The security for telemedicine law medical essay

Law

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \nThe use of information and telecommunications technology in the sharing of medical data and provision of health care for patients by medical experts is called telemedicine. Telemedicine helps provide medical services to patients in far and remote locations where it may have been almost impossible for medical personnel to get to on time. The availability of technologies such as, Patient telemonitoring systems (PTS) is used to get hold of a patient’s medical records, process the record and securely transmit this information to medical personnel. The advancement in technology with the use of 4G networks and tablets have made telemedicine much more reliable, allowing patients to communicate their various medical conditions to their doctors. A typical example is when a patient takes a picture of a rash infected area of the patient’s skin and sends this picture to his or her doctor who in return replies the patient whether to get an antiseptic ointment or come to the clinic for further medical analysis if need be. Another application of telemedicine is the use of wearable physiological monitoring system that posses an array of sensors rooted into the fabric of the patient to constantly keep an eye on the physiological parameters and transmit the patient’s information to a remote monitoring station. Most importantly is that data management has become a concrete challenge facing the healthcare system. However with the increasing usability of information technology,

data collection, analysis, empirical testing, prescriptions and use of medical devices and applications have created a holistic approach to health and this creates a well defined information healthcare system. For more proactive ways of dealing with health data management and concise empirical analysis, this study seeks to outline the classifications of data collection in healthcare, medical records of patients, data analysis center, information and reporting, use of codes and measurements. Over the decade, about 550 projects which have direct linkage to the reliability of PIP (patient identification process) in the healthcare structure have been analyzed by two major groups, Madison’s Analytic Services and Professional Services. Assessing the Master Patient Index files used as an indicator to clinical data in hospitals and health facilities, it has been observed that duplication error rates have spiraled to a ridiculous rate of twenty percent, leaving most errors within the range of nine and eleven percent. EMPI (Enterprise Master Patient Index) posses considerably more challenges in the incorporation of patient data from multiple system and has often been interchangeably used with Multi-facility Master Patient Index. In the present scheme of things in healthcare practices, information management professionals grapple with reaching a hundred percent recovery of patients’ medical history/records towards facilitating excellent patient care delivery. It is pertinent to note that cases lower than a hundred percent recovery rates are regarded inadequate. If the MPI becomes unreliable in the accessing of patients data, the HIM searches through other sources ranging from date of birth, social security number and alternative identification modes until exhausted. This is not say that the intricacies of patients identifications have been devoid of the earlier stated error rates [1]. Physicians have been bound by an ethical code of

conduct which stipulates that they are not obliged to discuss patients' data garnered either through consultation or through diagnosis. The said code of conduct is contained in AMA's Code of Medical Ethics. This code basically reveals a symbiotic relationship in that patient-physician confidentiality enables the patient to attain full disclosure which, in turn, ensures that the physician attains adequate diagnostics toward an effective treatment. Despite the fact that the AMA's moral guidelines doubles as both an officially authorized guideline as well as a moral duty, it is not a legal obligation. Usually physicians are guided by legal/ethical standards and are usually obliged to follow court orders. However in the case of breach in confidentiality by physicians concerning patients medical history without appropriate authorization, there is a provision under the law and court that punishes such acts. Nonetheless requests for confidential medical history of patients have assumed a substantial increase. With the presence of electronic health information system, there has been an increase in the transmission and access to health information. Through the integration of delivery networks system, physicians now have access to clandestine medical data of all patients. This confidential data is also disbursed via shared databases and clinical repositories. The availability of these medical records helps physicians in treating patients effectively without further complicating their health. The dilemma here for physicians is the use of this technology without breaching the confidentiality obligations they have to their patients. UNDERSTANDING BREACH OF CONFIDENTIALITY IN TELEMEDICINEBreach of confidentiality in health can be described as a situation whereby a patients' medical record or status discovered via consultation or by accident is disclosed to a third party without the approval

of the patient or the issuance of a court order. This form of breach can be written, oral or through electronic means. It is interesting to note that the legal aspect of the breach of confidentiality is more comprehensive than the ethical obligation. Nevertheless the legal parameters in this area have often been referred to as a radical aspect of federal and state law. Also in this legal code of conducts are privacy rights and regulations governing patients' information/history, and licensing which are created to shield sensitive patients' data such as DNA records, HIV results, Hepatitis results, drug and alcohol history and mental health history. Patients Consent on the Release of Confidential Medical HistoryIt is quaint essential to note that patients' medical information can only be revealed to a third party only when authorization has been granted by the patient. As a matter of fact, patients' information can only be released to quarters including: attorney or insurance company; patient's employer, unless an employees' compensation claim is involved; patients' family members, except where the family member has been appointed the patient's legal representative under a durable power of legal representative for health care; government agencies; after due authorization of the patient. A number of state laws particularly permit disclosure to any individual upon approval of the patient. Other state laws allow discharge on patient consent only to particular classes of people. Further, once the patient has given approval to discharge the record, the condition of the disclosure may be obligatory for the owner of the health record or simply permissive. HIPAA has created additional patient confidentiality considerations. Under the confidentiality policies, enclosed entities may typically discharge protected medical information devoid of approval merely to assist treatment, imbursement or medical care

operations. Managed care organizations (MCO) often necessitate members to sign a common discharge form on enrollment in the plan. These forms permit the discharge of health information to the MCO. The language generally used in a discharge might entail " that any supplier may equip the MCO with such health information as may be necessary and that the associate acknowledges the MCO's right to carry out a skilled utilization evaluation plan of medical services and to organize remuneration and/or reimbursements amid other wellbeing or indemnity programs." Preceding the transfer of health information to an MCO, utilization appraisal programs or other medical programs, physicians, clinics, and others ought to obtain a signed duplicate of the patient's discharge of medical information.

Who Can Authorize the Discharge?

Usually, the right to discharge health information is conferred on: (1) the patient, if a knowledgeable grown-up or emancipated minor; (2) an officially authorized custodian or close relative if the patient is inept or a small child; and (3) the overseer or the person responsible for of the patient's assets if patient is late. The patient's right to permit discharge of health report is contained in many state laws. These laws all state that health records are not to be disclosed and right to access varies from state to state. Some states allow the health care professional or provider to establish patient's right of access. Some states particularly allow patients access the health information enclosed in their health records. What Is The Content Of The Release? Patients’ mode of identification (Name, age and sex)Address of the physician and the health institution instructed to relinquish medical informationA narrative of the information to be given outProper identification

of the third party to be given informationTerms of authorization of information releasePatient/guardians' signature or court signatureLastly time frame of releaseImplied Consent And Public Policy Exceptions Or Required DisclosuresMost times, without explicit authorization from patients, medical records or health history can be disclosed by physicians once the patients have accepted to be under their care. By implication the patients' acceptance treatment or consultation from the physician, implies that he/she has given the physician certain rights. Also consent is implied when the patient agrees to transfer from one health institution to another. In situations like this, disclosure of medical history is mandatory to enable continuation of treatment. A corollary to the above is that despite the physicians' ethical and legal obligations to keep patient data confidential, they still have the overall duty to release information of patients especially when there is an overriding societal need. For example, if there is an evidence that a patient might harm other patients, it is the duty of the physician to inform prospective targets and also law enforcement agents. Also, communicable diseases and other forms of disease that are airborne should be reported in order to avoid an epidemic. Thus it is safe to say that societal interest seldom overrides confidentiality.

General management safeguards and security tips

It is quaint essential for physicians to have a memorandum of understanding which would be reviewed by an attorney with healthcare providers, system vendors and consultants who participate in data repository. Also there should be a uniformly comparable confidentiality policies and controls over sensitive patient data such as abortion details, mental health history and HIV status. It

is also imperative to maintain efficient security system, staff training and signing of confidentiality contracts. It is instructive to note that enlisting the services of security experts to occasionally evaluate the security of the clinical data storehouse and require users who access the information to sign appropriate user agreements is advisable. Medical practitioners are required to put some office measures in place to check the discharge of medical reports without the patient’s consent. The procedure might just entail something as simple as attaching administrative forms every time medical records are required. The form should include information such as date the request was made, date the copy of the patient's release form was released, and date that the medical records were approved for sending to the requester.

The Importance of Protecting Client Confidentiality

Prior to the vision of the information highway, ethics and laws concerning confidentiality existed. Today's computerized systems do not always fit well with the old principles and laws. Owing to issues bordering non conformity, a couple of physicians and networks have only handled issues pertaining to protecting patient confidentiality with levity. This is short-sighted and unwise approach. The law will slowly catch up with the new system and device means to ensure the confidentiality of client records. In the meantime, physicians should make attempts to safe-guard information to a possible degree and to conform to the " hodgepodge" of federal and state laws. Physicians should notify their clients of the restrictions of privacy protections and allow them weight the balance between treatment and the possible risks of the leakage of sensitive records. Clients expect their physicians to ensure

the confidentiality of their medical information and should not be let down. If information must be disclosed, the client has to give appropriate authorization for discharge. General releases will not be adequate for reports including sensitive matters like HIV. Physicians should acquaint themselves with laws concerning the responsibility to ensure discretion. Violation of confidentiality—it doesn’t matter how trivial—can result in distrust and, probably, a court case and/or punitive action [2]. The best know method to secure patient information that is being transferred via the internet is through the use of Advanced Encryption Standard. AES (Advanced Encryption Standard) is a symmetric 128-bit block information encryption method which was created by two Belgian cryptographers Vincent Rijmen and Joan Daemen. It is pertinent to note that the Algorithm as an encryption mode was adopted by the United States government in 2002 as a form of replacement of the initial DES, and it has been verified that the AES functions simultaneously at multiple network. The United States Department of commerce who has a sub group called NIST (National Institute of Standards and Technology) chose the algorithm known as Rijndael which is one out of a group of five algorithms under deliberations, including MARS from the research team at IBM. Most times Rijndael and AES are used interchangeably; however there are some existing differences between the two. Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits while AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits [3]The process involved in the encryption of data via AES include; 1. Convert to state arrays2. Transformations [Add round key, sub byte, shift row and mix columns]3. Key expansionThe soaring presence of the cyber world in the

medical environment has brought up important issues concerning the confidentiality, availability and integrity of medical data transferred via the internet. Thus my research work will be on the developing of a model for a glucometer that can transmit accurate and secure information about the glucose level of a patient to a medical personnel and also alert both the patient and the medical personnel during critical clinical conditions of the patient