REVIEW ARTICLE

EMR Access and Confidentiality Based on Patient and Hospital Staff Perspectives

Dhillon K[1], Tan E[2], Akseer R[3], Alhosani MS[3], Ho GF[4], Lim SHE[3,5,*] and Jamaludin ANSJ[1,*]

[1]*Department of Epidemiology and Public Health Medicine, Royal College of Surgeons in Ireland, Perdana University, Block B & D Level 1, MAEPS building, MARDI Complex, Jalan MAEPS Perdana, 43400 Serdang, Selangor Darul Ehsan, Malaysia*

[2]*Royal College of Surgeons in Ireland, 123 St. Stephen's Green, Dublin 2, Ireland*

[3]*Health Sciences Division, Abu Dhabi Women's College, Higher Colleges of Technology, 41012 Abu Dhabi, United Arab Emirates*

[4]*Faculty of Medicine, University of Malaya, 50603 Kuala Lumpur, Malaysia*

[5]*Center for Research Excellence and School of Data Sciences, Perdana University, Block B & D Level 1, MAEPS building, MARDI Complex, Jalan MAEPS Perdana, 43400 Serdang, Selangor Darul Ehsan, Malaysia*

Abstract:

Introductions:

The Electronic Medical Records (EMR) system is a longitudinal electronic record consisting of all the information relevant to a patients' health and well-being, generated by at least one encounter in a healthcare setting. It can be accessed within an institution with multi-level accessibility based on authentication customized to the type of user. Since the EMR system potentiates an organised and holistic medical history specific to a patient, it enables medical professionals to deliver a higher quality of healthcare services.

Aims:

The aims of this study were to understand the global perspective of EMR and its implementation as well as to locate the gaps of knowledge that still existed in the understanding and definition of EMR amongst patients and hospital staff.

Methods:

All major bibliographic databases such as PubMed and Google Scholar and several specialist datasets such as PsycINFO, MEDLINE and EBSCOhost from the previous 10 years (2007-2017) were employed in our search. Paper citations which utilised a reference standard were incorporated for quality assessment. An initial search found 2700 articles however after factoring in the inclusion and exclusion criteria, only 78 articles were included in this review.

Results:

Our findings indicated a discrepancy between the expectation of patients and what was actually practiced. Patient concerns mainly involved easy access of healthcare professionals other than doctors to their EMR in addition to non-medical information. The assumption of confidentiality was expected to be maintained by indifference; however, a good face-to-face explanation cannot be substituted with control over content and access to EMR. In the event of a breach in patient confidentiality, lawsuits against healthcare providers will rise exponentially as patients are now well-informed and more empowered to ask questions regarding the care they are receiving and information being disclosed to other parties.

* Address correspondence to this author at the Department of Epidemiology and Public Health Medicine, Royal College of Surgeons in Ireland, Perdana University, Block B & D Level 1, MAEPS building, MARDI Complex, Jalan MAEPS Perdana, 43400 Serdang, Selangor Darul Ehsan, Malaysia; Tel: +603-89419436; E-mails: annejamaludin@perdanauniversity.edu.my, lerin@hct.ac.ae

Conclusion:

Security of information can be attained with better modelling protocols, end-user training and refresher courses done on a regular basis. Finally, controls of access will need to be implemented *via* passwords and digital signatures.

1. INTRODUCTION

With technological advancements being developed at such a rapid pace, it is of little surprise that Information Technology (IT) is being recognized in the healthcare sector as a vital aspect in enhancing the quality of care delivered and ensuring patient safety [1]. Easy-access to the internet and the vast amount of medical-related information on the web have made patients become more literate and concerned about their symptoms, illnesses, and curative options [2]. For example, in North America, the majority of its population are reliant on the internet for general health education [3, 4]. They also use it as a tool when contemplating decisions about their lifestyle choices, medicines and treatment [3, 4]. One study found that 42% of American citizens keep health records for themselves and other family members, with 87% of these in the paper format [5].

In the United Arab Emirates, the use of EMR system was in existence since 1979, however, in Abu Dhabi, it was fully implemented by Health Authority of Abu Dhabi (HAAD) in 2008 [6]. According to Studies in Health Technology and Informatics (2017), the median Electronic Medical Records Adoption Model (EMRAM) score in 2016 for Dubai was (2.5) which is higher than Australia (2.2), New Zealand (2.3), Malaysia (0.06) and Thailand (0.5) [7, 8]

It is considered that electronic Health (eHealth) technologies have an enormous potential to promote patient participation and improve health outcomes [9]. The Electronic Medical Records (EMR) system is a longitudinal electronic record consisting of all the information relevant to a patients' health and well-being, generated by at least one encounter in a healthcare setting [10, 11]. EMRs have become an ever-present feature within the healthcare industry, with the majority of hospitals in the United States of America adopting it [12 - 15]. Thus, as a product of this digitization, patients are now more likely than ever to accept this system. An individuals' EMR may include information such as: socio-economic background and status, immunization history, laboratory test results, co-morbidities suffered, vital signs, current medication regime, past medical history, and reports of all kinds (*e.g.* radiology report, physician report) [16]. Moreover, this system also aids in integrating and automating the workflow of Healthcare Professionals (HCPs) on multiple levels such as administration, finance and clinicians, all of whom will enable a higher quality of care to be delivered whilst simultaneously enhancing the patient-provider communication [16, 17].

However, recent high-profile EMR security violations reported in the media [18, 19] have made patients more hesitant of the transition to the digital format, regardless of the potential advantages [20, 21]. Their main worry is the confidentiality of their information as it is stored and transferred across the health care system [22 - 24]. This indicates that the implementation of EMR involves many challenges and may result in a fallout of users against EMR, if not addressed immediately. In brief, the challenges include adaptation to changes, knowledge and skills, unstandardized health informatics and inadequate telecommunications infrastructure [25]. Another pressing issue is the effectiveness of an EMR system in protecting the confidentiality of sensitive information (*e.g.* mental health, sexual health) which still remains a grey area and raises a lot of concern [26]. The objective of this work aimed to understand the global perspective of EMR and its implementation. We also aimed to locate the gaps in knowledge that still exists in understanding EMR. Future work includes developing a questionnaire for both hospital staff and patients to assess the current levels of awareness of EMR in the United Arab Emirates and Malaysian settings to gauge the attitudes of people towards confidentiality of EMR.

2. METHODS

2.1. Search Strategy

The evidence for this review was obtained through searches of electronic databases for articles published in scientific journals and manually referring back to the references in those articles within the last 10 years (2007-2017). The three high-yield electronic databases searched were PubMed (monitored by United States National Library of Medicine), EBSCOhost and Google Scholar.

In PubMed, EBSCOhost and Google Scholar, the Medical Subject Heading (MeSH) terms used were: "E-Health", "Electronic Medical Records", "Personal Health Record" and "Patient Health Portal". Articles that are replicate

publications, studies of coding, databases of one variable (*e.g.* prescribing registers, disease registers), letters, editorials, posters and foreign language material (*i.e.* non-English language) were excluded. Only paper citations which utilised a reference standard was included for quality assessment. Furthermore, articles of review that did not provide original data and grey literature that was not formally published were also excluded. The articles that met the inclusion and exclusion criteria were then screened by four independent reviewers. The search process is shown in Fig. (**1**) below:
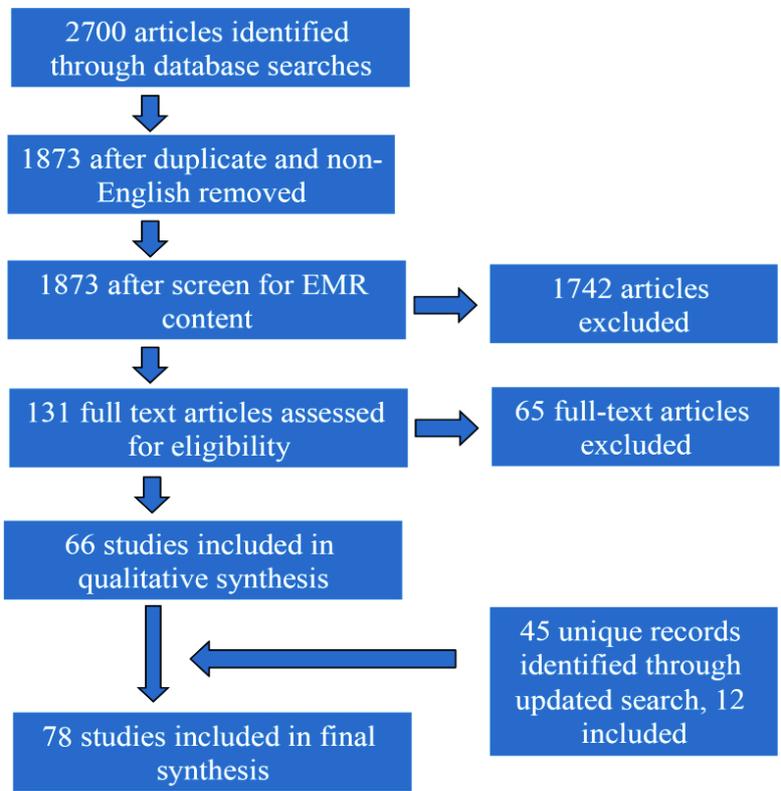

Fig. (1). Flow chart of search strategy processes

3. RESULTS

Across all articles that were selected, several emerging themes were found and are as follows:

Themes	No.	References
Patients' expectation on the content of EMR	7	[27 - 33]
Better regulation for content access of EMR		
-Patient access to their own EMR	9	[34 - 42]
-Patient perspective on HCPs access to their EMR	4	[43 - 46]
-HCPs access to patients EMR	16	[47 - 62]
-HCPs perspective on patient accessing their own EMR	6	[63 - 68]
Issues on confidentiality of EMR	10	[69 - 78]

4. DISCUSSION

4.1. Patients Expectations on the Content of EMR

In a study carried out in England, interviewees were questioned regarding the kind of data they expected to be noted down in their medical records. Two main lines of thought were observed. Firstly, compared to hospital records, patients expected records in general practice to be more detailed in terms of taking personal history including social status, among others. Next, all respondents anticipated that every encounter with a doctor would be recorded [24]. The justifications provided for such a detailed record were for proper diagnosis, safety and continuity of care [27].

Concerns regarding the content have been expressed in most studies of patient attitudes toward personalised EMR, especially when it involves data regarding mental and sexual health [28]. In one study aimed to assess the amount of information patients would be comfortable for their EMR to share on a national platform, the items they identified that they would not want to be shared were generally regarding issues of pregnancy, fertility, birth control, mental well-being and sexual health [29].

When it comes to matters regarding abortion in Malaysia, Section 312 of the Penal Code states that an abortion can only be allowed in instances that pose a significant risk to the pregnant woman's life or if signs of detriment to her mental health and physical well-being are present [30]. Even though termination of pregnancies is a vital part of a patient's history, many people are still uncomfortable in disclosing such information due to the societal taboo placed on this issue thereby making it more difficult for them to accept the concept of EMR. While there are instances where terminations can be carried out, limitations to the law do exist. According to the Malaysian Penal Code, the doctor is the sole individual that decides whether or not to follow through with a termination [30]. However, based on a study carried out in 2007 by the Reproductive Rights Advocacy Malaysia (RRAAM), they found that of the 120 HCPs surveyed, only 57% were aware that a termination of pregnancy is legal in special situations [31]. Without healthcare professionals being well-informed on these issues, patients will feel less comfortable sharing such information on their EMR as it may come across as a crime. The same general perception was seen in countries where abortion is legal.

Furthermore, the stigma associated with mental health has become a major barrier in providing care to people with this disorder [32]. These patients are seen in low regard, leading to discrimination and reluctance when providing treatment for physical illness in those who are mentally ill [32]. People with mental disorders tend to lose their self-confidence and over time reinforce the stereotype image of the person with mental illness that takes no effort in self-care and sustenance [32]. This pre-conceived notion strengthens the stereotype whereby issues regarded to be sensitive or embarrassing, that can have an effect on how an individual is treated by others including HCPs, have a higher likelihood of being omitted by patients. Highlighted issues and patient hesitance in sharing such information in the EMR are listed in Table **1**.

Table 1. Issues which patients are hesitant to disclose in their EMR.

Health issue	Pertaining to	Notes	References
Pregnancy	Termination of pregnancy	Apart from special circumstances, abortion is illegal in Malaysia, making it a social taboo for people to share this kind of information. In countries where abortion is legal, patients feel more comfortable in sharing such information if their health care professionals were well-informed on such issues.	[29 - 31]
Mental Health	Anxiety/Depression	Those diagnosed with mental disorders are often discriminated when it comes to the provision of care.	[28, 32]
Sexual Health	Referral to sex therapy / Lack of libido / Emergency/Routine contraception	Any issue relevant to the sexual well-being of an individual, including but not limited to the use of contraception is stereotyped as promiscuous behaviour.	[28, 29]
Others	Overdose attempt / Medication history / Life insurance	Patients universally are afraid of reporting significant health information in the fear of their insurance company retracting their current policy or increasing their annual premium rate to an unaffordable amount.	[28, 29]

Since societal stigma is very prevalent locally (in Malaysia), the use of EMR does not meet patient expectations in these areas, hence majority would be unwilling to share sensitive information as they do not know who will have access to their information and what the consequences of disclosure are [33].

4.2. Better Regulation Required for Content Access to Medical Records

4.2.1. Patients' Access to Their Own EMR

The patient internet portal is a recent technological development which provides individuals with access to medically-related information and also clinical care [34]. Several portals enable patients to access their personal EMR encompassing doctor's notes, test results and the ability to electronically message their doctors [34]. This creates an avenue for many benefits not only for clinicians but also their patients. For example, patients can take advantage of their access to a significant amount of legitimate health information and data to manage their diseases and improve their health [35].

In the U.A.E for example, the Ministry of Health and Prevention (MOHAP) has revealed the launch of its new Smart Patient Portal Direct Booking system. Under the new implementation, appointments made through direct booking

are now available for Smart Patient Portal users who visit some health centres. The user receives a short text message (SMS) to confirm the booking, as a part of an e-services package that provides a comprehensive medical record that includes laboratory tests, medical reports and list of medications taken. This aids in facilitating access to health data from smart devices [36].

The portal in the U.A.E allows patients to directly see their health records anytime, anywhere. Results of their medical consultations are directly posted to the portal as soon as they become available. This is made possible through the "Wareed" system, which is implemented in virtually all of the Ministry's healthcare facilities and hospitals. The system offers a safe and cost-friendly network in agreement with the highest quality of standards. Under the system, medical reports can be downloaded and saved to the patients' personal computers. Persons can also easily print their records and look through details of their future appointments for scheduling in their `own calendars [36].

Other advantages include a decline in errors of medical nature, improving the standard of care provided as well as various enhancements regarding patient-related matters that encompass the appropriateness of care [37]. Interestingly, however, growing enthusiasm regarding the access and use of a portal is related to displeasure with the doctor-patient relationship, including dissatisfaction with communication skills, failure to build rapport, and the inability to obtain important and relevant medical information [38].

A critical benefit of EMRs is that they create an ongoing link between doctor and patient, which transforms the dynamics of communication from episodic to continuous, hence significantly reducing the time to address problems that may arise [35]. One study carried out in Chicago, USA found that 90% of their participants (95/106) were satisfied with their physician using EMR whereby 59% (63/107) admitted that the digital programme have an affirmative effect on their relationship in a positive way while only 7% (8/108) believed that the EMR served as a hindrance to the communication with their doctors [39]. Hence, with such a system in place, it would allow patient preference to take precedence. Using the EMR will help standardise the collection of medical history, allowing linkage of records across hospitals, aid insurance companies to expedite approval of finance for medical purposes and improve the management of national epidemiologic records to mitigate health issues as a whole for research focus and budgetary planning.

When it comes to the general accessibility of these portals and medical records, there are a few issues that act as limitations. Among them are organisational resources (lack of computers, internet provision, computer training), nurses' individual characteristics (lack of time for patients, low motivation to use computers), patient-related factors (limited literacy and e-health literacy, inadequate social support) and portal-related factors (demands better navigation skills than most patients have) [40, 41].

One study in the United States found that there was a lower probability for older patients with poor educational backgrounds to use the patient portal in order to access their EMR when compared to younger, more educated patients [37]. This suggests that differing levels of acceptance and adaptability as well as issues with accessing the internet play a part in the social disparity of EMR usage [41]. Interestingly, however, when comparing groups who had sufficient internet and computer access, older patients had a higher chance of using their EMR and this may be because of issues related to their health and well-being [41]. A study concluded that EMRs have the unique ability to improve the self-management of patients with multiple chronic conditions and enhance patient engagement [42]. However, additional measures are needed to make certain that the EMR is accessible to these group of patients [42].

Recently, studies have found good early adoption rates and usage of EMR during the initial years of its deployment amongst a population of primarily low-income, especially among those with chronic diseases [33]. The discrepancy in access to and usage of the portal were present, therefore a more concentrated attempt is required to ensure that portals are usable for and used by minority groups so that all patients benefit equally from these advancements [33].

4.2.2. Patients' Perspective on HCPs Access to Their EMR

Another important aspect of EMR accessibility that needs to be discussed is patients' views on who, what and how much other people can access and use. One article states that the fundamental threat of such access is not the excessive information for the patient or the danger to medical hegemony but rather to vulnerable people that might not be able to control record access [43]. For example, would a victim of domestic abuse really be able to prevent the perpetrator from accessing their records to find out their history or what they may have said to the doctor about them [43]? However despite this, patients are generally positive towards the idea of data from their records (anonymous and identifiable) being used in research for the 'greater good' [44].

One study showed that a patient would support the notion of sharing their de-identified EMR if the sole purpose was for research, though they admitted to being unclear regarding data usage, rendering it challenging to obtain trust [37]. Despite being worried about their data being misused by the wrong parties (*e.g.* insurance agencies), 98% of respondents believed that the benefits of sharing healthcare information outweighed the uncertainty [37].

Another study found that patients have a desire to share their electronic health information but they would want complete control over the kind of information and level of access that is shared with specified people [45]. Respondents were more inclined to share access to medication lists and prescription refill activities rather than their communications with care providers [45]. Also, a research carried out in the UK on patients attitudes towards informed consent models of EMR reported that 91% of their respondents deemed it compulsory for consent to be explicitly taken before their identifiable health records were accessed by healthcare professionals at any level and/or researchers [46]. Interestingly, only 49% of respondents in this study expected to be asked for consent prior to accessing their de-identifiable medical records [46].

All of this indicates that patients want the ability to selectively share access to their EMR, so that they can grant access to 1 or more persons while being specific as to what information said person can view and what kinds of activities he/she can perform on behalf of the patient [17]. The most important aspect of accessing a patient's EMR is to explain clearly the purpose of use and document that consent was obtained.

4.2.3. HCPs Access to Patients' EMR

Since the implementation of Health Information System (HIS) in some hospitals in Malaysia, EMR has improved accessibility to medical records, making healthcare delivery more efficient. It has removed the need for physical storage, search and retrieval of patient chart, as the patient's information can be accessed using the computers available at all workstations [47 - 49]. The storage of patient information electronically also eliminates issues regarding losing of charts [49]. With the benefits of convenient access to patient information, HCPs are able to act immediately and provide prompt healthcare to a patient. This is especially useful in emergency situations where the patient is unable to provide necessary information due to extreme injury/illness [16]

However, the lack of access to the system is ironically one of the barriers to the adoption of EMR by HCPs. Technological barriers have arisen following the transition of paper-based records to electronic ones. The most commonly reported limitations associated with access are inadequate computer literacy/skills, lack of computer/hardware, computer crashes and power failure [50, 51]. Computer literacy is a major factor in the acceptance of EMR and it is correlated with user satisfaction [52, 53]. Those with inadequate computer skills found the system time consuming to use and believed that it would disrupt clinical encounters [52]. The EMR contains a range of functions that require computer skills such as good typing proficiency and the ability to navigate around the system in order to provide smooth workflow [54]. But, EMR providers seem to underestimate the level of skills needed from the users to use the system [50]. Two studies have found that by providing a mandatory computer-training programme to the HCPs, computer literacy was significantly improved and further increased the overall users' satisfaction with EMR [55, 56]. Computer training helps HCPs to gain a better understanding of the system by introducing features and functions with which they may not be familiar with [57].

Despite quick access to electronic data *via* the EMR, access needs to be limited to protect patient's privacy and to maintain trust between healthcare providers and patients. Therefore, confidentiality of medical records is actively being maintained by two mechanisms, audit trails and access control. Audit trails record the user information, such as the person, date, time and circumstance when data is accessed [58]. It serves to detect security violations, recreate security incidents and prevent future reoccurrence [58]. In December 2011, the Ministry of Health of Malaysia published a user access control policy and guidelines for EMR to ensure the protection of patient's confidentiality and to guide the design, custody and use of the clinical information system. It serves as a yardstick for all healthcare facilities in Malaysia to create the operational policy and procedures for access control [58].

A healthcare setting usually consists of multi-disciplinary teams, thus, it is important to set clear definitions as to who shall have access to patient information and the restrictions on the use of patient's information. Patient data use is not limited to HCP; it is also used for purposes other than direct patient care. Hence, users are categorised into primary and secondary. Primary users are those who use patient information for the management of patient's health. Secondary users are those who use patient information for other purposes, such as, audits, quality management, research, education *etc* [58]. Secondary use of medical records is also subjected to user access control policy [58]. The rules and restrictions

to secondary use of patient information are listed below:

    i. Access to data extractions shall be given with restrictions and cautions.

    ii. Patient data can only be given to a third party with patient's consent.

    iii. Discharge summaries shall be given in the case where patient agrees to seek treatments from other practitioners.

    iv. Patient data shall be depersonalized for the purpose of audits, quality management *etc*.

    v. For the purpose of research, the relevant head of departments, medical research/ facility research ethics committee, shall decide the amount of data that can be accessed.

    vi. For the purpose of education, consent shall be obtained from patients.

The user control matrix defines specific user roles and their level of accessibility to the medical records in a standard operating environment. For example, doctors that are responsible for patient care are allowed to read demographic data, read and edit clinical data but have no access to financial bills of the patient that he/she is treating within the department. Some roles are allowed to override the access control in cases like emergency situations, on call or referred patient to his/her department. But, they will be required to fill in the reasons and the system will automatically send an alert to the director of facility regarding the override of access [58].

Access control may also be able to prevent unauthorized access to certain extent, but this alone is seldom enough to ensure information security [59]. Evidence has shown that the number of incidents related to information security is increasing, despite the investments in technology-based solutions [59]. These incidents are closely related to the level of competence and conscience of the people using the technology. Data breach due to human can happen in 2 ways, one is by unintentional negligence as a result of oblivion to the security guidelines and the consequences of their work; another is by an intentional human violation of information security [60]. Hence, staff's compliance with the policy and their upholding of ethical values are also essential in maintaining the confidentiality of patient's information [61]. In a study carried out in Malaysia, healthcare professionals were interviewed about their views' on the current privacy mechanisms. Many have expressed their needs for a clear policy guideline, which indicate that most HCPs are unaware or have very little knowledge of the access control policy [62]. Without the proper knowledge of the operation procedures, human misconduct/malpractice could easily happen, attributing to data breaches unintentionally.

This calls for healthcare institutions to prioritise setting clear information on security policies, to ensure compliance from all healthcare staffs in addition to raising awareness on the importance of maintaining patient's confidentiality.

4.2.4. HCPs Perspective on Patient Access to EMR

Healthcare professionals, especially doctors' view on whether the patient should have access to their own medical records have been expressed in several studies. Although doctors' opinions on patient access vary across different studies, they are generally positive on the idea of patient reading their medical records [63 - 65] Firstly, doctors found that by allowing the patient to access their notes, it promotes transparency that strengthened the doctor-patient relationship, enhanced mutual trust and encourage communication during consultations [64]. Patients reportedly seemed more empowered and satisfied [64]. Secondly, doctors noticed a change in approach to documenting sensitive information like substance abuse, mental health issues, weight issues *etc*. This is to avoid evoking negative feelings in patients with overtly direct words [64]. Thirdly, medical records could serve as a tool to educate patients on their health and conditions, encouraging them to engage in their own care [64, 66]. Two studies found that more than half of their patients who had access to doctors' notes has reported improved adherence to medical regimens as the notes act as a reminder for the patient to take their medicine [64, 67]. However, doctors are concerned that uncensored honesty to patients may cause unnecessary alarm and anxiety [65]. Moreover, doctors are often self-conscious about the possible errors and typos in their notes, especially on busy days, and the potential repercussions of these mistakes [65]. There are benefits and drawbacks on granting patient access to their medical records. Nevertheless, it is HCPs' professional and ethical onus to act in the patient's best interest and choose how to inform his/her patient and decide on the appropriate amount of information disclosure [68].

4.3. Issues on Confidentiality of EMR (Inclusive of Legal Aspects)

There are two main objectives in attaining medical confidentiality. Firstly, it is aimed to protect the privacy of a patient thereby preventing them from feeling vulnerable or shamed [27]. Secondly, the doctor-patient relationship is a platform to establish an avenue for honest exchange [27]. It is, admittedly extremely challenging to preserve confidentiality in a modern-day technological health care system delivered by multidisciplinary teams. The apparent

inconsistency is attributed to the differing opinions within the profession and contrasting national policies [69]. Additionally, it may also be due to the disparity in the relative values placed upon the autonomy of a patient, societal benefit from usage of personal medical information and protection of the "innocent other" [69]. On one end of the spectrum, cogent arguments are made for absolute confidentiality [70]; an argument that effectively results, as in France, in a criminal offence if such confidentiality is breached [71]. At the other end of the spectrum, people argue for the complete dismissal of the duty of confidentiality [72]; for example, in England and Wales, the current stance taken is that confidentiality is not absolute. When the doctor-patient relationship is bounded by a fee-for-service or similar agreement, a condition of the contract, usually implied by law, states that it is compulsory for a doctor to protect the privacy of information a patient discloses on the principle of seeking medical attention (e.g. diagnosis, therapy) [73]. Moreover, it dictates that the other medical staff who may be involved in managing a patient are in no way allowed to breach this confidentiality [73].

There are several ways in which telemedicine (e-health) is given moral direction (69). Professional code of ethics have evolved within almost all professions related to healthcare, designed in a way such that they are almost identical to the fundamental legal obligations bonded to that profession; non-maleficence (do no harm) and respecting patient autonomy [74]. There are multiple issues related to telemedicine that play an important role in providing a sense of morality to healthcare. These issues require national guidelines and public policies since having a moral direction is vital in developing an excellent policy [74]. Table **2** highlights some of the various legal and ethical issues relevant to telemedicine [74].

Table 2. Legal and ethical issues in telemedicine. [Adapted from Legal and Ethical Issues in Telemedicine Article, 2006].

Issues that are fundamental to telemedicine **Ethical fundamentals** - Autonomy and consent, confidentiality and other aspects of the patient-professional relationship, non-maleficence and beneficence, justice and access
Issues mostly affecting the use of telemedicine **Using and sharing health information** - Consent to information sharing, confidentiality, privacy and data protection, information security management **Responsibility, liability and good practice** - Duty of care, registration and training, indemnity insurance, clinical governance and risk management **Guidelines, protocols and best practice** - Evolution, provenance and content of published guidelines, standards and protocols
Issues mostly affecting the supply of telemedicine **Supplying telemedicine services** - Directives on Electronic Commerce and Distance Selling, advertising of medical and pharmaceutical products, media and broadcasting regulations **Standards and interoperability** - 'New Approach' Directives, standards bodies, obligations relating to procurement by public bodies **Medical devices, product liability and safety** - Medical devices regulations, CE marking, FDA approval, Directives on Product Liability and General Product Safety **Intellectual property rights** - Copyright, patents, trademarks, design rights, passing off and other infringements, exploitation

The implementation of the Data Protection Act 1998 (DPA) [75], together with the Human Rights Act 1998, resulted in a shift of control regarding individual data. Now, the data subject (*i.e.* patient) legally owns all the information that encompasses personal data in its entirety. Table **3** illustrates the principles that encompass the Data Protection Act 1998.

Under common law, the duty of medical confidentiality is not absolute. Circumstances do exist whereby a breach of confidentiality is justified, including statutory cases requiring confidential data to be disclosed [76]. If a patient is deemed competent enough to provide consent (i.e. of sound mind to understand and process the possible detriments and consequences of disclosure) then it is within the law to legally waive confidentiality [76]. In fact, the first principle of the Data Protection Act 1998 (DPA) has incorporated the common law of confidentiality whereby all data that is considered personal to the patient, including medical data, must be processed justly [76]. In instances that the private information is not protected by the DPA, the common law of confidentiality continues to do so (*i.e.* an individual's thoughts and/or habits remain protected) [76]. The Irish Medical Council has four instances in which exceptions can be made to waive confidentiality without the consent of the patient:

Table 3. The 8 data protection principles of the Data Protection Act, 1998. [Adapted from: Confidentiality, No Blame Culture article, 2006].

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. 4. Personal data shall be accurate and, where necessary, kept up to date. 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. 6. Personal data shall be processed in accordance with the rights of data subjects under this Act. 7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. 8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. **Conditions relevant to the first principle** Personal data should only be processed fairly and lawfully. In order for data to be classed as 'fairly processed', at least one of these six conditions must be applicable to that data (Schedule 2). 1. The data subject (the person whose data is stored) has consented ("given their permission") to the processing; 2. Processing is necessary for the performance of, or commencing, a contract; 3. Processing is required under a legal obligation (other than one stated in the contract); 4. Processing is necessary to protect the vital interests of the data subject; 5. Processing is necessary to carry out any public functions; 6. Processing is necessary in order to pursue the legitimate interests of the "data controller" or "third parties" (unless it could unjustifiably prejudice the interests of the data subject).

1. When ordered in a court of law by Judge or by a Tribunal established by an Act of Parliament.
2. To safeguard a patients' personal interest.
3. To maintain societal welfare.
4. To protect others from third party harm.

One study carried out to assess the general attitudes towards privilege found that, 37/42 (88%) responses supported the notion of professional privilege between doctors and patients, but 36/42 (86%) felt that it should not be absolute and 41/42 (88%) advocated that there should be a right to disclose information in certain circumstances, so long as there was adequate protection for those involved [77].

Another survey of 5331 participants in West London, UK found that if their health records were a part of a national EMR system, 79% of participants admitted to have worry and doubt over its security [78]. At the point in which this study was done, 71% felt that the National Health Service (NHS) would not be able to ensure the confidentiality of their EMR. Nearly half (47%) of the respondents felt that compared to EMRs, the current way in which their health records were being held were safer and more secure [78]. Regardless of all the doubt over the implementation of EMR, 55% of respondents would still support the development, while only 12% would completely reject national EMR system [78]. Concerns regarding the security risks associated with EMRs prove the need for higher levels of social awareness and engagement initiatives, whilst simultaneously building reliable privacy and security mechanisms related to health information sharing [78]

When it comes to confidentiality as a duty, it is relative in nature. There are no such guidelines explaining every ethical or legal aspect of confidentiality of EMR. Breach of confidence may have dire implications, especially to the relationship between physician and patient, however, sometimes, the disclosure is of paramount importance to avoid detrimental consequences to the patient itself and/or society in general. The most important aspect, however, is to always maintain the integrity of the patient and respect them. In current times, it is important to break the assumption that sharing data *via* the EMR system automatically increases its vulnerability. Patients need to be educated that the EMR may also act as a protective hub for their information, prioritising confidentiality and only releasing information that is necessary, and nothing more.

CONCLUSION

The findings of this review exploring the perspective of patients to the confidentiality of EMR highlighted a discrepancy between the expectation of patients and what actually happens in practice. Majority of patients were uninformed regarding the issue that HCPs apart from doctors had easy access to their personal EMR. There were also worries concerning the access doctors' had whilst majority expected that none of the administrative, financial or other

staff should be provided access. Another issue that was brought to the discussion is the recording of information that is not medically related to the EMR. There seemed to be hope that de-identifiable EMR of patients would not be misused and/or mishandled by those with access, thereby maintaining confidentiality by indifference. A good face-to-face explanation is still preferred over full control of content and access to EMR; patients were optimistic about building a strong doctor-patient relationship.

It is imperative for clinicians and the EMR team to work hand-in-hand in protecting the confidentiality of all patients. If there is a compromise in patient confidentiality, lawsuits against healthcare providers will rise exponentially as patients are now well-informed and more empowered to ask questions regarding the care they are receiving. Patient associations have to be more aware of such issues and have adequate technological advice. Security of information can be attained with better modelling protocols for risk and vulnerability. End-user training and refresher courses must be done more efficiently and it should be compulsory for password/digital signature requirements to obtain access.

CONSENT FOR PUBLICATION

Not applicable.

CONFLICT OF INTEREST

The authors declare no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENTS

REFERENCES

[1]   Gill R, Borycki EM, Eds. The use of case studies in systems implementations within health care settings: A scoping review. ITCH 2017.

[2]   Archer N, Fevrier-Thomas U, Lokker C, McKibbon KA, Straus SE. Personal health records: A scoping review. J Am Med Inform Assoc 2011; 18(4): 515-22.
[http://dx.doi.org/10.1136/amiajnl-2011-000105] [PMID: 21672914]

[3]   Bliemel M, Hassanein K. Consumer satisfaction with online health information retrieval: A model and empirical study. E-serv J 2007; 5(2): 53-84.
[http://dx.doi.org/10.2979/esj.2007.5.2.53]

[4]   Rideout V NT, Kitchman M. e-Health and the Elderly: How seniors use the internet for health information. Kaiser Family Foundation 2005.

[5]   H T. Two in five adults keep personal or family health records and almost everybody thinks this is a good idea. Health Care News 2004.

[6]   Al Alawi S, Al Dhaheri A, Al Baloushi D, Al Dhaheri M, Prinsloo EA. Physician user satisfaction with an electronic medical records system in primary healthcare centres in Al Ain: A qualitative study. BMJ Open 2014; 4(11): e005569.
[http://dx.doi.org/10.1136/bmjopen-2014-005569] [PMID: 25377010]

[7]   El-Hassan O, Sharif A, Al Redha M, Blair I. Tracking the implementation of electronic medical records in Dubai, United Arab Emirates, using an adoption benchmarking tool. Stud Health Technol Inform 2017; 245: 64-8.
[PMID: 29295053]

[8]   El-Hassan O, Sharif A, Al Redha M, Blair I. Tracking the implementation of electronic medical records in Dubai, United Arab Emirates, using an adoption benchmarking tool. Stud Health Technol Inform 2017; 245: 64-8.
[PMID: 29295053]

[9]   Barello S, Triberti S, Graffigna G, *et al.* eHealth for patient engagement: A systematic review. Front Psychol 2016; 6: 2013.
[http://dx.doi.org/10.3389/fpsyg.2015.02013] [PMID: 26779108]

[10]   Ismail A, Jamil AT, Rahman AFA, Bakar JMA, Saad NM, Saadi H. The implementation of Hospital Information System (HIS) in tertiary hospitals in malaysia: A qualitative study. Malays J Public Health Med 2010; 10(2): 16-24.

[11]   Hassan R. Implementation of total hospital information system (this) in malaysian public hospitals: Challenges and future prospects. International Journal of Business and Social Research 2012; 2(2): 33-41.

[12]   Adler-Milstein J, DesRoches CM, Furukawa MF, *et al.* More than half of US hospitals have at least a basic EHR, but stage 2 criteria remain challenging for most. Health Aff (Millwood) 2014; 33(9): 1664-71.
[http://dx.doi.org/10.1377/hlthaff.2014.0453] [PMID: 25104826]

[13]   DesRoches CM, Charles D, Furukawa MF, *et al.* Adoption of electronic health records grows rapidly, but fewer than half of US hospitals had at least a basic system in 2012. Health Aff (Millwood) 2013; 32(8): 1478-85.
[http://dx.doi.org/10.1377/hlthaff.2013.0308] [PMID: 23840052]

[14]   Furukawa MF, Patel V, Charles D, Swain M, Mostashari F. Hospital electronic health information exchange grew substantially in 2008-12. Health Aff (Millwood) 2013; 32(8): 1346-54.

[http://dx.doi.org/10.1377/hlthaff.2013.0010] [PMID: 23918477]

[15]   Mennemeyer ST, Menachemi N, Rahurkar S, Ford EW. Impact of the HITECH Act on physicians' adoption of electronic health records. J Am Med Inform Assoc 2016; 23(2): 375-9.
[http://dx.doi.org/10.1093/jamia/ocv103] [PMID: 26228764]

[16]   Noraziani K. An overview of electronic medical record implementation in healthcare system: Lesson to learn. World Appl Sci J 2013; 25(2): 323-32.

[17]   Mohan J, Razali Raja Yaacob R. The Malaysian Telehealth Flagship Application: A national approach to health data protection and utilisation and consumer rights. Int J Med Inform 2004; 73(3): 217-27.
[http://dx.doi.org/10.1016/j.ijmedinf.2003.11.023] [PMID: 15066550]

[18]   Abelson RCJ. Data breach at Anthem may forecast a trend. The New York Times 2015 .

[19]   K W. Hospitals aren't the only ones bleeding stolen health records. Atlantic 2015.

[20]   Ancker JS, Silver M, Miller MC, Kaushal R. Consumer experience with and attitudes toward health information technology: A nationwide survey. J Am Med Inform Assoc 2013; 20(1): 152-6.
[http://dx.doi.org/10.1136/amiajnl-2012-001062] [PMID: 22847306]

[21]   Kwon J, Johnson ME, Eds. The market effect of healthcare security: Do patients care about data breaches?. WEIS 2015.

[22]   Ancker JS, Brenner S, Richardson JE, Silver M, Kaushal R. Trends in public perceptions of electronic health records during early years of meaningful use. Am J Manag Care 2015; 21(8): e487-93.
[PMID: 26625503]

[23]   Patel V, Hughes P, Savage L, Barker W. Individuals' perceptions of the privacy and security of medical records. ONC Data Brief 2015; p. 27.

[24]   Patel V, Beckjord E, Moser RP, Hughes P, Hesse BW. The role of health care experience and consumer information efficacy in shaping privacy and security perceptions of medical records: National consumer survey results. JMIR Med Inform 2015; 3(2): e14.
[http://dx.doi.org/10.2196/medinform.3238] [PMID: 25843686]

[25]   Abd Ghani MK, Bali RK, Naguib RN, Marshall IM, Wickramasinghe NS. Electronic health records approaches and challenges: A comparison between Malaysia and four East Asian countries. Int J Electron Healthc 2008; 4(1): 78-104.
[http://dx.doi.org/10.1504/IJEH.2008.018922] [PMID: 18583297]

[26]   Ghazvini A, Shukur Z. Security challenges and success factors of electronic healthcare system. Procedia Technology 2013; 11: 212-9.
[http://dx.doi.org/10.1016/j.protcy.2013.12.183]

[27]   Carman D, Britten N. Confidentiality of medical records: The patient's perspective. Br J Gen Pract 1995; 45(398): 485-8.
[PMID: 7546873]

[28]   Pagliari C, Detmer D, Singleton P. Potential of electronic personal health records. BMJ 2007; 335(7615): 330-3.
[http://dx.doi.org/10.1136/bmj.39279.482963.AD] [PMID: 17703042]

[29]   Powell J, Fitton R, Fitton C. Sharing electronic health records: The patient view. Inform Prim Care 2006; 14(1): 55-7.
[PMID: 16848967]

[30]   Malaysian penal code act 574 (2015).

[31]   Joint stakeholder submission on sexual and reproductive rights in Malaysia, (October 2013).

[32]   Sartorius N. Stigma and mental health. Lancet 2007; 370(9590): 810-1.
[http://dx.doi.org/10.1016/S0140-6736(07)61245-8] [PMID: 17804064]

[33]   Weingart SN, Rind D, Tofias Z, Sands DZ. Who uses the patient internet portal? The PatientSite experience. J Am Med Inform Assoc 2006; 13(1): 91-5.
[http://dx.doi.org/10.1197/jamia.M1833] [PMID: 16221943]

[34]   Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. J Am Med Inform Assoc 2006; 13(2): 121-6.
[http://dx.doi.org/10.1197/jamia.M2025] [PMID: 16357345]

[35]   Menachemi N, Collum TH. Benefits and drawbacks of electronic health record systems. Risk Manag Healthc Policy 2011; 4: 47-55.
[http://dx.doi.org/10.2147/RMHP.S12985] [PMID: 22312227]

[36]   Ministry of health and prevention unveils new smart patient portal direct booking system: AL press 2016. Available from: http:// www.al-press.com/ index.php/ en/government-ngo/ government/ 4451-ministry-of-health -and-prevention- unveils-new-smart- patient-portal-direct-booking -system.

[37]   Zickmund SL, Hess R, Bryce CL, *et al.* Interest in the use of computerized patient portals: Role of the provider-patient relationship. J Gen Intern Med 2008; 23(1)(Suppl. 1): 20-6.
[http://dx.doi.org/10.1007/s11606-007-0273-6] [PMID: 18095039]

[38]   Lee WW, Alkureishi MA, Ukabiala O, *et al.* Patient perceptions of electronic medical record use by faculty and resident physicians: A mixed methods study. J Gen Intern Med 2016; 31(11): 1315-22.
[http://dx.doi.org/10.1007/s11606-016-3774-3] [PMID: 27400921]

[39]   Koivunen M, Hätönen H, Välimäki M. Barriers and facilitators influencing the implementation of an interactive Internet-portal application for patient education in psychiatric hospitals. Patient Educ Couns 2008; 70(3): 412-9.
[http://dx.doi.org/10.1016/j.pec.2007.11.002] [PMID: 18079085]

[40]   Sarkar U, Karter AJ, Liu JY, *et al.* Social disparities in internet patient portal use in diabetes: Evidence that the digital divide extends beyond access. J Am Med Inform Assoc 2011; 18(3): 318-21.
[http://dx.doi.org/10.1136/jamia.2010.006015] [PMID: 21262921]

[41]   Greenberg AJ, Falisi AL, Finney Rutten LJ, *et al.* Access to electronic personal health records among patients with multiple chronic conditions: A secondary data analysis. J Med Internet Res 2017; 19(6): e188.
[http://dx.doi.org/10.2196/jmir.7417] [PMID: 28576755]

[42]   Ancker JS, Barrón Y, Rockoff ML, *et al.* Use of an electronic patient portal among disadvantaged populations. J Gen Intern Med 2011; 26(10): 1117-23.
[http://dx.doi.org/10.1007/s11606-011-1749-y] [PMID: 21647748]

[43]   BH M. Vulnerable people have most to lose from online access. BMJ 2007; 334: 599.

[44]   Clerkin P, Buckley BS, Murphy AW, MacFarlane AE. Patients' views about the use of their personal information from general practice medical records in health research: A qualitative study in Ireland. Fam Pract 2013; 30(1): 105-12.
[http://dx.doi.org/10.1093/fampra/cms036] [PMID: 22850249]

[45]   Zulman DM, Nazi KM, Turvey CL, Wagner TH, Woods SS, An LC. Patient interest in sharing personal health record information: A web-based survey. Ann Intern Med 2011; 155(12): 805-10.
[http://dx.doi.org/10.7326/0003-4819-155-12-201112200-00002] [PMID: 22184687]

[46]   Riordan F, Papoutsi C, Reed JE, Marston C, Bell D, Majeed A. Patient and public attitudes towards informed consent models and levels of awareness of Electronic Health Records in the UK. Int J Med Inform 2015; 84(4): 237-47.
[http://dx.doi.org/10.1016/j.ijmedinf.2015.01.008] [PMID: 25649841]

[47]   Poissant L, Pereira J, Tamblyn R, Kawasumi Y. The impact of electronic health records on time efficiency of physicians and nurses: A systematic review. J Am Med Inform Assoc 2005; 12(5): 505-16.
[http://dx.doi.org/10.1197/jamia.M1700] [PMID: 15905487]

[48]   O'Malley AS, Grossman JM, Cohen GR, Kemper NM, Pham HH. Are electronic medical records helpful for care coordination? Experiences of physician practices. J Gen Intern Med 2010; 25(3): 177-85.
[http://dx.doi.org/10.1007/s11606-009-1195-2] [PMID: 20033621]

[49]   Erstad TL. Analyzing computer based patient records: A review of literature. J Healthc Inf Manag 2003; 17(4): 51-7.
[PMID: 14558372]

[50]   Boonstra A, Broekhuis M. Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. BMC Health Serv Res 2010; 10(1): 231.
[http://dx.doi.org/10.1186/1472-6963-10-231] [PMID: 20691097]

[51]   Banerjee PK, Bagha H, Eds. Emr Adoption by Small Clinics in Malaysia: An Exploratory Study and Theoretical Explanation. PACIS 2014.

[52]   Alasmary M, El Metwally A, Househ M. The association between computer literacy and training on clinical productivity and user satisfaction in using the electronic medical record in Saudi Arabia. J Med Syst 2014; 38(8): 69.
[http://dx.doi.org/10.1007/s10916-014-0069-2] [PMID: 24957393]

[53]   Terry AL, Giles G, Brown JB, Thind A, Stewart M. Adoption of electronic medical records in family practice: the providers' perspective. Fam Med 2009; 41(7): 508-12.
[PMID: 19582637]

[54]   Ajami S, Bagheri-Tadi T. Barriers for adopting electronic health records (EHRs) by physicians. Acta Inform Med 2013; 21(2): 129-34.
[http://dx.doi.org/10.5455/aim.2013.21.129-134] [PMID: 24058254]

[55]   Chisolm DJ, Purnell TS, Cohen DM, McAlearney AS. Clinician perceptions of an electronic medical record during the first year of implementaton in emergency services. Pediatr Emerg Care 2010; 26(2): 107-10.
[http://dx.doi.org/10.1097/PEC.0b013e3181ce2f99] [PMID: 20093997]

[56]   Bredfeldt CE, Awad EB, Joseph K, Snyder MH. Training providers: Beyond the basics of electronic health records. BMC Health Serv Res 2013; 13(1): 503.
[http://dx.doi.org/10.1186/1472-6963-13-503] [PMID: 24295150]

[57]   Edwards G, Kitzmiller RR, Breckenridge-Sproat S. Innovative health information technology training: Exploring blended learning. Comput Inform Nurs 2012; 30(2): 104-9.
[http://dx.doi.org/10.1097/NCN.0b013e31822f7f7a] [PMID: 21915046]

[58]   Ministry of health Malaysia. User access control policy and guidelines 2011.

[59]   Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. Manage Inf Syst Q 2010; 34(3): 523-48.
[http://dx.doi.org/10.2307/25750690]

[60]   Ayatollahi H, Shagerdi G. Information security risk assessment in hospitals. Open Med Inform J 2017; 11: 37-43.

[http://dx.doi.org/10.2174/1874431101711010037] [PMID: 29204226]

[61]　Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A. Security and privacy in electronic health records: A systematic literature review. J Biomed Inform 2013; 46(3): 541-62.
[http://dx.doi.org/10.1016/j.jbi.2012.12.003] [PMID: 23305810]

[62]　Rahim FA, Ismail Z, Samy GN, Eds. Information privacy concerns in electronic medical records: A preliminary investigation. International Conference on Knowledge Management in Organizations 2014. Springer.

[63]　Leveille SG, Walker J, Ralston JD, Ross SE, Elmore JG, Delbanco T. Evaluating the impact of patients' online access to doctors' visit notes: Designing and executing the OpenNotes project. BMC Med Inform Decis Mak 2012; 12(1): 32.
[http://dx.doi.org/10.1186/1472-6947-12-32] [PMID: 22500560]

[64]　Delbanco T, Walker J, Bell SK, *et al.* Inviting patients to read their doctors' notes: A quasi-experimental study and a look ahead. Ann Intern Med 2012; 157(7): 461-70.
[http://dx.doi.org/10.7326/0003-4819-157-7-201210020-00002] [PMID: 23027317]

[65]　Delbanco T, Walker J, Darer JD, *et al.* Open notes: Doctors and patients signing on. Ann Intern Med 2010; 153(2): 121-5.
[http://dx.doi.org/10.7326/0003-4819-153-2-201007200-00008] [PMID: 20643992]

[66]　Esch T, Mejilla R, Anselmo M, Podtschaske B, Delbanco T, Walker J. Engaging patients through open notes: An evaluation using mixed methods. BMJ Open 2016; 6(1): e010034.
[http://dx.doi.org/10.1136/bmjopen-2015-010034] [PMID: 26826154]

[67]　Nazi KM, Turvey CL, Klein DM, Hogan TP, Woods SSVA. VA OpenNotes: Exploring the experiences of early patient adopters with access to clinical notes. J Am Med Inform Assoc 2015; 22(2): 380-9.
[http://dx.doi.org/10.1136/amiajnl-2014-003144] [PMID: 25352570]

[68]　Wainer J, Campos CJ, Salinas MD, Sigulem D. Security requirements for a lifelong electronic health record system: An opinion. Open Med Inform J 2008; 2: 160-5.
[http://dx.doi.org/10.2174/1874431100802010160] [PMID: 19415143]

[69]　James DS, Leadbeatter S. Confidentiality, death and the doctor. J Clin Pathol 1996; 49(1): 1-4.
[http://dx.doi.org/10.1136/jcp.49.1.1] [PMID: 8666676]

[70]　Kottow MH. Medical confidentiality: An intransigent and absolute obligation. J Med Ethics 1986; 12(3): 117-22.
[http://dx.doi.org/10.1136/jme.12.3.117] [PMID: 3761330]

[71]　France Penal Code Article 379.

[72]　Warwick SJ. A vote for no confidence. J Med Ethics 1989; 15(4): 183-5.
[http://dx.doi.org/10.1136/jme.15.4.183] [PMID: 11644403]

[73]　Dickens BM, Cook RJ. Law and ethics in conflict over confidentiality? Int J Gynaecol Obstet 2000; 70(3): 385-91.
[http://dx.doi.org/10.1016/S0020-7292(00)00286-1] [PMID: 10967176]

[74]　Stanberry B. Legal and ethical aspects of telemedicine. J Telemed Telecare 2006; 12(4): 166-75.
[http://dx.doi.org/10.1258/135763306777488825] [PMID: 16774696]

[75]　Data protection act 1998 (1998).

[76]　White SM. Confidentiality, 'no blame culture' and whistleblowing, non-physician practice and accountability. Best Pract Res Clin Anaesthesiol 2006; 20(4): 525-43.
[http://dx.doi.org/10.1016/j.bpa.2006.09.002] [PMID: 17219939]

[77]　Beran RG. The doctor/patient relationship, confidentiality and public responsibility. Med Law 2002; 21(3): 617-37.
[PMID: 12437207]

[78]　Papoutsi C, Reed JE, 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): 86.
[http://dx.doi.org/10.1186/s12911-015-0202-2] [PMID: 26466787]