, Markus; Liang, Qianhui; Lee, Bu Sung, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," HP Laboratories Technical Report, http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.

[12] Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese, and Paul Hopkins, "The Cloud: Understanding the Security, Privacy and Trust Challenges, Final Report," TR-933-EC, 30 November 2010, Prepared for Unit F.5, Directorate-General Information Society and Media, European Commission.

[13] Cloud Security Alliance, "Top Threats to to Cloud Computing Report (Ver.1.0)," 2010, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[14] *"2010 Data Breach Investigations Report - A Study conducted by the Verizon RISK Team in Cooperation with the US Secret Service*," http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.

[15] "*2011 Data Breach Investigations Report – A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit,"* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

[16] Piliouras, T.; Pui Lam Yu; Housheng Huang; Xin Liu; Siddaramaiah, V.K.A.; Sultana, N.; "Selection of electronic health records software: Challenges, considerations, and recommendations," Systems, Applications and Technology Conference (LISAT), 2011 IEEE Long Island, Issue Date: 6-6 May 2011.

[17] Ryan K L Ko, Bu Sung Lee, Siani Pearson, "Towards Achieving Accountability, Auditability and Trust in Cloud Computing," HP Labs, http://ryanko.files.wordpress.com/2011/06/acctcloud-hpls_final.pdf.

[18] Rubinson, Teresa C., A Fuzzy Multiple Attribute Design and Decision Procedure for Long Term Network Planning, Ph.D. dissertation, Polytechnic University, June 1992.