information

Article

Healthcare Professional and User Perceptions of eHealth Data and Record Privacy in Dubai

Fatima Mohamed AlMarzooqi [1], Immanuel Azaad Moonesar [2,*] and Raeda AlQutob [3]

[1] Primary Healthcare Sector, Dubai Health Authority, Dubai P.O. 4545, UAE; Fatmalmarzooqi@dha.gov.ae
[2] Health Administration and Policy, Mohammed Bin Rashid School of Government, Dubai P.O. 72229, UAE
[3] Public Health, School of Medicine, University of Jordan, Amman 11942, Jordan; ralqutob@ju.edu.jo
* Correspondence: immanuel.moonesar@mbrsg.ac.ae

Received: 28 July 2020; Accepted: 21 August 2020; Published: 28 August 2020

Abstract: Introduction: Dubai city made a significant leap forward, which aligns with the vision of leadership, in the region's eHealth services by adopting a unified electronic medical record system across the country. Electronic medical records provide a better, more efficient standard of care and a vital database that will streamline the administrative process and promote better outcomes with less utilization of resources. Medical records form an essential part in patient management and include a variety of patient data information that might be sensitive. Therefore, the primary challenge is to maintain data privacy of the electronic medical records. Objective: Current studies to measure the user and health provider perceptions of electronic medical records data privacy are limited in the region. We aimed to investigate the perceptions of healthcare professionals and healthcare users toward electronic medical records and data privacy in eHealthcare facilities in Dubai. Methods: In this quantitative descriptive study, we explored the perceptions towards electronic medical records and data privacy using an online survey as a data collection tool. The dependent variables were the user and provider perceptions, while the independent variables included gender, nationality, income and age. A random sample of 201 eHealthcare facilities professionals and users was included. Results: The findings of the study revealed that most healthcare professionals and users agreed on the presence of good eHealth data protection practices and privacy principles in Dubai. There was a statistical correlation between the surveyed privacy practice perceptions and gender, nationality and income. However, age had no statistically significant association. Conclusions: These research findings can influence policymakers and stakeholders when developing electronic medical records and data privacy policies and guidelines across the United Arab Emirates' healthcare facilities, in particular, during the implementation of unified electronic medical records. Future research could investigate the effect of the specific demographic variables on the perception of privacy among eHealthcare facility users that might influence electronic medical records and data privacy.

Keywords: eHealth; Dubai; privacy laws; electronic medical records; health policy; healthcare professionals

1. Introduction

eHealth is an inevitable, real-time technological advance that enhances patient-centered communication in the age of globalization. The use of electronic medical records (EMR) offers potential improvements in the legibility and accessibility of medical records among multiple healthcare provider sites [1,2].

Electronic medical records allow the immediate and complete exchange of patient health information. This property can improve the quality and safety of healthcare services, reduce healthcare costs and facilitate research. Electronic records also enhance the safety of healthcare services through strengthening the continuity of care and increasing the documentation accuracy, accessibility of test results and availability of online medication reordering with drug alerts and error notifications [2,3]. However, successful digital healthcare infrastructure, created by an EMR system, requires a better understanding of the healthcare user's views, concerns and experiences, as healthcare professionals are using EMR daily to deliver the services [1]. The benefits of an EMR system must be balanced against the possibility of a potential loss of information privacy and cyber-attacks, which are more prominent than for paper medical records. Patient health information is stored in the system of healthcare providers, insurance companies and government entities for record, references and research purposes. Storing sensitive patient information in the eHealth system can lead to unauthorized access and misuse.

Without the presence of legislation, eHealthcare service users may fear unauthorized access to sensitive personal information and, thus, avoid the use of eHealth services. Therefore, the perception of users is critical to determine their behaviors and interactions with the system. Hence, it is the responsibility of the provider to maintain the privacy of the data through the implementation of proper privacy and liability mechanisms to increase trust in the eHealth system and services provided, including the internet of medical things [1,4,5].

Interviewing healthcare professionals in London showed that there is a superficial level of perception regarding the importance of healthcare system security, which might significantly threaten the integrity of the healthcare system [6]. A cross-sectional study conducted in New Zealand showed that 73.3% of participants were apprehensive regarding the privacy and security of their medical records [7].

A survey conducted in the United States on primary care physicians revealed that the majority of physicians perceived the benefit of electronic health records. However, they reported a primary concern for the privacy and confidentiality of eHealth services [8]. A study conducted on the impact of health disclosure laws on health information exchanges showed that the presence of secure privacy and confidentiality laws that limit disclosure of health information data led to more significant health information exchanges between healthcare facilities [9,10]. Other studies focused on individual attitudes toward electronic health records, indicating that privacy concern was reduced by the perceived effectiveness of regulatory mechanisms and the perceived effectiveness of technological mechanisms, where both showed a positive impact on the trust, while technological mechanisms positively impacted the perceived privacy control and trust [4,11,12].

Electronic medical record users may experience serious financial, social and psychological problems if sensitive information and other determinants of health informatics adoption and diffusion are disclosed [10,13]. A previous study on privacy perception in Dubai was performed during the period 2015–2016, before the EMR implementation at Dubai Health Authority (DHA) began. Privacy protection laws and the public perception of data privacy study showed that most of the survey respondents trusted the eHealthcare services in Dubai, and they did not feel that their data privacy and confidentiality were at risk [13]. There is limited evidence regarding the current use and perception of electronic medical records and data privacy in Dubai. In this study, we investigated the perception of healthcare professionals and healthcare users toward electronic medical records and data privacy in eHealthcare facilities in Dubai after the implementation of electronic medical records for the most significant public healthcare service provider in Dubai, DHA. This study was built on the review of Sarabdeen and Moonesar by replicating their survey [13].

2. Materials and Methods

This quantitative descriptive cross-sectional study investigated the perceptions of healthcare users toward eHealth data and record privacy in Dubai in terms of user perceptions regarding the data protection practices of eHealthcare facilities in Dubai as well as their understanding of the adoption of useful privacy measures. We also investigated the privacy principles offered by healthcare providers and users to maintain data privacy and measured their association with some demographic variables, including gender, age, nationality and income.

Respondents of the research study (the Mohammed Bin Rashid School of Government (MBRSG)) ethics approval number as REC-02-2019 and the DHA ethics approval number as DSREC-SR-01/2019_01) consisted of a sample of eHealthcare facility professionals and users, between January and February 2019. The healthcare professionals included physicians, nurses, paramedics and nutritionists, while the healthcare users represented the patients receiving care from such facilities. The survey inclusion criteria required literacy in Arabic or English. Users who did not speak either English or Arabic were excluded.

The data collection procedure was through a universal link sent by a convenient method through email and social media programs to the citizens and residents of Dubai. At the same time, healthcare professionals were contacted by the primary healthcare sector of DHA using the Qualtrics program. Participation was entirely voluntary, and the participant could stop the survey based on their convenience at any time while answering the survey questionnaire. There was no identifiable information obtained from the participants, and the participants were anonymous. Data collection was carried out over four weeks. By the end date, the collection period survey was closed, and the data were downloaded from the survey platform.

The researchers used email, mobile phone and social media programs to recruit participants; the universal link was sent to different contacts, to reach a maximum number of users in the months of January–February of 2019. After data cleaning, the final number obtained from survey respondents for providers and users was 201. Similar to providers, the users' sampling method was based on volunteer sampling. The survey link had the same message sent to all participants explaining the purpose of the study, the informed consent form and the survey questions. The previous research carried out in Dubai regarding eHealth data privacy was based on a survey as well [13]. Many types of research tackling the same topic area used the survey method, which made the cross-sectional survey approach the best to collect the required data [14–17].

The demographic variables obtained for both users and providers in the survey included gender, age, nationality, employment designation, length of service, type of healthcare sector and income. Nationality measured all nationalities to capture all non-Emirati living in Dubai, considering that Dubai is a multinational city. Nationality was then divided into United Arab Emirates (UAE) and non-UAE. The healthcare sector was divided into public, private and other, as public and private are the two main categories, while other will cover an additional minority if it exists. Income was measured as categorical variables from the highest, which was more than dirhams (AED) 50,000 to the lowest levels, which was below AED 10,000, as at least 30% of the population lies within this group.

The dependent variables (DVs) were obtained through posing three questions; the first was about how the user feels while using the eHealthcare facility regarding their rights, data record accuracy and protection and if they trust and feel comfortable while using the EMRs. The second DV question was regarding the seven privacy principles used to measure the degree of privacy offered by healthcare providers in Dubai to maintain data privacy. The seven principles are the notice principle, choice principle, disclosure principle, security principle, data integrity principle, access principle and enforcement principle. The third DV question was regarding the perception of healthcare users of the right adoption of data privacy measures by healthcare providers in Dubai. The dependent variables were measured against a Likert scale.

Qualtrics is a software for flexibly collecting data to design the survey. The data collected were exported to Microsoft Excel in both forms as coded values and coded text and then exported into Statistical Package for the Social Sciences (SPSS). Data cleaning and screening procedures were applied to the exported SPSS data. After cleaning, a codebook was generated for all variables, the data entry was performed using the codebook, and descriptive tables for demographic data were generated.

Three domains of perceptions were investigated. This was carried out using 25 questions, with 6 for healthcare professional and user feelings regarding data privacy while using the eHealth facility in Dubai, seven for privacy principles and 12 for good provision of privacy and confidentiality of healthcare providers when dealing with patient data. Each question had seven options ranging across Strongly Disagree, Somewhat Disagree, Slightly Disagree, Slightly Agree, Somewhat Agree, Strongly Agree, and Not Applicable. They were given scores of 1, 2, 3, 4, 5, 6, and 7, respectively.

After applying the percentage score, descriptive tables were generated; cross tables regarding the correlations between demographic variables and the principle domains were also generated using SPSS. The statistical significance was calculated, and a p-value of less than 0.05 was considered the cut-off point of significance.

3. Results

In total, 78% of the survey respondents were healthcare professionals, while 22% (n = 44) represented healthcare users (Table 1). The description of demographic characteristics of the participants shows that 82% of the respondents were female while there were 18% male respondents. Approximately 86% of the respondents were 30 years of age or above. In comparison, 14.5% were 20 years of age. Nearly half (52%) of the survey respondents (including users and healthcare professionals) had an income of UAE 30,000 or above (Table 1).

Table 1. The demographic characteristics of the study.

Variable		**n**	**%**
Gender	Female	165	82
	Male	36	18
Age (years)	Below 20	5	2.5
	20–29	24	12
	30–39	86	42.8
	40–49	63	31.3
	Above 50	23	11.4
Respondent	Healthcare user	44	22
	Healthcare professional	157	78
Nationality	UAE	110	55
	Non-UAE	91	45
Income (Dirhams, AED)	Below 10,000	46	23
	10,000–20,000	30	15
	20,000–30,000	42	20
	30,000–40,000	46	23
	40,000–50,000	18	9
	Above 50,000	19	10
Healthcare sector	Public	180	90
	Private	21	10

The survey respondents were divided as 55% Emiratis and 45% expatriates. The expatriate countries of origin included India, Egypt, the Philippines, Yemen, Sudan, Pakistan, the United Kingdom, Jordan, Syria, Comoros, Iran, Iraq, Oman, Palestine, Somalia and the USA. Approximately 90% of the respondents (n = 180) utilized the private healthcare sector, as compared to 21 respondents (10%) who used the public healthcare sector. The healthcare users who reported that the purpose of the last visit to the healthcare institution or clinic included medical follow-up constituted 41%. In comparison, 27.3% used it for medical tests, 18% for emergency visits and 13,6% for regular check-ups (Table 2). On the other hand, healthcare professionals were 62.4% doctors, 27.4% nurses, 2.5% medical assistants, and 1.3% dieticians and nutritionists, while 6.4% were reported as other health-allied professionals, including pharmacists, radiographers and speech therapists. Forty-eight percent of the survey healthcare professionals had more than ten years of working experience within their respective designations (Table 3).

Table 2. Healthcare user purpose of the last visit to the healthcare facility.

Variable		**n**	**%**
Purpose of the last visit	Medical follow-up	18	41
	Medical test	12	27.3
	Emergency visit	8	18.1
	Regular check-up	6	13.6

Table 3. Length of service and designation of healthcare professionals.

Variable		**n**	**%**
	Less than 5 years	45	28
	5–10 years	37	24
	More than 10 years	75	48
Designation	Doctors	98	62.4
	Nurse	43	27.4
	Medical assistant	4	2.5
	Dietician	2	1.3
	Other health allied	10	6.4

3.1. Perception of the Participant on eHealth Privacy

Our findings of the perception of the data protection practice of the eHealthcare provider showed that more than 93% of the survey respondents reported that they were "comfortable when using eHealth services", "the data collected are recorded accurately and precisely" and "they could trust the eHealth services systems offered in Dubai". Ninety-one percent of the survey respondents reported that "they felt secured when using eHealth services". We found that 90% of the user respondents felt that their "data collected are protected", and 89% felt that "their right has not been violated".

Findings of the data privacy principles from the perspective of service providers were as follows in the context of Dubai:

1. Notice principles: This principle explains that the data user must inform the individual that their data are being collected; they also must provide their contact details, the type of disclosed data and if the third party will use the data. Ninety percent of the respondents agreed that this principle was evident.
2. Choice principle: This principle empowers individuals to have the authority to limit the usage of their data to only the collected purpose. Eighty-three percent of the respondents agreed that this principle was evident.
3. Disclosure principle: Data disclosure to the third party must be ensured after informing the subjects, and data should be transferred according to the purpose for which it was initially collected. Eighty-seven percent of the respondents agreed that this principle was evident.
4. Security principle: This principle protects the data from misuse, abuse, unauthorized access and disclosure while dealing with collected data. Ninety-two percent of the respondents agreed that this principle was evident.
5. Data integrity principle: According to this principle, the collected data should be accurate and consistent at all stages; during collection, usage and disclosure. Ninety-two percent of the respondents agreed that this principle was evident.
6. Access principle: According to this principle, the data should be accessible by an authorized individual to amend, delete and modify the data if required, in addition to tracking modification history. Eighty-six percent of the respondents agreed that this principle was evident.
7. Enforcement principle: This principle requires that the data user should provide a precise, transparent mechanism to ensure compliance with data principles. Ninety-two percent of the respondents agreed that this principle was evident.

The survey also included questions related to the providers' perception of the adoption and maintenance of ethical eHealth data privacy standards and practices by the eHealth service provider. The results showed that 95% of the respondents agreed that the service providers, in general, were following the data protection principles to: "maintain personal information", "continuously improve the process of collecting patients information", "continuously update and enhance the networks to the latest technology available" and "record all data and information precisely and accurately". In addition, 94% agreed to the notion of "maintain personal privacy", 93% agreed on "reassure patients that privacy is at its highest", "avoid being the violators of user trust" and implementation of the privacy policy. Over 89% of respondents agreed to statements such as "avoid being the worst privacy offenders", "store all patients' information and data in safe networks" and "have encrypted networks". We found that 84% agreed to the statement, "educate the patients on the standard privacy rules and procedures in place".

The data results also showed that there was a statistical association between the security principle and nationality. Additionally, there was a significant correlation between the access principle and the enforcement principle within the income levels. See Table 4 below.

Table 4. Statistical associations between the perceptions of participants on privacy principles and the practice of providers and users and selected demographic variables.

	Age	**Gender**	**Nationality**	**Income**
Notice principle	0.706	0.524	0.080	0.170
Choice principle	0.736	0.762	0.723	0.829
Disclosure principle	0.662	0.495	0.074	0.420
Security principle	0.710	0.752	0.006 *	0.402
Data integrity principle	0.509	0.081	0.636	0.090
Access principle	0.337	0.926	0.310	0.039 *
Enforcement principle	0.776	0.684	0.169	0.020 *

* *p*-value: significance less than 0.005.

Table 4 shows that there was no statistically significant association between age and gender (users and providers) for all privacy statements. The majority of UAE and non-UAE nationals perceived the presence of security principles, with a *p*-value of 0.006. Across all income level groups, the majority recognized the presence of the access principle, with a *p*-value of 0.039, and perceived the presence of the enforcement principle, with a *p*-value of 0.020.

Table 5 shows that the survey collected the opinion on the presence of the privacy principle at a healthcare facility, and more than 90% of respondents (users and providers) agreed with all the statements regarding the perception of data protection practice of eHealth. In comparison to the previous study [13], more than 80% of the respondents agreed with the following statements: "comfortable when using eHealth services", "secure when using eHealth services" and "the data collected is protected".

Table 5. Percent scores on the perception of data protection practice of eHealth providers in the current study in comparison to the previous study [13].

Perception of Data Protection Practice of eHealth	**Current Findings**	**Previous Study Findings [13]**
Comfortable when using eHealth services	94%	80%
Secure when using eHealth services	92%	80%
The data collected are protected	90%	80%
My rights have not been violated	90%	90%
The data collected are recorded accurately and precisely	92% (*p*-value of 0.031)	90% (no indication)
They trust the eHealth services systems offered	94% (*p*-value of 0.039)	90% (no indication)

p-Value: significance at less than 0.05 (association with the demographic variable income level).

3.2. Discussion/Conclusions

The massive volume of clinical data, new knowledge and advanced clinical tools, as well as integrated and coordinated patient clinical information, created the need for eHealth and electronic medical records. Patient health record data and information are crucial in the healthcare sector. Electronic medical records help to achieve massive cost savings, improve the efficiency and quality of care by increasing accessibility, aid in the provision of coordinated and comprehensive care and reduce medication error [18]. This study (Table 5) showed that there is an increased level of agreement on the data protection practice by an eHealthcare provider as indicated in the results achieved on 11 of the statements measured after EMR was implemented at the Dubai Health Authority. This was true except for the "rights have not been violated" statement, which showed a similar level of privacy perception before and after electronic medical records implementation according to "privacy protection laws and public perception of data privacy, the case of Dubai eHealthcare services [13]". A study on the perception of EMRs by nursing staff in a teaching hospital in India showed that 75% of the nurses were comfortable using the electronic medical records [19] while the results in this study showed a higher level of agreement particularly after the implementation of electronic medical records.

The rated data privacy principles showed an overall reduction in the level of agreement on the presence of privacy principles except for the data integrity and enforcement principle, which increased from 84% to 90% after electronic medical records implementation. A study carried out in the United States (n = 30) with mixed cultures to assess patients willingness to share their information showed that individuals with highly sensitive data were less likely to share their information unconditionally [20,21], especially if there was a lack of consent before data usage [12]. This might provide an insight into the reason behind the reduction in the notice, choice, and disclosure principle levels of agreements.

When the results of this survey were compared with the earlier study that was conducted before EMR implementation [13], the survey findings regarding the providers' opinions on the motives for adopting ethical eHealth data privacy principles by eHealth service providers showed an increased level of agreement, except for statements such as "educate the patients of the standard privacy rules and procedures in place", which remained the same before and after EMR implementation. A study by Gupta et al. (2016) showed that a user's trust could be positively impacted by the perceived effectiveness of the technological and regulatory mechanisms [11]. Respondent perceptions in this study might reflect the level of trust toward eHealthcare facility electronic medical record privacy measures.

In the Sarabdeen and Moonesar study [13], the majority of respondents were from healthcare users, and there was no significant association between all the demographic variables and the privacy principles in the study. In this study, the majority were from the healthcare professional category who are using electronic medical records to manage the patients. In this study, age had no statistically significant association with the different studied elements of privacy. However, there was a statistically significant correlation between income and "the data collected are recorded accurately and precisely" and "they trust the eHealth services systems offered." In addition, there was also a statistically significant relationship between income and the access principles and enforcement principles. The results of this study showed that income might have an impact on the individual perception of electronic medical record privacy in Dubai. A study by O'Donnell et al. showed that persons with personal earnings of more than USD 100,000 annually believed that EMR will improve the security and confidentiality of medical records [15].

There were statistically significant associations between the gender of the electronic medical record providers and "educate the patients of the standard privacy rules and procedures in place", "continually improve the process of collecting patient's information" and "the gender relationship needs to be further studied to understand how it affects users' and providers' perceptions". Regarding nationality, there were statistically significant associations between the nationality of the electronic medical records users and the security principle and "reassuring patients that privacy is at its highest." Another statistically significant association was between nationality and "educate the patients of the standard privacy rules and procedures in place." The results of this study showed that nationality had an impact on the individual perception of electronic medical record privacy in Dubai, similar to a study conducted by Papoutsi et al., which showed that there were differences in the security perceptions between different ethnic groups [14].

Privacy principle applications at various healthcare institutions must be encouraged by policymakers. The presence of EMR data protection, confidentiality, and privacy law will strengthen patient rights. Reserving patient and healthcare professional rights will increase satisfaction. Different areas of data protection and privacy adopted from the Sarabdeen and Moonesar study provide a baseline for healthcare leaders and policymakers [13,21]. The policy implications of those are as follows:

Perception of the data protection practices of eHealthcare providers: This provides insights regarding healthcare users perceptions of eHealth facility practices, and how users and healthcare professionals feel with regard to facility data protection and their rights. The majority of respondents agreed on all statements, and the only variable that affected the results was income. Involving individuals with different levels of income during all phases of policymaking might have an impact and provide more insights into the area discussed.

Perception of participants on adopting good eHealth data privacy practices by eHealthcare providers: This provides an insight into the motives for selecting ethical eHealth data privacy principles by the eHealth service provider. The variables that were associated were gender and nationality. This can be advised by the policymakers to invite and involve UAE nationals and non-nationals as well as both genders to address any issues related to data protection before the implementation of the national unified electronic medical records system.

Perception of participants on the privacy principle practices of eHealthcare providers: Although most participants agreed on the privacy principle practices by eHealth providers, the only variables that had an association were nationality and income. While income may be related to living standards, social status and education, which can explain differentials in privacy perceptions, culture may have a role to play in the understanding of privacy also. Different nationalities represent different cultural backgrounds. This phenomenon should be further explored in future studies. Policymakers should explore this area to further understand why the income and the nationality affected user perceptions of privacy principles through surveys, workshops and interviews during healthcare facility visits and in the community.

Future studies are required to investigate the further effects of specific demographic variables on the perception of privacy among eHealthcare facility users. Additionally, participant responses could be influenced by the questionnaire items, resulting in commonly biased answers. Future researchers should include an in-depth interview method and add the perception of non-eHealth facility users to compare the knowledge of both groups.

Author Contributions: Conceptualization, I.A.M. and F.M.A.; methodology, I.A.M. and F.M.A.; software, F.M.A. and I.A.M.; validation, F.M.A., I.A.M. and R.A.; formal analysis, F.M.A. and I.A.M.; investigation, F.M.A.; resources, F.M.A. and I.A.M.; data curation, F.M.A. and I.A.M.; writing—original draft preparation, F.M.A., I.A.M. and R.A.; writing—review and editing, I.A.M. and R.A.; visualization, F.M.A.; supervision, I.A.M.; project administration, F.M.A. and I.A.M.; funding acquisition, I.A.M. All authors have read and agreed to the published version of the manuscript.

Funding: We would like to acknowledge the Alliance for Health Policy and Systems Research at the World Health Organization for financial support as part of the Knowledge to Policy (K2P) Center Mentorship Program [BIRD Project].

Acknowledgments: The authors would like to acknowledge the support from the Dubai Health Authority and the Mohammed Bin Rashid School of Government, Dubai, United Arab Emirates.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alkureishi, M.A.; Lee, W.W.; Lyons, M.; Press, V.G.; Imam, S.; Nkansah-Amankra, A.; Werner, D.A.; Arora, V.M. Impact of Electronic Medical Record Use on the Patient–Doctor Relationship and Communication: A Systematic Review. *J. Gen. Intern. Med.* **2016**, *31*, 548–560. [CrossRef] [PubMed]
2. White, A.; Danis, M. Enhancing Patient-Centered Communication and Collaboration by Using the Electronic Health Record in the Examination Room. *JAMA* **2013**, *309*, 2327. [CrossRef] [PubMed]
3. Heurix, J.; Karlinger, M.; Neubauer, T. PERiMETER—Pseudonymization and personal metadata encryption for privacy-preserving searchable documents. *Health Syst.* **2012**, *1*, 46–57. [CrossRef]
4. Mou, J.; Shin, D. Effects of social popularity and time scarcity on online consumer behaviour regarding smart healthcare products: An eye-tracking approach. *Comput. Hum. Behav.* **2018**, *78*, 74–89. [CrossRef]
5. Shin, D.; Biocca, F. Health experience model of personal informatics: The case of a quantified self. *Comput. Hum. Behav.* **2017**, *69*, 62–74. [CrossRef]
6. Ondiege, B.; Clarke, M. Health care professionals&rsquo; perception of security of personal health devices. *Smart Homecare Technol. TeleHealth* **2017**, *4*, 35–42. [CrossRef]
7. Prajesh Chhanabhai, A. Consumers Are Ready to Accept the Transition to Online and Electronic Records If They Can be Assured of the Security Measures. 2007. Available online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1924980/ (accessed on 15 March 2019).
8. Anderson, J.G.; Balas, E.A. Computerization of Primary Care in the United States. *Int. J. Health Inf. Syst. Inform.* **2006**, *1*, 1–23. [CrossRef]
9. Idris Adjerid, R. Impact of Health Disclosure Laws on Health Information Exchanges. Available online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3243116/ (accessed on 18 March 2019).
10. Shin, D.-H.; Lee, S.; Hwang, Y. How do credibility and utility play in the user experience of health informatics services? *Comput. Hum. Behav.* **2017**, *67*, 292–302. [CrossRef]
11. Gupta, A.; Patel, V.; Greenes, R. *Advances in Healthcare Informatics and Analytics*, 19th ed; Springer International Publishing: Cham, Switzerland, 2016.
12. Whetten-Goldstein, K.; Nguyen, T.Q.; Sugarman, J. So much for keeping secrets: The importance of considering patients' perspectives on maintaining confidentiality. *AIDS Care* **2001**, *13*, 457–465. [CrossRef] [PubMed]
13. Sarabdeen, J.; Moonesar, I.A. Privacy protection laws and public perception of data privacy. *Benchmarking Int. J.* **2018**, *25*, 1883–1902. [CrossRef]
14. Papoutsi, C.; Reed, J.E.; Marston, C.; Lewis, R.; Majeed, A.; Bell, D. Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: Results from a mixed methods study. *BMC Med. Inform. Decis. Mak.* **2015**, *15*, 1–15. [CrossRef] [PubMed]
15. O'Donnell, H.C.; Patel, V.; Kern, L.M.; Barron, Y.; Teixeira, P.; Dhopeshwarkar, R.; Kaushal, R. Healthcare Consumers' Attitudes Towards Physician and Personal Use of Health Information Exchange. *J. Gen. Intern. Med.* **2011**, *26*, 1019–1026. [CrossRef] [PubMed]
16. Lakbala, P.; Dindarloo, K. Physicians' perception and attitude toward electronic medical record. *SpringerPlus* **2014**, *3*, 63. [CrossRef] [PubMed]
17. Rutten, L.J.F.; Vieux, S.N.; Sauver, J.L.S.; Arora, N.K.; Moser, R.P.; Beckjord, E.B.; Hesse, B.W. Patient perceptions of electronic medical records use and ratings of care quality. *Patient Relat. Outcome Meas.* **2014**, *5*, 17–23. [CrossRef] [PubMed]
18. Wang, S.J.; Middleton, B.; Prosser, L.A.; Bardon, C.G.; Spurr, C.D.; Carchidi, P.J.; Kittler, A.F.; Goldszer, R.C.; Fairchild, D.G.; Sussman, A.J.; et al. A cost-benefit analysis of electronic medical records in primary care. *Am. J. Med.* **2003**, *114*, 397–403. [CrossRef]
19. Pera, N.K.; Kaur, A.; Rao, R. Perception of electronic medical records (EMRs) by nursing staff in a teaching hospital in India. *Int. J. Adv. Med. Health Res.* **2014**, *1*, 75. [CrossRef]

20. Caine, K.; Hanania, R. Patients want granular privacy control over health information in electronic medical records. *J. Am. Med. Inform. Assoc.* **2013**, *20*, 7–15. [CrossRef] [PubMed]
21. Shin, D.; Hwang, Y.; Cheung, C. Integrated acceptance and sustainability evaluation of Internet of Medical Things. *Internet Res.* **2017**, *27*, 1227–1254. [CrossRef]