Web-Based Electronic Healthcare Records
Confidentially and Security

Samira Ali, RN, MSN (NI)
Lecturer, College of Nursing & Allied Health Sciences
Riyadh, Saudi Arabia
Web-Based Electronic Healthcare Records | Confidentially and Security

Introduction

The deployment of electronic healthcare records on the World Wide Web is rapidly expanding as means of communicating health information. While the Web may solve some issues of accessibility, availability, and use of health information and is considered a convenient and cost effective resource, this technology also places sensitive data on the Internet, some which may involve patient health records. This raises issues of privacy, confidentiality, and security of electronically based health information.

The move to Electronic Health Records

Many observers believe that economy and restructuring of the United States health care delivery system played a major role in the application of information technology to health care. The changes included consolidation as well as mergers of care providers and financing organizations. This has led to the emergence of sophisticated management approaches to share financial risks between industry and healthcare providers. These changes were the result of the constant pressure to reduce cost of care, coupled with efforts to enhance the ability to measure and improve the quality of care provided. These changes have led to an increased emphasis on outcome driven care.

The traditional paper-based system of healthcare documentation is inefficient in light of new technology and has multiple weaknesses related to accessibility, availability and retrieval of records. As a result, time and resources are wasted on duplication of test and treatment, (Milholland, 1996)

According to Laudon and Laudon (1998) the problem is extensive. Some medical centers have more than four million patients’ records that are stored for 25 years, depending on the applicable state of laws. The majorities of these medical records are currently on paper and are clumsy to access, vulnerable to errors and misplacement, and often illegible.
Over one trillion dollars is spent on healthcare annually and, of that amount, 200 billion dollars is spent on record keeping. Even though healthcare organizations are struggling with cost containment, they still have lagged behind other industries in resisting implementation and conversion to an electronic health record (Bowles, 1997). This non-integrated data collection method continues to produce redundant data, and does nothing to reduce duplication of services, treatments and healthcare costs.

Integrated delivery systems are rapidly being viewed as a means of consolidating multiple care providers across health continuum, such as hospitals and primary healthcare clinics. The move towards integrated system is motivated by the promise of cost savings, which can also support an expansion in market share to protect current business, and improve in the quality of care.

Reynor (1994) suggested that automating the documentation system in healthcare institution is cost effective as a result of increased productivity. According to Renner & Swart (1997), the rapid shift to managed care has resulted in an enormous amount of data being collected in a variety of settings and has driven an increased effort to electronically transfer patient information.

The application of information technology is intended to facilitate the management and processing of data to support patient care and ultimately improve nursing practice. The American Nurses Association Scope of Practice for Nursing Informatics (1995) has included this concept. Graves and Corcoran (1989) Bowles (1997), and Hammond (1997) agreed that integrated system could provide the ability to collect, aggregate, organized, move and re-present information in an economical, efficient way that is useful to the user of the system. Furthermore, the ability to share data in one of the biggest advantages of integrated information system in that data could improve efficiency and reduce redundancy, while improving quality and lowering cost.

The computer-based patient record plays increasingly important role in the formation, dissemination and management of clinical, administrative, and financial data in a highly competitive, cost-contained environment. The recent expansion of interest in development of Web-based electronics health care records has generated growing concern regarding confidentiality and security of health information (reference) because these records typically include sensitive patient data. The risk of breeches in information security presents new concern for nurse informaticians.
According to the American Nurses Association (1995) Scope of Practice for nursing informatics, the collection and use of data to generate information and knowledge to support nursing care delivery is essential. Furthermore nursing informatics theory addresses the way nurses use the data, information, and knowledge to support care delivery decisions. In that the electronic health records in the culmination of patient care data, input from nursing informatics professionals is essential if integrated systems are to serve patients and healthcare professionals successfully. By assuring nursing representation in the information system development process, the needs of nurses can be represented at all phases of information system development and implementation.

As early as 1992, Turley advocated nursing input to development of future patient information system (Turley, 1992). Turley encouraged nurses to evaluate their current modes of information management and position themselves to influence the framework of integrated system.

Architecture of the Web-base Electronics health Records

The electronic health records is defined as an electronic version of the patient records that resides in a computer system specifically designed to support users by providing accessibility to complete and accurate data, clinical alerts, reminders, and clinical decisions support (Andrew & Dick, 1996). An electronic health records may be located in a stand-alone computer system, a networked system, or a system that allows access from the Internet via the Web. It is widely believed that the development of electronic healthcare records on the Web is a step towards decreasing cost and improving healthcare quality and access (Kohane et al., 1996).

Architecture of the Web-based Electronic Health Records

A critical abstraction layer in the Web-based electronic medical record is the Common Medical Model, a shared set of conventions for visual presentations of the clinical data. According to Kohane et al. (1996), the first step involves developing a Common Medical Model that represents an agreement of what information should be present in the electronic medical record. This step is designed to bridge the divergent information model each institution. The second step involves converting data from the information model of one institution to that of another by utilizing the Health Level Seven (HL7) messaging standard. HL7 is one of the more popular interchange formats for communication between clinical information systems. HL7 communicates data as a
sequence of defined American Standard Code for Information Interchange (ASCII) characters that are hierarchically organized into segments, fields, and components.

The second abstraction layer is the Visual Presentation layer that is designed to provide independence from the particular presentation conventions of an existing electronic medical record. It describes layout of the clinical data elements such as flow sheet, timeline graphs, annotated pictures and how the elements of theses presentation correspond to allow user interaction with the Common Medical Record.

The third layer in the Web-based Electronic Medical Record architecture is the Screen Rendering Layer. This requires implementation of a set of transformations between existing Electronics Medical Record and the abstraction layers (http://aspe.os.dhhs.gov/admnsimp/).

Informatics Issues of the Web-based health record

The difficulties associated in accessing information, either about the a specific patient or about a general issue related to patient management, a re a frustrating and common occurrence for nurses. This problem is coupled with the lack of integration and external connectivity that would enable the sharing of information across settings.

Interoperability

Current electronic health records are limited and do not lend themselves to cross institution settings. Some of these systems are based on old architectural models, idiosyncratic local organization and old implementation technologies that make their interoperation with other system difficult (Kohane et al., 1996). With increasing pressures to decrease cost and enhance clinical productivity, nurses have begun to press for more reliable system that provide intuitive access to the information they need at the time they are providing care for patients. The electronic health record on the Web can supply the nurse with improved access to patient-specific information, and should better support providers in facilitating quality of care and quality of life. The ability to share data is one of the biggest advantages integrated system can offer toward improving efficiency, eliminating redundancy, and inconsistency, while maintaining data integrity (Bowles, 1997).
Uniform Access

The Web-based electronic health record system provides uniform access to a vast interlinked resource library of information that is available independently of the computer and operating system platform on which it happens to run (e.g. PC, Mac, Unix). It also allows access to multimedia data (including formatted text, pictures and graphical images, sound, and video), and it is defined in terms of a general, relatively flexible and extendible set of protocols that allow and encourage experimentation and evolution. The electronic health record on the Web overcomes many technical problems of sharing clinical data and allows the sharing of data across multiple institutions despite their heterogeneous particularities. Internet technologies may be easier and less expensive to develop a system based on Internet technologies than other alternative technologies such as integration of current health records. Other advantages of Web-based applications include ease of use, since hypertext technology is a very intuitive interface. Portability is ideal for information sharing since browsers have been designed for every operating system and hardware platform.

Confidentiality and Security

Despite the potential advantages of Web-based health records a major threat associated with the Web network and computer crimes. According to Rahanu (1999), computer crime is a growing problem for all organizations. Every new technology introduced into society creates new opportunities for crime, and healthcare information technology is no exception. A new generation of high-technology criminals is busy stealing data, doctoring data, and threatening to destroy data for monetary gain. This ultimately increases the public’s concern about the potential abuse of this technology or breeches of confidentiality. Healthcare records contain a large amount of sensitive and personal data. That information may range from demographics including age, sex, race, and occupation, to financial information such as diagnoses of AIDS, mental illness, alcohol abuse, or treatment.

Regardless of the nature of information dissemination or storage, people have the right to protect their confidential information from unnecessary public disclosures.
Privacy and confidentiality issues have been long-standing issues in healthcare and the Web-based healthcare applications are no exception. Web-based healthcare applications can potentially bring unprecedented information access to everyone, thus increasing the risk of data interception, alternation, deletion or misuse.

Privacy is the right of the individual to be left alone, free of unreasonable personal intrusions, interference from other individuals, or organizations (Amatayakul, 2000a). According to Gostin (1997), the primary justification for respecting privacy resides in the principles of respect for autonomy of individuals who wish not to be observed or have information about them released. Respecting privacy also enhances the development of maintenance of trusting relationships between patients and providers. The ethical justification for protecting privacy addresses the psychological impact or damage that results from the disclosure of personal information as well the economics damage that might be associated with inappropriate released or discovery of personal information. Economic damage might include loss of employment or health insurance.

Equally compelling ethical can be made to support a more efficient system of maintaining healthcare information. Access and efficient use of healthcare information would promote higher-quality health care, more cost-effective services, and better scientific research (Gostin 1997).

The professional code of ethics for nurses prescribes moral behavior and actions based on moral principles. The American Nurses Association Code of Ethics (2001) states that the nurse has responsibility to safeguard client’s right to privacy. The rules of respecting client confidentiality and accountability are mentioned in the code for nurses as both morally and legally required.

Protecting patient privacy and confidentiality is an expectation at all levels of healthcare. Confidentiality is the expectation that the information provided to an authorized user will not be re-disclosed. It is the status accorded to data or information that is sensitive and therefore needs to be protected against theft, disclosure and improper use.

Data security in the sum of measures that safeguard data and computer programs from undesired occurrences or disclosure. System security entails a total safeguard including the protection of information against threats or disclosure as well as policies, procedures and technical measures used to prevent unauthorized access and sabotage, and errors (Buckovich, Rippen, & Rozen, 1999).
Privacy and confidentiality of information are critical to healthcare organizations’ missions. However, few organizations focus on their most important information assets, patient records, when making decisions about protecting information. It is widely agreed that today’s security issues are not merely related to technology problems; it is also attributed to lack of security standards in healthcare organizations. Twenty percent of providers have no security plans to cover their information systems. In addition, ninety percent of institutions possessing some sort of electronic medical records have not updated their security technology to reflect new technology and trends (Halamka, et al. 1997). There is a consensus that threats related to computer crime are associated with data access by authorized users and not always by unauthorized hackers. Furthermore, there are often poor security standards, such as utilizing a general login in such as “RN” or “MD” and this does not authenticate the user properly.

Current Health Insurance Portability and Accountability Act (HIPAA, 2000) regulations on security requirements include administrative, physical, and technical mechanisms to safeguard the confidentiality, availability and integrity of health information. However security measures must be implemented in the context of an organization’s privacy policies (Amatayakul, 2000b).

There are three major areas that this regulations addresses: preserving privacy; security legislation, and compliance. Current changes in privacy legislation entail significant changes in the regulation and now extends to all individually identified health information in the hands of covered entities, regardless of the storage format, i.e., electronic or paper form. Privacy provisions include several features that impact all covered entities, including healthcare providers who transmit health information electronically and even paper format, health plans, and healthcare clearinghouses. These entities are required to have a contract with the agencies they do business with so that they would comply with HIPAA regulations. The agencies are required to revise their practices to assure compliance; particularly the way health data transmission is handled.

According to Waldo (1999), HIPPAA regulations outline four general compliance issues that require organizations to have:

- Policies and procedures to govern confidentiality, data integrity, and access
- Physical safeguards to control access and protect computers system against fire and other disaster.
• Technical security measures to protect data held in information systems.
• Technical security measures that protect and prevent interception and access to information sent via network.

**The Role of Nurse Informaticians**

The nurse informaticians have a major role in the education of nurses regarding to HIPAA regulations. The educator role and training entails activities that might impact directly on the success or failure of newly implemented informatics solutions in their organization. The full regulations can be found at [http://aspe.hhs.gov/admnsimo/](http://aspe.hhs.gov/admnsimo/).

**Security goals consists of:**

- Limiting access to the assets of computing systems only to authorized users.
- Ensuring that only authorized users can modify data.
- Permitting data access to authorized user only.

The security plan should identify and organize the activities protecting a computing system. The plan should entail a description of the status of security measures as well as a plan for change.

**Every security plan should address the following six components:**

- The goals of a computer security policy, and the willingness to achieve those goals.
- Currents state of the security system describing the status of measures being taken at the time of the plan.
- Recommendations and requirements, which lead to meeting the security goals.
- A description of who is responsible and accountable for each security activity.
- Timetable identify when different security functions are to be done.
- Specification of the system by which the security will be periodically updated.
According to Pfleeger (1997) some controls on computing are achieved through added hardware or software solutions but other controls are matters of policy. Some of the simplest controls such as frequent change of passwords can be achieved at cost.

**General controls consist of:**

- Physical hardware controls including door locks, back up copies.
- Software controls monitor the use of a system e.g. Internal program controls, operating system controls, or development controls.
- Data security controls ensure that valuable data stored on a disk or tape is not subjected to unauthorized access. E.g. data security software can limit access to specific files.
- Administrative controls entail standards; rules, procedures and control that ensure that organization’s controls are enforced and executed. E.g. written policy.
- Input controls entail procedures that check data for accuracy and completeness when entered in a system. E.g. input authorization, data editing.

According to Woodhead (1997), Informatics nurses are also responsible to educate, implement, and help integrate information system throughout healthcare organizations. Nurse informaticists must assure that nursing representations is available in system so that nursing care delivery is considered at all phases of information system development and implementation.

Nursing representation is also needed in HL7 development, as interoperability of healthcare information and security that entails sending message transactions over the Internet is of key importance.
Conclusion

The Internet is a step toward advancement of increasing accessibility and availability of health information and is considered a convenient and cost effective resource. The drawback to this technology is the vulnerability of data contained in any future Web-based patient health records. A Web-based health records requires considerable attention to security to minimize the risks of inappropriate disclosure. Security measure must be designed to protect patient information and should include personal identifiers, password restrictions, and data security controls. Security levels that prevent users from accessing unauthorized data should be implemented, and audits must be performed routinely to identify inappropriate or fraudulent access.

References


Contact Address:
Samira Ali, RN, MSN (NI)
Lecturer, College of Nursing & Allied Health Sciences
Riyadh, Saudi Arabia
E-mail: samar22193@yahoo.com

Copyright © 2006 by Samira Ali, RN, MSN (NI). All rights reserved.