JOURNAL OF THE INTERNATIONAL SOCIETY FOR TELEMEDICINE AND EHEALTH

TELEHEALTH IN LIGHT OF CLOUD COMPUTING: CLINICAL, TECHNOLOGICAL, REGULATORY AND POLICY ISSUES

Hassane Alami PhD(c)[1,4], Marie-Pierre Gagnon PhD [1, 2,4], Jean-Paul Fortin MD MPH, FRCP[3,4]

[1] Axe Santé des Populations et Pratiques Optimales en Santé, CRCHUQ, Québec, Canada
[2] Faculté des Sciences Infirmières. Université Laval, Québec, Canada.
[3] Faculté de Médecine. Université Laval, Québec, Canada.
[4] Centre de Recherche sur les Soins et Services de Première Ligne (CERSSPL), Québec, Canada

Abstract

In the health sector, information and communications technologies (ICT) are transforming the modes of practice and service delivery. Telehealth, which is the use of ICT to provide care and health services, is an example of this new model of services. However, telehealth is accompanied by many questions regarding the terms of exchange, archiving, control and security of medical and administrative patient data. These may be very useful but also harmful to patients, healthcare professionals, organizations and even countries. Indeed, with the globalization of information, national data protection policies are being overtaken by this new reality where the "regulatory sovereignty" of a country is challenged. The increasing use of Cloud Computing, as a form of exchange, management and storage of data in the practice of telehealth, is an illustrative example of such challenges.

Keywords: Healthcare; telehealth; cloud computing; cross-border data transfers; technology provider; regulation.

Introduction

New information and communication technologies (ICT) are revolutionizing all sectors of society. In the health sector, we are witnessing a transformation in the modes of medical care and delivery of care and services.[1-4] Telehealth, which is the use of ICT to provide care and health services, is an example of this new service model.[5] It is considered as a means of improving access and continuity of care and services, especially in areas where there are shortages in health professionals or in certain medical specialties.[2,4,6]

As a social, cultural and technological innovation, telehealth is accompanied by a number of challenges and issues that health systems must overcome to aspire delivering the expected benefits for the population. One of these challenges is related to exchanging, managing, archiving, controlling and securing medical and administrative patient data. This point is particularly sensitive since ICT are by definition the translation of the globalization of the information society. Indeed, data can now pass through a multitude of countries and jurisdictions with different cultures, social values and norms that result in very different interpretations and regulatory rules. National data protection policies are thus overwhelmed by this new reality where "regulatory sovereignty" of the country is put to the test. The emergence of Cloud Computing, as a form of exchange, management and data storage, is an illustrative example of such challenges.

In this paper, we will discuss the use of "Cloud Computing" as a service for exchange, management and archiving of medical and administrative data in the context of telehealth practice. We will focus on issues related to clinical, technological, regulatory and political issues from handling, processing and exchange of these data.

Telehealth and cloud computing: a significant potential

Cloud computing can be defined "...as a method of availing computing resources from a provider, on demand, by a customer using a computer connected to a network (usually the Internet)"[7,8] (the term "Cloud" will be used for the remainder of the text). It allows information to be made available everywhere through a simple Internet connection and via a web portal that provides access to a set of shared and configurable IT

resources, at the request and "self-service" for people or authorized third parties.[7,8] The Cloud offers flexibility by allowing multiple users, geographically separated from one another, to have access to information and data by all and from anywhere. This is due to its huge capacity for calculation, compilation, processing and analysis of data.[9-11] In this sense, in situations where organizations confront important workloads and need higher data processing capabilities than they usually have to deal with (e.g. health crisis, major incident, etc.), cloud services allow provision of more power and resources in a near-instantaneous way. The customer pays only for the total resources used.[7] This option also allows the client to avoid storage, energy consumption and maintenance costs associated with traditional infrastructures.[9] Another aspect of the Cloud is that it requires little initial investment compared to conventional physical IT infrastructures, especially for organizations. Thus, from the economic point of view, it reduces costs.[9]

In addition, it offers the possibility that physical servers cannot provide, to manage, store and share massive amounts of information and data with high availability, with the capacity to secure and safeguard data by duplicating it in different datacentres, making retrieval possible in the event of blackouts or damage to machines.[12] The Cloud offers potential information security features and savings through standardized interfaces and achieving economies of scale requiring less investment than traditional protection tools (incident management, maintenance, filtering, standards upgrading, etc.). In addition, the Cloud offers the possibility to respond rapidly to security attacks.[9]

These features make the cloud suitable for the exchange, management and archiving of data for telehealth services. The requirements of availability, speed, ease of use and security, necessary for a best practice of telehealth, are at first glance “guaranteed” by the Cloud. The imperative to have full access of data from the patient record for diagnostic needs, follow-up, expert consultation, discussion of clinical cases and preparation of diagnosis or prescription of medical treatment is made easier. In this sense, the strength of the Cloud is that it can be connected to the information systems of one or several care organizations at the same time.[7] The Cloud makes medical and administrative data available, which facilitates the pooling of clinical history of patients by combining different sources of information in the same interface.

Regulatory issues related to cross-organizational and cross-border data transfers

The rules applying to confidentiality and security of information extend to telehealth. The content of the medical record must remain inviolable and unalterable at all times. Health professionals must ensure the integrity of the content of the patient's medical record, for which they are responsible, and they must be identifiable.[7,13]

There is agreement that the Cloud offers greater security and performance. However, issues related to the confidentiality, integrity, traceability and data availability are always asked.[14] With respect to the availability of data, the Cloud allows greater availability in time and space compared to conventional storage systems.[15] Indeed, the cloud allows availability ranging from 99.95% to 99.99% per year.[16] For 0.05%, this corresponds to 4.4 hours of downtime a year, in a continuous or discontinuous mode.[9]

Given the vital importance of the availability of information in medical practice, what would happen in the case of a medical emergency where instant access to patient information is critical? The question of availability also arises with interoperability problems that could happen between the Cloud and other technologies used by the client, but also between different Clouds that are involved in the same customer service. Indeed, it could be very difficult, if not impossible, to interconnect these systems together, especially in the current situation where each Cloud is often sold with its own architecture and interface.[17] Therefore, it could be difficult to transfer or exchange data between the different parties.[18] The significant levels of security and protection of data offered by the Cloud do not necessarily guarantee their integrity. In this case, how would we know if the data available via the Cloud exactly conform to the original data?[19]

Furthermore, the content of the electronic medical record is subject to the same requirements as the paper medical record. That said, telehealth involves new elements that modify the content and the nature of the patient record. Thus, new issues and difficulties are emerging regarding the production, management and protection of information, including pictures and

documents exchanged electronically, etc..[20] The question that arises in this case remains the “real” place of preservation of the information, which remains very complex especially with the Cloud.

The question of data preservation also refers to the concern of organizations and States of loss of control and "sovereignty" of the data, because many of the cloud providers are unable to guarantee the actual location of the centres where data are stored.[9] This is a central issue as some jurisdictions require that information be stored on physical servers located in their territory.[20] However, this requirement is not obvious or readily applied in practice. This is mainly due to legal frameworks that are not synchronised with the reality of growing use of smart phones and tablets,[21] which are often on systems that use the Cloud technology.[22,23]

This transcendence of geographical borders brings questions and concerns in respect to the protection and securing a person’s data. The situation is even more complex given that the requirements for data control and protection and regulation of information flow are very different from one country to another. The issue of jurisdiction has a major impact on which laws are applicable in the event of disputes.[18] This regulatory gap can result in a lack of control by patients and States of the data, including how medical information is exchanged and managed. In this sense, the guarantees of confidentiality, portability and integrity of transmitted or received data are not currently present.[24,25]

Telehealth: the cloud provider as a new participant in the provision of services

Telehealth involves the use of ICT to make contact and exchange information and data between a healthcare professional and a patient or between two or more healthcare professionals.[26] Thus, the *telemedical* act cannot be done without the intervention of a new “technological actor". This situation refers to the question of the definition of the responsibilities of the various stakeholders in the light of the arrival of the third party technology in the landscape. According to some authors, this situation generates an "erosion" in responsibilities.[13,27,28]

Several technology providers can intervene in a telehealth service. For example, the Cloud service provider intervenes to ensure good transfer and availability of the patient’s history, as well as data and images required for the proper conduct of a telehealth session to establish a diagnosis or for patient follow-up. Telehealth can be considered as a medical device and must meet the requirements and compliance standards with the obligation for the user to declare and report risks of malfunction or incidents that can alter the security and integrity of the patient’s data.[13] Thus, in case of unavailability of information and data, or truncated or altered data, which may result in harm to the patient, what would be the degree of responsibility of the Cloud provider? How can this responsibility be distinguished from that of other technology providers? Furthermore, what would be the degree of responsibility of the healthcare professional, because the risk of unintentionally engaging the responsibility of the latter is still present?

The novelty with telehealth is that the responsibility is no longer limited solely to clinical considerations. Thus, for data transiting in the Cloud, the service provider could be held liable. Indeed, in cases of technical problems during a teleconsultation or transmission of patient data, one or more providers could be held responsible.[13] In these cases, liability could not be entirely that of the healthcare professional but would be shared between the provider of the technology (including the Cloud), the Internet network and organizations.

The role of the technology provider has moved from that of a simple “*business partner*” to an intervener in the provision of medical services to patients. This new status requires new responsibilities for the protection and security of patient data.[18] In the case of the Cloud, it implies the possibility of having several providers who are involved in the same service, via subcontracting contracts between providers. These providers can be located in different territories and jurisdictions, thus increasing contractual and regulatory frameworks that could apply.[29,30] This complicates any attempt to formalise the contractual and management conditions needed to identify the "real" places of backup and hosting information.

In addition, this multiplication of providers also increases the risk that the client will not be able to control and manage his data appropriately including changes or limitation of access to information in the medical record (e.g. in the medical history).[31] In this sense, how to ensure that data removal is well effected without leaving traces that could be detrimental to the

patient and organizations, particularly in the case of their use by external third parties (ex: insurers, pharmaceutical companies, etc.)?

Still on the question of the “physical” location of information, which can be located almost anywhere on the planet, if the data are stored in a jurisdiction other than that of the client (the owner), what law will be applied in case of prejudice, that of the country of data storage, the client, or the technology provider (if the jurisdiction of headquarters is different from that of the place of storage)?[9] In the light of new realities that have emerged with the Cloud this situation requires an in depth understanding of nuances and subtleties inherent in regulatory frameworks and compliance requirements.[18] There is a need, therefore, to review the classical definition of subcontracts.

Future directions

Both for telehealth and for the Cloud, we are facing a social innovation that disrupts the practice but also our concept of service and the notion of medical care. In the context of a growing ageing population, increasing prevalence of chronic diseases and comorbidities, and the will of citizens to have an active role in managing their health and their disease, ICTs are an integral and ever growing part of this new ecosystem service that is emerging. We can already see from the proliferation of health platforms, applications of m-Health, etc.[32-34]

As stated by Marston & al., "*Cloud computing is here to stay...*".[9] In fact, this technology offers significant opportunities for improving the quality and access of health services in the era of telehealth and digital health. The Cloud is perhaps one of the missing links for better integration of telehealth into routine health activities and organizations which require optimum fluidity in the exchange and management of medical and administrative data while requiring the highest security levels that exist. Thus, we are away from the time when patient records could be left on trolleys along the hospital corridors. This promise implies the importance that States invest and focus on the topic, given that the Cloud can be a lever for improving the performance of the health system.

Indeed, beyond its potential, the Cloud brings a number of issues and challenges that governments and health organizations must take into account. One of these challenges is characterised by the globalisation of data transfers as they may cross several jurisdictions and countries. This point refers to the sensitivity of the issue of "sovereignty" of states on their data, especially their regulatory requirements on access, integrity, confidentiality and portability of data of their citizens and organizations. This issue is even more sensitive as countries where data transit may not have the same standards or regulations, which could be detrimental, especially in the absence of agreements between countries, but also between countries and industries. In this sense, the Cloud is the perfect example of such a dilemma that governments and industry must manage to make the most of the potential of this technology by implementing adequate regulations. This would ensure levels of security and optimum data protection, while avoiding rigid regulations that could threaten this innovation.

In this context, the responsibility of "sovereign jurisdictions" as regulators becomes more complex. This requires Cloud providers to respect national rules and laws on the exchange, access and protection of information and places States in "grey" areas where the imperative of compliance with their rules is increasingly uncertain. This is partly explained by the fact that they are devoid of any means of pressure or control, especially when it comes to providers that are located in jurisdictions or countries that do not have the same standards and requirements of regulations.

In this landscape, we should now consider technology providers as stakeholders and partners in all the processes of implementation and formulation of standards and regulations. In the field of health we can no longer consider the provider as a mere "seller", but as a full-fledged member of the care team and a major player in the reorganization of the health system. All actors must now get around the table in a context of shared responsibility, but also a shared mission of quality, effectiveness and performance of health systems. This new role should push technology providers to revise their business models and review the scope of their "social responsibility" in a more comprehensive way.

In Europe, the new agreement on "the protection of personal data" adopted by European countries in June 2015 is perhaps the beginning of international harmonization of laws and regulations of compliance, at least at the level of the European Union.[35,36] Although it may be very difficult to operationalise, this approach in itself confirms that such a question cannot be addressed by each country in isolation, but must now be dealt on a geopolitical scale with a leadership that now exceeds the sole national considerations to

integrate a global perspective.[18] It is also a major step to improve the dissemination and use of ICT, particularly in the health sector which is struggling so far to benefit from the full potential of the technology. This is explained by varying issues of security and regulations between countries, but also by the gap existing between legislation and the technological reality.

For the Cloud, this is also perhaps the end of fragmentation of regulations, which slows down the development of a uniform market, with more regulatory transparency. Indeed, the proliferation of regulations also makes it difficult for providers to have an overview of their markets, particularly in terms of requirement and standards to meet whenever they offer their services in a given territory. This European initiative is, in our opinion, interesting to monitor because it could pave the way to agreement and advance an issue of fundamental importance, in the context of multiple countries with different social, cultural and political traditions, and varying economic and technological levels. In this sense, policy makers and regulatory authorities should take into account the changing international context in terms of policies and strategies for ICT implementation. This is no longer a choice, but a fundamental duty insofar as digital health and e-health can no longer be ignored in strategies to improve the effectiveness and efficiency of contemporary health systems. Thus, decision makers must be sensitive to the multiple changes going on, the first challenge being not to "miss" the digital shift that is taking place worldwide.

Telehealth, with all the promises associated with it in terms of improving access to care and services, cannot fulfil its mission if the requirements of optimization and fluidity of trade and timely access to medical information are not met. Indeed, the availability of information and the fluidity of its exchanges are now “the sinews of war” of modern medicine (e.g.: epidemic breakouts, natural catastrophes, health emergencies, etc.). The Cloud could easily provide answers to such challenges if the standards and regulations are well adapted, and shared at a transnational scale. This will reduce the risk of regulatory “gap” between countries and jurisdictions and allow transparency at both the State and industry levels leading to successful reorganization of health systems.

Conclusion

With the central role that ICT, including telehealth and Cloud Computing, is taking in the delivery of care and services health systems are currently in upheaval. It is time for society to debate the choices and orientations of eHealth in health policy. Indeed, the debate is no longer limited to the issue of using a technology or not, but goes far beyond the question to cover the service type set up, as well as the choice to make for better protection and exchange of medical and administrative information of patients-citizens. ICT involve major societal changes, "for better or for worse".[37] This, in a context where the notion of national geographical boundaries no longer means the same, nor national regulations have (or little) power beyond their sovereign borders. Thus, the complexity of such contexts leads to favour involving, more than ever, citizens in decisions on regulatory and health policies that are made increasingly difficult by the challenges raised by ICT. It is with an active citizen, as a decision-making partner, that policymakers can make informed decisions on topics that are at the heart of the transformations that contemporary health systems are experiencing.

.....

Corresponding author:
Hassane Alami, PhD(c)
Axe Organisation, Informatisation et Évaluation
Centre de recherche sur les soins et les services de première ligne de l’université Laval (CERSSPL-UL)
880, rue Père-Marquette, 3e étage.
Québec (QC), G1S 2A4. Canada.
Tel: (+1) 418 681-8787 ext. 3706
eMail: hassane.alami.1@ulaval.ca

Conflict of Interest. The authors declare no conflicts of interest.

References

1. Kay M, Santos J, Takane M. mHealth: New horizons for health through mobile technologies. Global Observatory For eHealth vol 3. Geneva, World Health Organization, 2011:66-71.
2. Potter A, Mueller K, Mackinney A, Ward M. Effect of tele-emergency services on recruitment

and retention of US rural physicians. *Rural Remote Health*. 2014;14(3): 2787.
3. Margolis KL, Asche SE, Bergdall AR, et al. Effect of home blood pressure telemonitoring and pharmacist management on blood pressure control: a cluster randomized clinical trial. *JAMA* 2013;310(1):46-56.
4. Schulz R, Wahl H-W, Matthews JT, Dabbs ADV, Beach SR, Czaja SJ. Advancing the aging and technology agenda in gerontology. *Gerontologist* 2015;55(5):724-734.
5. Clarke M, Shah A, Sharma U. Systematic review of studies on telemonitoring of patients with congestive heart failure: a meta-analysis. *J Telemed Telecare* 2011;17(1):7-14.
6. Monteiro EJM, Silva LAB, Costa C, editors. CloudMed: Promoting telemedicine processes over the cloud. Information Systems and Technologies (CISTI), 2012 7th Iberian Conference on; 2012: IEEE.
7. Rajaraman V. Cloud computing. *Resonance* 2014;19(3):242-258.
8. Mell P, Grance T. The NIST definition of cloud computing [Recommendations of the National Institute of Standards and Technology-Special Publication 800-145]. Washington DC: NIST. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf accessed 5 March 2015.
9. Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A. Cloud computing—The business perspective. *Decis Support Syst* 2011;51(1):176-189.
10. Parikh A, Mehta N, editors. PACS-Next Generation. *Proc of SPIE* 9418, Medical Imaging 2015. PACS and Imaging Informatics: Next Generation and Innovations Available at: http://dx.doi.org/10.1117/12.2081987 accessed 13 October 2015.
11. Zombek L. Du suivi trans-téléphonique au cloud computing: quelles sont les technologies de la télécardiologie? Mémoire d'études, Université Libre de Bruxelles, 2015. Available at: http://student.ulb.ac.be/~lzombek/ASI.pdf accessed 13 October 2015.
12. Hsieh J-C, Li A-H, Yang C-C. Mobile, cloud, and big data computing: contributions, challenges, and new directions in telecardiology. *Int J Environ Res Public Health* 2013;10(11):6131-6153.
13. Alami H, Gagnon M-P, Fortin J-P, Kouri R. La télémédecine au Québec: état de la situation des considérations légales, juridiques et déontologiques. *Eur Res Telemed* 2015;4(2):33-43.
14. Bastiao Silva L, Costa C, Silva A, Oliveira JL, editors. A PACS Gateway to the Cloud. Information Systems and Technologies (CISTI), 2011 6th Iberian Conference on; 2011: IEEE.
15. Bolan C. Cloud PACS and mobile apps reinvent radiology workflow. *Appl Radiol* 2013;42(6):24-29.
16. Gupta PKD, Nayak M, Pattnaik S. Cloud computing: based projects using distributed architecture. PHI Learning Pvt. Ltd. 2012.
17. Toosi AN, Calheiros RN, Buyya R. Interconnected cloud computing environments: Challenges, taxonomy, and survey. *ACM Computing Surv* 2014;47(1):7.
18. Seddon JJ, Currie WL. Cloud computing and trans-border health data: Unpacking US and EU healthcare regulation and compliance. *Health Policy Technol* 2013;2(4):229-241.
19. Sébastien S. Les enjeux du Cloud Computing comme support à la télémédecine, 2014. Available at: http://www.journaldunet.com/solutions/expert/56601/les-enjeux-du-cloud-computing-comme-support-a-la-telemedecine.shtml accessed 9 July 2015.
20. Brunette G, Mogull R. Security guidance for critical areas of focus in cloud computing v2. 1. Cloud Security Alliance 2009:1-76.
21. Xu B, Xu L, Cai H, Jiang L, Luo Y, Gu Y. The design of an m-Health monitoring system based on a cloud computing platform. *Enterp Inf Syst*2015(ahead-of-print):1-20.
22. Wu H. Analysis of mHealth Systems with Multi-cloud Computing Offloading. In: Adibi S editor. Mobile Health. Switzerland: Springer; 2015;589-608.
23. Fernandez-Llatas C, Pileggi SF, Ibañez G, Valero Z, Sala P. Cloud Computing for Context-Aware Enhanced m-Health Services. In: Fernandez-Llatas, Garcia-Gomez JM editors. Data Mining in Clinical Medicine: Springer. 2015;147-155.
24. Kumar C. *Cross-border data flow regulation and data privacy law*. Oxford, Oxford University Press, 2013.

25. Vermeys MN, Gauthier MJ. Étude sur les incidences juridiques de l'utilisation de l'infonuage par le gouvernement du Québec. Étude présentée au Conseil du Trésor du Québec ; Québec; 2014.
26. Monteiro EJM, Silva LAB, Costa C, editors. CloudMed: Promoting telemedicine processes over the cloud. Information Systems and Technologies (CISTI), 2012 7th Iberian Conference on; 2012: IEEE.
27. Card RF. Individual responsibility within organizational contexts. *J Bus Ethics* 2005;62(4):397-405.
28. Stanberry B. Telemedicine: barriers and opportunities in the 21st century. *J Intern Med* 2000;247(6):615-628.
29. Iyer B, Henderson JC. Business value from clouds: learning from users. *MIS Q Executive* 2012;11(1):51-60.
30. Iyer B, Henderson JC. Preparing for the future: understanding the seven capabilities cloud computing. *MIS Q Executive* 2010;9(2):117-131.
31. Berry R, Reisman M. Policy challenges of cross-border cloud computing. *J Int Commer Econ* 2012;4(2):1-38.
32. Kay M, Santos J, Takane M. mHealth: New horizons for health through mobile technologies. Global Observatory For eHealth Vol 3. Geneva,World Health Organization. 2011:66-71.
33. Kumar D, Arya M. mHealth is an innovative approach to address health literacy and improve patient-physician communication–an HIV testing exemplar. *J Mob Technol Med* 2015;4(1):25-30.
34. Pramana G, Parmanto B, Kendall PC, Silk JS. The SmartCAT: an m-health platform for ecological momentary intervention in child anxiety treatment. *Telemed e-Health* 2014;20(5):419-427.
35. European Commission. Stronger data protection rules for Europe, June 2015. Available at: http://europa.eu/rapid/press-release_MEMO-15-5170_en.htm accessed 15 August 2015.
36. European Commission. A Digital Single Market Strategy for Europe, June 2015. Available at: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf accessed 15 August 2015.
37. Currie WL, Seddon JJ. Social innovation in public health: can mobile technology make a difference? *Inf Syst Manage* 2014;31(3):187-199.