Digital Health and Cyberspace

Introduction

Rapid advances in information technology have led to the development of the medical field known as digital health. Diagnostic instruments are no longer the sole preserve of physicians and the gathering of health relevant data is being revolutionized through wearable, ingestible, and implantable devices. For example, there now exist digital pills which can inform an external sensor when a patient takes her medication. This is only one of what are known as SAMDs (self-activated medical devices).

Advances in information technology enable a much easier and rapid circulation of data between patients, caregivers, and physicians. Data concerning a patient's condition can be registered by a device, sent to a physician who analyses it, the ensuing recommendation sent back to the device, which then provides the patient or caregiver with information on how best to address the patient's condition. The shared and rapid flow of data is characteristic of digital health. It has tremendous promise, but also necessitates applying well established ethical requirements in new, hitherto unanticipated circumstances.

Note that in this chapter I will use the terms 'physician' and 'health care professional' interchangeably. This should not be taken to mean that I view physicians as the only health care professionals.

Telehealth and Telemedicine

One of the greatest benefits of the rapid advance of information technology is the dramatically increased ability to provide patients with health care from a distance. This

technology supports long distance clinical care for patients who are housebound or who live in remote or underserved areas. It also facilitates easy access to professional health-related education. Whether the terms 'telehealth' and 'telemedicine' remain distinct in the future, at present, telemedicine has a narrower definition than telehealth, being understood as involving real time, direct two-way communication between a patient and a health-care professional at a distant site. Telehealth, on the other hand, is a broader category, including, for example, websites where there is no direct communication with a health professional.

The different types of patient-physician interactions that occur in telehealth and telemedicine give rise to different levels of responsibility for health care professionals. These levels are best understood as lying on a continuum. At one end of the continuum are general health related websites such as WebMD (https://www.webmd.com/default.htm). Such websites involve no direct interaction between the person seeking health information and the physician providing it. Health professionals contributing material are responsible for the quality of the material they contribute but have no therapeutic responsibility to specific individuals.

More responsibility is expected of health professionals who operate in the context of a website or service where patients can ask for an individualized response to specific personal questions. Health professionals in such circumstances are not simply offering general information, but some degree of therapeutic advice.

Further along the continuum of responsibility, are specialists who act as consulting physicians at a distance. Through interpreting test results or symptoms, these specialists offer advice that directly informs the therapeutic decisions made by the patient and treating physician. The level of responsibility in such instances is exactly as the specialist has consulting in person.

Yet more responsibility accrues to physicians who act as the primary treating physician, but at a distance. These physicians direct their patients' clinical care in real time through telecommunications. For instance, in teleoncology, a remote specialist might be the treating physician who coordinates and directs the care provided for a patient by a team of health care professionals at remote setting or different institution. The responsibility of the specialist as the treating doctor is not lessened by distance and remains the same as if giving treatment in person.

Ethical Requirements of Medical Care

In the introduction we noted that telehealth and telemedicine necessitate applying well established ethical requirements in new, hitherto unanticipated circumstances. It is appropriate to say something about these requirements.

Fidelity and Continuity of Care

Health care providers' primary professional responsibility is the health of their patients. It is essential, therefore, that they reveal any financial or other interests that might affect them in their interaction with commercial health websites or services. Their duty of fidelity requires avoiding any conflict of interest that could, or might reasonably be perceived, as influencing their treatment of patients.

The duty of fidelity also has implications as regards continuity of care. Physicians who provide responses to individual health questions on a website have a responsibility to encourage patients to seek in person health care if such care is appropriate to the symptoms presented. If clinical services are being provided from a distance, then it is important that the physician providing these services be in direct communication with the primary care physician

on a regular basis to exchange information. Collaboration between the specialist acting from a distance, the primary care physician, and patient or surrogate is important in ensuring appropriate follow up and continuity of care.

Informed Consent

Informed consent requires that patients be given the relevant information needed for them to participate in decisions concerning treatment. In the previous section we noted a continuum of different levels of responsibility for health care providers involved in telehealth and telemedicine. What counts as informed consent lies along this continuum. At one end, for patients consulting a website such as WebMD, a physician's responsibility is only to provide his or her credentials as a qualified provider of health information. At the other end of the continuum, where a physician is acting at a distance as the treating doctor, informed consent requires discussion with the patient of medical issues and treatment options.

Competence

Health care professionals have a duty to provide competent care. Like informed consent, this duty has different requirements at different points along the continuum of telehealth and telemedicine services. Physicians providing general non-individualized health information for online sites must only ensure that they provide accurate, objective information. Physicians at websites that provide responses to specific individual health questions have a greater responsibility, which includes clinical experience and the gathering of any needed information need to offer a personalized recommendation for treatment. Physicians who provide clinical services at a distance must meet further requirements in demonstrating

competence, which include proficient in the use of the relevant technologies and recognizing the limitation of those technologies in caring for an individual patient at a distance.

Confidentiality

Physicians have a duty to protect the privacy of their patients. Health information websites should have well defined, thought out privacy policies which they make available to their users. Physicians providing health related information to a website have a duty to check that the website has an appropriate privacy policy.

Health care professionals who answer individual personalized questions arising on a website equally have a duty to check whether the website has an appropriate privacy policy in place and have taken steps to ensure the confidentiality of individual information exchanged through the website. In addition, they have the duty to inform the patients with whom they are interacting that, despite precautions, there are always risks to privacy when information is communicated electronically.

In instances where clinical services are being provided at a distance, the physician must observe strict privacy practice herself and have taken reasonable steps to assure herself that those with whom she collaborates also comply with privacy protocols. The medical team, as a whole, is responsible for assuring itself that steps have been taken to protect any unauthorized access to patient information. At the same time, given the inherent risks in transmitting information electronically, they have a duty to inform patients of such risks and the steps taken to alleviate them.

The Responsibility of Patients

We have been noting the responsibilities of physicians to patients and how those responsibilities apply in cyber space. It is appropriate to note that patients also have responsibilities. Material available on the Internet varies enormously in reliability. Patients should seek authoritative advice on which sites provide trustworthy medical information. Equally, they should realize that such information is often highly complex, and as laypersons, they may lack the requisite skill to interpret it properly.

Digital Health and Big Data

We have noted how cyberspace and its technologies facilitates the circulation of data. Diagnostic data generated by patients is recorded and transmitted by devices to sites where it is analyzed and then sent back to devices that can provide the patients or treating physicians with advice concerning the patients' health. This feedback loop can provide large bodies of health-related data with the potential to be mined for impressive advances in medicine. The availability of such data opens the possibility of pragmatic trial designs that utilize less restrictive inclusion requirements than traditional randomized controlled clinical trials. Such pragmatic trials avoid the high costs of randomized controlled trials and might possibly prove more representative of real populations.

Concerns exist, however. Mining large databanks concerning sensitive health data raises issues concerning privacy protection and the effective use of data.

Protecting privacy becomes much more difficult as data sources become larger and more numerous. Adding to this difficulty is that advanced methods of analysis can be applied to these data sources with many different goals in mind. Safeguards for protecting anonymity are

not fail-proof and consent for use of one's data cannot be so specific as to cover all possible future uses that might be made of it.

There are also concerns around the effective use of data. Increasingly, data is being collected by private nongovernment entities, whose health-related technology is unlicensed. It is important that the products and services provided by such corporations be developed in the context of taking their corporate responsibility seriously.

The Importance of Trust

A culture of trust between health care professionals and those they serve is essential for the successful advancement of digital health. This is especially the case regarding the use of big data. The public must be given good reason to trust the uses to which its data is put. Protection of privacy is, of course, of paramount importance. A culture of trust, however, requires much more than simply protecting privacy. At a societal and institution level, individuals and communities need to know that digital health advances benefit all stakeholders and that oversight measures are in place to ensure that values of transparency and accountability are safeguarded. Particularly, policies concerning data ownership and control need to be clearly defined and shown to be in the interests of the common good.

College of Nurses of Ontario v Mclellan, 2016 CanLii 102076 (ON CNO)

Citation: College of Nurses of Ontario v Mclellan, 2016 CanLII 102076 (ON CNO), <http://canlii.ca/t/h2sb5>

In early 2011, Melissa Mclellan worked on a full-time basis as a nurse in an Ontario hospital. The hospital used a hybrid paper and electronic record system, some records being in paper form and some in electronic form. Each nurse in the hospital, using a unique username and self-selected confidential password, had full access to all electronic health records of the hospital's patients.

In March 2011, an inpatient of the hospital's Acute Inpatient Psychiatric Unit, who was also an employee of the hospital, reported that a number of other employees of the hospital visited in the Psychiatric Unit, even though she had not informed them of her whereabouts. Her concern was that her electronic health records had been inappropriately accessed. As a result, an audit was performed by the hospital.

The audit revealed inappropriate accesses to the patient's electronic health records by Mclellan and some other staff members of the hospital. When questioned, Mcllellan admitted that she had accessed the patient's records without authorization. She also stated that she routinely accessed health records for patients not under her care, but that she never shared any of this information with anyone. Concerned about her statement that she regularly accessed the health records of patients not under her care, the hospital conducted a further audit of the times she had accessed electronic health records.

The hospital maintained that its audit revealed that Mclellan, between August 2005 and April 2011, accessed the personal health information of over 5000 patients who were not under care, without consent or other authorization, or other professional purposes. This number might be disputed since the parameters of the audit were never made clear by the hospital.

Certainly, however, the number was large. Mclellan stated that she was interested about the medical conditions of clients, including those not under her care, and that she felt that accessing client records facilitated self-education and keeping current with best medical practices. In retrospect she recognized that it was wrong to access patients' health care records without appropriate authorization. The audit confirmed her claim that she had never disclosed any personal health information for patients not under her care and that she had no malicious motive in accessing the electronic health records of patients not under her care.

The hospital notified over 5000 patients that their personal health information might have been accessed inappropriately. This resulted in a class action suit brought against the hospital and Mclellan by upset patients. Mclellan invoked the protection in s. 14 of the *Statutory Powers Procedure Act*, s. 9 of the Ontario *Evidence Act*, and s. 5 of the *Canada Evidence Act*. Furthermore, she did not waive the protection in s. 36(3) of the *Regulated Health Professions Act, 1991*.

Mclellan was charged provincially with breaches of the *Personal Health Information Protection Act, 2004* in September 2011. The charges were stayed,[i] for delay in January 2015 on the grounds that her rights under s. 11(b) of the *Canadian Charter of Rights and Freedoms* had been violated. The delay was primarily a result of the Crown's extensive, late disclosure relating to the methodology used by the hospital to conduct the audit and the Crown's change in tactics for the trial.

The College of Nurses of Ontario imposed a four-month suspension on Mclellan. In addition, Mclellan was required to attend training sessions both online and with a nursing expert on 1)

professional standards and 2) confidentiality and privacy regarding personal health information. The College also required that upon resuming employment three random audits of Mclellan's access to electronic health records take place at six-month intervals.

[i] The decision by the Crown to stay or withdraw charges means that they discontinue the prosecution. If stayed charges are not 'brought back to life" within one year of the day they are stayed, then they are dismissed, so long as one had not committed new offences during that one-year period.