Cloud Computing and Patient Engagement

Here's how to leverage available technology.

BY ALICE NOBLIN, PHD, KENDALL CORTELYOU-WARD, PHD, AND ROSA M. SERVAN

Cloud-based systems have interoperability potential with electronic health records (EHRs), personal health records (PHRs), computerized physician order entry (CPOE), home monitoring systems, and many other record-keeping or data-exchanging systems used by healthcare organizations.[1] With a patient's consent, the information stored within these record-keeping systems can be exchanged or accessed by other organizations via the cloud system.

This type of storage would allow for a faster exchange of information via the Internet, because everything could be housed within the cloud system.[2] Outside organizations could be provided specific login information that would grant access to only the data for which they have security authorization. This would improve communication between practitioners, thus improving the coordination of care through efficient data exchange. Exchanging data between practitioners and organizations in a quicker, more efficient manner leads to greater patient satisfaction.[2] This would also shorten the amount of time that elapses between a patient's request for his or her own personal health information and the time when it is actually received.

The American Recovery and Reinvestment Act of 2009 (ARRA) included the Health Information Technology for Economic and Clinical Health (HITECH) Act. HITECH will require patient portals and other means of secure messaging between patients and physicians to earn reimbursement as part of Meaningful Use requirements for Medicare and Medicaid subsidy programs in the future.[3] In addition to improved patient–physician communication benefits, this engagement in the healthcare process offers patients the opportunity to take control of their healthcare and be active participants in decision-making.[4]

Many people find that being able to participate in the formation and ongoing supervision of their own care improves their satisfaction and actually motivates them to follow instructions and treatment plans. A distinct advantage of both PHRs and portals is that they allow the patient to be an active member of the medical team and not just a passive consumer of healthcare services.

© Shao-chun Wang | Dreamstime.com

Cloud Computing (from page 65)

A patient portal is a cloud-based application that allows secure, confidential, and efficient access to personal medical information and communication between patient and provider. This access can be provided via Web sites apart from a provider's existing Web site, within the provider's existing Web site, or through a provider's EHR.[5] Via the portal, patients may view or enter their own medical information online, complete forms, send secure messages to physicians, view and apply payment to accounts, request appointments, or download their information into a PHR.[5]

Personal Health Record

A "personal health record" is defined as "an electronic, lifelong resource of health information needed by individuals to make health decisions."[6] As implied by its name, the PHR is maintained by the patient and is not considered to be a part of the legal medical record. A PHR can be tethered to a physician's EHR, which provides a direct link between the patient and provider. One advantage of the PHR is its ability to provide improved communication between the patient and physician, thereby allowing the patient to become more engaged in the healthcare process.[7,8]

Patients have some choices as to the format of the PHR, such as whether they prefer hard copy/paper records, documents on a disk or USB drive, or an online record possibly connected (tethered) to a physician or other provider(s). One method of storing Web-based PHRs is the use of a cloud-based computing system, which can be accessed remotely via the Internet at any time from any location. These systems have the potential to enhance health information exchange, which cannot be done with hard copy records or documents on a USB drive.

Patient Portals

Increasing patient engagement by providing patient portal access increases efficiency and decreases costs for healthcare providers by means such as lowering phone bills or printing costs. Patient portals also assist in streamlining processes re-

lated to routine patient communications, such as completion of forms, scheduling, educational material, prescription refills, or billing. In addition to the benefits provided to patients, providers also stand to gain from the implementation of a patient portal in their efforts to meet Meaningful Use compliance guidelines.

The Office of the National Coordinator for Health, the Centers for Medicare & Medicaid Services, and the Department of Health and Human Services established Meaningful Use

regulations in a three-stage process to ensure the adoption and use of certified health information technology. Meaningful Use compliance guidelines focus on the improvement of patient outcomes through the establishment of electronic methods of data collection, information access, communication, and improved clinical outcomes. These guidelines were established to improve safety and efficiency of care, increase quality of care while reducing health concerns and engaging patients, and improving the coordination of care with an emphasis on privacy and security of patient health data.[9]

Meaningful Use Stage 2

In Meaningful Use Stage 2, healthcare professionals are required to provide electronic copies of health information, such as medication lists or lab results, to patients upon request, providing electronic access to this information within four days of the information being available to the provider and clinical summaries within three business days of a clinical visit, and also to establish secure messaging methods to communicate with providers.[9] These functions can be implemented within a patient portal.

In addition to providing electronic access to personal health information, a patient portal allows patients to view or request appointments, update personal information, access medication lists or lab results, send secure communications to their provider, and

submit other medical requests, such as refills or referrals, that normally would be handled by staff.[9]

Consequently, the portal will continue to assist healthcare professionals in the daily operations of their organization while also providing near-instant access to patients online.

When considering types of cloud-based programs and deployment models, providers should consider what type of access they wish to grant to individuals within their office and whether they wish to allow any others

HIPAA regulates who uses or discloses personal information.

to access their records. Four types of cloud-based system deployment models are available: public, private, community, and hybrid.[10] These models provide the basic groundwork regarding who is able to operate, manage, or share the information contained within the specific cloud.

Public Cloud

In a public cloud, all resources, applications, and stored data are made available to everyone over the Internet.[10] This is an open access model—the information stored within the cloud would be viewable by the general population and is not restricted. The risks of a public cloud service include a lack of confidentiality of patient health information. Although the information would still be available for use within the business, the general population also could access all data saved to this public cloud. In other words, a public cloud is not useful for PHRs or portals, but is suitable for providing health tips and guidelines to the general public.

A private cloud is operated, managed, and shared by a single office.[10] All resources and applications are available only for that business. This model often is selected due to concerns regarding security of in-house information and for research and teaching facilities, because it makes stored data accessible to anyone within the office who is granted access to the private cloud.[11] Many

Cloud Computing (from page 66)

offices may opt to use a private cloud for PHRs and portals to avoid concerns related to improper use of confidential patient health data and other privacy concerns.[10] This would be ideal for solo practitioners or other small healthcare entities. However, other options are available for providers in partnerships where several people need to access the same information.

Community Clouds

Community clouds are accessed, operated, managed, and shared by more than one administrative center with a common purpose, requirements, and regulations.[10] For example, Patient-Centered Medical Homes or Accountable Care Organizations have the same healthcare objectives of improved patient satisfaction and outcomes, as well as the same federal compliance regulations for privacy such as HIPAA. One group could maintain the databases in-house, or there could be a third-party vendor to manage and store all patient information.[11]

Hybrid Clouds

A hybrid cloud would include two or more of the previously discussed cloud systems—private, public, and community models.[10] A combination of the three cloud systems could potentially provide the best option, depending on the medical practice and its objectives. For example, if an office wished to maintain a database of its own patient information while also allowing certain resources to be available to other medical practices, a hybrid cloud system combining private and community would be beneficial. Such a system could be used by hospitals with several local clinics, or research hospitals providing certain information for use by research institutions.[11] As with any computing system that allows for shared information, however, there will be concerns regarding the privacy, safety, and confidentiality of information.

Privacy and Security

Overall objectives regarding privacy and confidentiality of information include protection of data, networks, and communication against misuse, natural disasters, virtual attacks, or other types of network breaches.[12] Meeting these objectives would ensure the availability, confidentiality, and integrity of healthcare information and services. Several key points must be considered regarding privacy and security of patient health information, such as HIPAA regulations, data storage, or any organization permission settings.[12]

When considering safety of information within the organization, authenticated logins for all users ensure protection of health records and encryption of data for proper data exchange within or outside of the organization, as well as maintaining access control via permission settings.[2] HIPAA regulates who uses or discloses personal information as well as if, when, and how it is used or disclosed. Encryption of data for proper data exchange is especially important to guarantee the safe exchange of data, and setting specific access control is beneficial for accessing such information.

Organizations should consider which techniques they would prefer for data backup services and disaster recovery. One approach is to store multiple copies of data across several servers.[2] This can be done by an in-house IT department or by an outsourced company for data storage. This choice would depend on the organization's current IT department capabilities and the organization's desire to outsource or control for cost when storing in-house servers.

Outsourced data storage units have been found to be more secure as compared with healthcare facilities and organizations, not just on a technical level, but also due to the server physical location being off-site. It would be difficult for an individual to steal data from server farms that store sensitive patient data, because determining which servers contain critical personal information versus noncritical information would be extremely challenging.[13]

Firewalls and protected, private networks still will be necessary when any model of cloud computing is used.[13] A firewall analyzes any data coming into the network or leaving the network. In a cloud-based system that allows for data exchange between organizations or even other systems, maintaining secure firewalls becomes very important. These methods should be coupled with regular maintenance and other protective software, such as notifications if a network breach occurs or regular virus scans. The system also should have the ability to continue operating if such a breach were to occur in order to prevent an automatic shutdown or freezing of the system.[12]

Access control means that specific privileges or permission settings are established to limit the amount or type of information accessible by specific users or groups of users.[14] For instance, certain users can be provided access to specific contact informa-

Data monitoring systems can transfer real-time data to the cloud 24/7.

tion. Another tier of users, such as healthcare providers, can be provided access to private, health-specific information. Insurance providers may have a separate permission setting for information that specifically relates to billing purposes. An administrative permission set would allow administrative access to all information within the system for reporting or analytic purposes, as made possible by the cloud-based system.[14] Administrative entities can then use these analyses to further improve patient satisfaction, outcomes, and healthcare services.

Capabilities of Cloud Computing to Improve Quality of Care

Because a cloud-based computing system can be accessed from anywhere at any time, this enhances the efficiency of healthcare providers.[1] The system would include the ability to make notations or store data regarding the provider–patient encounter at the time of the encounter through the use of mobile devices connected to the cloud.[15] A healthcare provider can collect data from the patient and input the data di-

Cloud Computing (from page 68)

rectly into the patient's record through the cloud system immediately, in the presence of the patient. This reduces typing errors and issues of the reliability of memory.[10] Inputting findings and health information in the room with the patient can ensure that the information remains accurate and true to the patient's expressed concerns.

Another opportunity provided by a cloud-based system is the addition of a network of sensors attached to medical devices used to monitor patient health data, such as heart rate.[10] In fact, data monitoring systems, either bedside at the healthcare facility or at home, can transfer real-time data to the cloud 24 hours a day, 7 days a week.[10] This information then can be processed and analyzed by another system or by

healthcare practitioners to detect patterns or monitor for specific concerns.

The cloud system also can store images, such as results of examinations or scans, which can be utilized by healthcare providers when meeting with patients.[15] These images also can be exchanged between networks of organizations or in-house departments for further review or consid-

TABLE 1:
Cloud Types Summary

Type of Cloud	Description	Ideal Use	Patient Engagement	Quality of Care
Public	• Open to everyone • Unrestricted access • Viewable by general population	• Distribution of general health information • Provide health tips and guidelines • Not ideal for patient portals	• Provides educational material but no means of communication between patient and provider	• Improved if patient reads and becomes engaged actively in care • Provider may share location with patients as educational resource • Improved communication regarding shared educational material
Private	• Operated, managed, shared by provider • Access restricted to preferred users, such as patients and staff	• Single office, solo practitioners • Private practices • Ideal for patient portals • Ideal for practices with privacy and security concerns	• Patients given an opportunity to interact with practitioners via portal or Web site • Means of communication between patient and provider	• Improves if patients are provided access to view or edit their own secured, patient information • Improved if used as an additional means of communication between patient and provider
Community	• Accessed, operated, managed, shared by more than one healthcare organization • Access is both restricted and unrestricted	• Larger healthcare providers • Patient-Centered Medical Homes • Accountable Care Organizations • In-house or third-party vendor maintenance • Ideal for patient portals	• Secure patient–provider messaging • Patient participates in own care • Patient may access both personal health information and educational resources	• Improved communication among providers • Improved coordination of care • Improved if patient accesses personal health information and educational resources • Improved patient engagement, if used, which may lead to improved satisfaction and outcomes
Hybrid	• Combination of two or more other cloud models—public, private, community • Flexible, based on provider needs	• Hospital with local clinics • Research hospitals • Larger healthcare providers with multiple locations	• May maintain the same advantages of patient engagement as the individual cloud models that are combined	• May maintain the same advantages and improvement to quality of care as the individual cloud models that have been combined

Cloud Computing (from page 70)

eration. These data can be retrieved at any time, which may be useful when comparing the progression of a health concern over time.

Having a cloud-based system at the healthcare provider's disposal also makes it possible to schedule patient appointments, schedule rooms for examinations, or devise medication and treatment plans.[1] This function allows the provider to view availability in real-time and limits the potential of scheduling or rescheduling, all of which would affect the patient experience. It also allows the provider to order specific medications and, depending on the capabilities of the office's EHR, also may demonstrate alerts or notifications of issues within the cloud. Because of the efficiency of the cloud system, alerts would be received before the patient was subject to any potential health risks.

Using the cloud to its full capabilities enhances efficiency; reduces the risk of clinical errors, and, therefore, clinical costs; and allows for a more personalized provider–patient experience. The waiting time for data exchange, extraction, or processing is significantly lessened. The ability to incorporate multiple system capabilities, such as CPOE or monitoring system sensors, allows for both a general and granular picture of the patient's health, which can improve health outcomes and patient satisfaction.[1]

Conclusion

Access to medical information, such as through a portal or PHR, has been shown to provide numerous benefits, such as improved communication with providers, improved understanding of treatment regimens, and, ultimately, improved compliance with healthcare plans.[16-18] Physicians must play an active role as the change agents for adoption, but ultimately the patient can control his or her destiny through adoption and continued active use of these systems. See Table 1 for a summary of cloud computing methods and their attributes. **PM**

References

[1] Low C, Chen YH. Criteria for the evaluation of a cloud-based hospital information system outsourcing provider. J Med Syst. 2012;36:3543-3553.

[2] Ahuja SP, Mani S, Zambrano J. A survey of the state of cloud computing in healthcare. Network and Communication Technologies. 2012;1(2):12-19.

[3] Hogan SO, Kissam SM. Measuring meaningful use. Health Aff (Millwood). 2010;29:601-606.

[4] Tang P, Lansky D. The missing link: bridging the patient-provider health information gap. Health Aff. 2005;24:1290-1295.

[5] Health Technology Review. Patient portal: what is a patient portal? http://www.healthtechnologyreview.com/patient-portal.php. Accessed June 18, 2014.

[6] Burrington-Brown J, Fishel J, Fox L, et al. Defining the personal health record. J AHIMA. 2005;76(6):24-25.

Cloud Computing (from page 71)

[7] Wolter J, Friedman B. Health records for the people. J AHIMA. 2005;76(10):29-32.

[8] Survey finds Americans want electronic personal health information to improve own health care. Markle Foundation. November 2006; www.markle.org/publications/1214-survey-finds-americans-want-electronic-personal-health-information-improve-own-hea.

[9] Health Technology Review. Meeting Meaningful Use Stage 2 with a Patient Portal. 2012; www.healthtechnologyreview.com/meaningful-use-stage-2-patient-portals.php. Accessed June 18, 2014.

[10] Kuo AMH. Opportunities and challenges of cloud computing to improve health care services. J Med Internet Res. 2011;13(3):e67.

[11] Dillon T, Wu C, Chang E. Cloud computing: issues and challenges. Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, April 20-23, 2010, Perth, Australia, pp. 27-33.

[12] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comput Syst. 2012;28:583-592.

[13] Rosenthal A, Mork P, Hao Li M, Stanford J, Koester D, Reynolds P. Cloud computing: a new business paradigm for biomedical information sharing. J Biomed Inform. 2010;43:342-353.

[14] Barua M, Liang X, Lu R, Shen X. ESPAC: enabling security and patient-centric access control for eHealth in cloud computing. International Journal of Security and Networks. 2011;6(2):67-76.

[15] Doukas C, Pliakas T, Maglogiannis I. Mobile healthcare information management utilizing cloud computing and Android OS. Proceedings of the 32nd Annual International Conference of the IEEE on Engineering in Medicine and Biology Society. August 31-September 4, 2010, Buenos Aires, Argentina, pp. 1037-1040.

[16] Green B, Cook A, Ralston J, et al. Effectiveness of home blood pressure monitoring, web communication, and pharmacist care on hypertension control: a randomized controlled trial. JAMA. 2008;299: 2857-2867.

[17] Hassol A, Walker J, Kidder D, et al. Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging. J Am Med Inform. 2004;11:505-513.

[18] Winkelman W, Leonard K, Rossos P. Patient-perceived usefulness of online electronic medical records: employing grounded theory in the development of information and communication technologies for use by patients living with chronic illness. J Am Med Inform. 2005;12:306-314.

Dr. Noblin is an Assistant Professor in the Health Informatics and Information Management Undergraduate Program Director at the University of Central Florida. She is the 2014 recipient of the AHIMA Triumph Research Award for her peer-reviewed publications and conference presentations.

Dr. Cortelyou-Ward is an Associate Professor and the Director of the Graduate Program in Health Care Informatics at the University of Central Florida. She has numerous peer-reviewed publications and regularly presents her research at academic and practitioner conferences.

Rosa Servan is a student in the Health Care Informatics graduate program at the University of Central Florida.