B Sides
http://ir.uiowa.edu/bsides
U of I SLIS Journal

11|16|2010

Cloud Computing and Health Information

Leah C. Osterhaus

Editors | Julia Skinner and Katie DeVries Hassman
Associate Editors | Melody Dworak & Samantha Bouwers
Faculty Advisor | Jim Elmborg
Layout & Identity design | Colin Smalter

Abstract:

Osterhaus discusses cloud computing technologies and their impact on healthcare and implications for privacy and the collection of medical records.

Keywords:
Cloud computing | the cloud | privacy | health information | health records | medical records

B Sides Fall 2010
http://ir.uiowa.edu/bsides/19

Cloud Computing and Health Information

Technology is increasing the connectedness of society. People use cell phones, the Internet, and handheld devices to stay in-touch and connected with friends, family, and work. A recent study conducted by the Pew Internet & American Life Project found that 74% of American adults use the Internet and that 55% of adults connect wirelessly, either using WiFi or WiMax via their laptops or using handheld devices, such as a smart phone (Rainie, 2010).

In the 1960s, long before the advent of laptops and smart phones, computing relied on mainframe systems, which often filled entire rooms. In the 1980s microcomputers enabled people to use desktop computers for processing that previously had been completed on mainframes. Web-based services, which have been widely offered since the 1990s, started the transition of computing power from desktop computers to the Internet (Fox, 2009). Now web-based applications are emerging that reside in cyberspace and use the infrastructure of the Internet for "cloud computing".

Cloud computing is a computing architecture that "links computers in a grid and allows users to buy access to data and software stored on the grid or processing power that is harnessed for specific purposes by the grid of computers" (Horrigan, 2008, p.3). Businesses, such as Amazon and Google, have invested in creating distributed grid computing architecture and use this architecture to provide services that historically have been desktop-based. Cloud computing includes: infrastructure as a service (IAAS), platform as a service (PAAS), and software as a service (SAAS) (Rubin, 2010).

Internet users use the cloud to store data, process data, and collaborate on documents, excel spreadsheets, and more. Users that upload content to "the cloud" are storing information on distant servers instead of on their own hard drives. Likewise, using software in "the cloud" means the user is interacting with applications on the Internet instead of on their personal computer. Cloud applications are often provided to companies for a subscription fee (Rubin, 2010) or as a pay-as-you-go service (Jaeger, Lin, Grimes & Simmons, 2009). Other cloud applications, such as email, are offered without fees but often have hidden costs, such as in the form of advertisements. Cloud computing eliminates boundaries because everything in the cloud is accessible from any location, as long as there is a way to connect to the Internet.

Many Internet users use cloud computing applications, although they may not know the term "cloud computing" or realize that what they are doing is classified as such. Consumer services such as email (Gmail, Hotmail, Yahoo Mail), social networks (Facebook, MySpace), virtual worlds (Secondlife), photo and video services (Flickr, YouTube) and online applications (Google Docs, Adobe Express) represent some of the most visible cloud computing applications (Nelson, 2009). Consumers of these services upload and store personal data to remote servers, which they can then access at any time from any location. The Pew Internet & American Life Project reported that 69% of all online Americans make use of cloud computing by either storing data online or using a web-based software application (Horrigan, 2008).

SAAS and other cloud computing services are appealing to organizations for many reasons, most of which involve cutting costs. Cloud vendors have the bulk of the responsibility for software upgrades, infrastructure support, security, storage, and hardware (Fox, 2009). Shifting these responsibilities to the vendor saves the organization both time and money. The major disadvantages to cloud computing include less control of data and lack of local customization of applications. Customers don't know where their information is being stored or processed when it is in the cloud, therefore they must have total trust in the cloud system that is controlling their data.

Organizations that handle private consumer information, such as law firms and hospitals, need to be cautious about cloud computing because of security and client privacy. Society's increasing level of connectedness and level of comfort with online applications and data storage results in high expectations in regards to quick and easy information access. In a medical setting, the cloud offers the potential of easy access to electronic medical records. Quick access to a person's medical history could speed up treatment, help avoid complications, and even save lives (Gottlieb, Stone, Stone, Dunbrack & Calladine, 2005). However, the use of cloud applications in health care introduces another potential place for security breaches and invasions of patients' privacy and also adds complications to current privacy policies.

Privacy, confidentiality, and security are important features of health informatics applications. Security is the system's ability to protect itself and its data, confidentiality requires assigning permission levels for access to information, and privacy addresses the amount of control an individual has over what data is collected on them and who has access to the data (Wood, 2008). Americans are concerned about their privacy and the security of their personal information. Samuel Warren and Louis Brandeis vocalized the concept of law protecting privacy in their 1890 journal article *The Right to Privacy* (Warren & Brandeis, 1890). The United States created such a law for records maintained by the federal government with the Privacy Act of 1974.   The Privacy Act "establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies" (United States Department of Justice, 2010). The Act prohibits the unauthorized disclosure of the information it protects and gives individuals the right to review and request amendments for records about themselves (United States Department of Health & Human Services, 2010). In addition to the Privacy Act, there are a number of US laws that pertain to other aspects of privacy beyond federally controlled documents. Medical information is addressed and protected in the Health Insurance Portability And Accountability Act of 1996 (HIPAA). In 2001 the HIPAA Privacy Rule was issued by the Department of Health and Human Services to further protect individuals' personal health information. The Privacy Rule requires all included entities (health plans, hospitals, clinics, health care providers) to have policies that protect individually identifiable health information that contain at least 1 of 18 identifiers (Wilson, 2006). Examples of identifiers are: names, Social Security numbers, phone numbers, and addresses. A proposal with the American Recovery and Investment Act expanded the security and privacy provisions of HIPAA and the Privacy Rule to the business associates of the currently covered entities (Pike, 2009). This extension, called the HITECH Act, requires that cloud computing applications used by health care entities adhere to HIPAA (Rubin, 2010).

Currently the technical, legal, economic, and security details of the cloud remain undefined (Nelson, 2009). Data in the cloud could be stored and processed on servers residing in countries all over the world. How privacy and ownership issues are addressed worldwide could impact the development and acceptance of cloud computing for health care organizations. Many of the policies that would address the larger security issues with the cloud would have to be set by government. Health organizations can create policies for how their data is managed locally and how their data is managed by an outsourced data center, however they are unable to create policies that will impact how data is handled in the cloud.

Health IT in the cloud could be successful without government regulating policies as long it can satisfy the rigorous legal and risk management requirements of health organizations (Rubin, 2010). Harry Rubin identified 6 prisms of risk relating to Health IT structure that must be met for the cloud to be acceptable for health information. Regulatory risks, one of the six prisms, are those that involve meeting HIPAA regulations. Addressing regulatory risks would include activities such as encrypting data and preventing unauthorized access. Other risks identified by Rubin are: performance, intellectual property, liability, business continuity, and enforcement (Rubin, 2010).

Americans have conflicting values in regard the use of cloud computing for health information. On one hand society desires the instant gratification, easy access, and connectedness that the Internet provides in their daily lives. The boundary-less access offered by the cloud could aid health professionals with patient care. Quick access to electronic medical records would help emergency departments by supplying important information about a patient's medical history and current prescription medications (Gottlieb et al, 2005). Also, the cloud could make it easier for patients to locate and keep track of their own medical history. However on the other hand society wants privacy and guarantees that their health information is secure. Peoples' desire for privacy has resulted in records being stripped of identifying information to comply with HIPAA. Also, the fluidity and openness of the cloud makes it difficult for cloud vendors to meet the security and privacy requirements of health care organizations and HIPAA. The current structure and law surrounding health information indicate that the need for privacy trumps the need for access. Before cloud computing can be fully embraced as a structure for Health IT vendors must gain the trust of a concerned society by demonstrating that they can meet HIPAA regulations and minimize all areas of risk.

References

Arnold, S. E. (2008). Cloud computing and the issue of privacy. *KM World, 17*(7), 14-22.

Couillard, D. (2009). Defogging the cloud : Applying fourth amendment principles to evolving privacy expectations in cloud computing. *Minnesota Law Review*, 93, 2205-2238.

Gottlieb, L. K., Stone, E. M., Stone, D., Dunbrack, L. A., & Calladine, J. (2005). Regulatory and policy barriers to effective clinical data exchange: Lessons learned from medslnfo-ED. *Health Affairs, 24*(5), 1197-1204.

Horrigan, J. B. (2008). *Use of cloud computing applications and services*. The Pew Internet & American Life Project. Retrieved January, 2010, from http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx

Jaeger, P. T., Linn, J., Grimes, J. M., & Simmons, S. N. (2009). Where is the cloud? geography, economics, environment, and jurisdiction in cloud computing. *First Monday, 14*(5)

Malin, B., Karp, D., & Scheuermann, R. H. (2010). Technical and policy approaches to balancing patient privacy and data sharing in clinical and translational research. *Journal of Investigative Medicine, 58*(1), 11-18.

Murley, D. (2009). Law libraries in the cloud. *Law Library Journal, 101*(2), 249-254.

Nelson, M. R. (2009). The cloud, the crowd, and public policy. *Issues in Science & Technology, 25*(4), 71-76.

Nicholson, S., & Smith, C. A. (2007). Using lessons from health care to protect the privacy of library users: Guidelines for the de-identification of library data based on HIPAA. *Journal of the American Society for Information Science & Technology, 58*(8), 1198-1206.

Pike, G. H. (2009). HIPAA gets new privacy rules. *Information Today, 26*(4), 13-15.

Rainie, L. (2010). *Internet, broadband, and cell phone statistics*. The Pew Internet & American Life Project. Retrieved February 7, 2010, from http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx

Rubin, H. (2010). Risk and reward: Health IT SAAS licensing models. *Licensing Journal, 30*(1), 13-15.

United States Department of Health & Human Services. (2010). *Health Information Privacy*. Retrieved February 7, 2010, from http://www.hhs.gov/ocr/privacy/index.html

United States Department of Justice. (2010). *Privacy and Civil Liberties Resources*. Retrieved February 7, 2010, from http://www.justice.gov/opcl/prr.htm

Warren, S. V., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220.

Wilson, J. F. (2006). Health insurance portability and accountability act privacy rule causes ongoing concerns among clinicians and researchers. *Annals of Internal Medicine, 145*(4), 313-316.

Wood, S. (Ed.). (2008). *Introduction to Health Sciences Librarianship*. New York: Haworth Press.