EDITOR'S CHOICE

Reconciliation of the cloud computing model with US federal electronic health record regulations

Eugene J Schweitzer

Department of Surgery, Division of Transplantation, University of Maryland Medical School, Baltimore, Maryland, USA

Correspondence to
Dr Eugene J Schweitzer, 29 S. Greene Street Suite 200, Baltimore, MD 21201, USA; gschweitzer@smail.umaryland.edu

Received 2 February 2011
Accepted 10 June 2011
Published Online First
4 July 2011

ABSTRACT

Cloud computing refers to subscription-based, fee-for-service utilization of computer hardware and software over the Internet. The model is gaining acceptance for business information technology (IT) applications because it allows capacity and functionality to increase on the fly without major investment in infrastructure, personnel or licensing fees. Large IT investments can be converted to a series of smaller operating expenses. Cloud architectures could potentially be superior to traditional electronic health record (EHR) designs in terms of economy, efficiency and utility. A central issue for EHR developers in the US is that these systems are constrained by federal regulatory legislation and oversight. These laws focus on security and privacy, which are well-recognized challenges for cloud computing systems in general. EHRs built with the cloud computing model can achieve acceptable privacy and security through business associate contracts with cloud providers that specify compliance requirements, performance metrics and liability sharing.

INTRODUCTION

The costs of electronic health records (EHRs) and their low return on investment are cited as the main barriers to adoption.[1,2] High costs accrue from the size and complexity of these systems, which must be useful to clinicians and administrators while complying with privacy regulations. Large, expensive systems designed with a traditional in-house, client—server architecture are typically purchased as a major capital expenditure by healthcare institutions and deployed within the corporate perimeter. The buyer also allocates funds to acquire, maintain, and upgrade the hardware to host the system, and supports an IT department to manage it. Vendors often charge substantial fees to code custom interfaces to outside EHR systems. This traditional approach makes EHR applications expensive to acquire and modify, and often renders them unresponsive to the business workflow and other special needs of individual clinical practice groups within the organization.

The software cost, complexity, and inflexibility issues of traditional EHR systems have also burdened other business sectors, which have developed modern, innovative architectures to resolve them. New approaches like cloud computing are emerging and gaining increasing attention.[3,4] These modern design patterns could be used to achieve more ideal EHR applications (table 1).

CLOUD COMPUTING

Widespread connectivity to computers outside our own office, company, and even national boundaries provides the pre-requisite for recent trends like cloud computing. The internet itself is sometimes referred to as 'the cloud' because, historically, networks would often be depicted as the outline of a cloud in diagrams representing transport of data from one endpoint to another.[6] However, 'cloud computing' does not mean 'internet computing' as one might infer from this metaphor. The term refers to a family of computing architectures that offer utility programming, where resources are provided as a metered service, similar to the way a public utility company supplies gas and electricity.[7] As defined by the National Institute of Standards and Technology (NIST), 'Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.' The NIST definition of cloud computing lists five essential characteristics:

1. **On-demand self-service**. Customers can utilize or release more or less computing resources as needed, and automatically, without the need for human intervention at the cloud provider.
2. **Broad network access**. Services are provided over the network in formats that promote access by a wide variety of desktop and mobile client devices.
3. **Resource pooling**. The cloud provider pools its computing resources, dynamically allocating and releasing resources like storage, processing, memory, network bandwidth, and virtual machines, to multiple consumers.
4. **Rapid elasticity**. The provider's resources can be elastically scaled out or quickly released to scale in, depending on customer demand, giving the customer the appearance that resources are unlimited.
5. **Measured service**. The provider monitors and reports consumer usage of services.

Currently, the three most common cloud computing service models are Software-As-A-Service (SAAS), Platform-As-A-Service (PAAS), and Infrastructure-As-A-Service (IAAS).[8] The SAAS model offers software, PAAS offers a development environment, and IAAS offers processing power and disk space, all rented on a pay-per-use charge plan. Cloud providers can offer combinations of these services, so a PAAS provider might offer a software development environment, and then rent server space to host the applications and store data. Services can be deployed as public clouds (multiple customers from the general public share a common infrastructure), private clouds (a single

Table 1 Implementation of desirable EHR qualities with the cloud computing model

Quality	Description	How cloud computing could implement the quality
Economical	System's price should fall within a range that would permit its inclusion in the budget of most practices that could benefit from it	Cloud computing can be less costly than buying traditional in-house EHR systems through more efficient use of computing resources like networks, servers, storage, applications, and services, which are shared among clients, and can be rapidly provisioned and released
Interoperable	System should allow electronic exchange of data with other EHR systems without the need for expensive custom data conversion libraries or third party EDI clearinghouses	An EHR system offered by a SAAS or PAAS provider could feature membership in the NHIN, and implementation of the CONNECT[5] networking functionality, including a variety of data exchange mechanisms with other NHIN members
Useful, agile	System should facilitate and be responsive to changes in business requirements and workflow	The PAAS model could supply a basic, generic EHR system to clients, while offering the tools to quickly customize it as needed to accommodate local requirements
Secure, compliant	System implements effective mechanisms to protect data integrity and confidentiality at the host, network, and application levels, and complies with government regulations	An EHR system offered by a SAAS or PAAS provider would have to implement all HIPAA requirements, and specify them in business associate contract with clients (table 2)

EDI, electronic data interchange; EHR, electronic health record; HIPAA, 1996 Health Insurance Portability and Accountability Act; IAAS, Infrastructure-As-A-Service; NHIN, National Health Information Network; PAAS, Platform-As-A-Service; SAAS, Software-As-A-Service.

organization uses the cloud services), community clouds (infrastructure is shared by several organizations with a common mission), or hybrid clouds (several clouds bound together by some technology that allows data and application sharing).[9]

Cloud computing is gaining acceptance as a model for business information technology (IT) applications because of its potential to increase capacity and functionality on the fly without major investment in infrastructure, personnel, or software licensing fees.[10] The NIST believes that government and industry should work to overcome the barriers[11] and migrate to cloud computing because it offers the potential for massive cost savings and increased IT agility.[12]

Cloud computing service models could be used for entire EHR systems, or to support some of their components. EHR software applications and data storage are already starting to appear through cloud providers that advertise SAAS.[13–17] Clients can access their systems in a variety of formats, including desktop client executables, browsers, and smartphones. These companies advertise their SAAS systems as economical because a capital expenditure is converted to operational expense, they have device and location independence, and they automatically increase capacity with demand.[17 18] Such SAAS systems are being marketed to small practices that seek rapid EHR adoption to become eligible for federal 'meaningful use' incentives.[19] Potentially, EHRs built with the PAAS model, using programming and database tools from vendors like Microsoft, could be offered to practices large enough to have IT support, who are interested in rapidly customizing their EHR.[20] Such systems would not only offer the pre-fabricated EHR software offered by SAAS providers, but would also supply the customer's software developers with the tools needed to build on the basic functionality. This additional flexibility over immutable SAAS software would address clinician's concerns that EHR applications would be more useful if they were agile and adaptable to local business workflow. The PAAS provider's framework would facilitate EHR application development by supplying standard features like user account management, encryption, database backup, terminology picklists, and National Health Information Network (NHIN) messaging.

Rather than implementing entire EHRs, cloud providers could support components of complex EHR systems that the owners wish to outsource. An obvious example would be medical database storage or backup by an IAAS provider. Cloud providers could offer data aggregation and software services to support personal health record (PHR) repositories. Health information exchange services, data processing for connectivity with the NHIN, and offsite master patient indexing could also be supplied on demand by specialized cloud providers. Outsourcing to cloud providers could be used to make EHRs more useful, agile, economical, and interoperable. However, in order to implement the features of being secure and compliant, they must adhere to government regulations and industry standards.

FEDERAL SECURITY AND PRIVACY REGULATION

The federal legislation which calls for regulations to safeguard the privacy and security of electronic protected health information (ePHI) is part of the 1996 Health Insurance Portability and Accountability Act (HIPAA).[21] The rationale behind the HIPAA legislation includes (1) enhancing patients rights by providing them with access to their medical records; (2) protecting their rights by controlling access to their records; (3) improving the efficiency and effectiveness of healthcare delivery and data exchange; and (4) reducing healthcare costs.[22] The security regulations concerned with electronic medical information were published by the Department of Health and Human Services as The Security Rule in 2003.[23] The regulations require appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of stored or in-transit ePHI, and to protect it against any reasonably anticipated threats or hazards.[24] Failure to comply with federal HIPAA regulations carries severe sanctions, including fines of up to $1.5 million and up to 10 years in prison. The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, is also relevant because it has several provisions that strengthen the civil and criminal enforcement of the HIPAA rules, mainly by defining levels of culpability and corresponding penalties.[25] The penalties are intended to have ePHI owners take privacy and security seriously.

The Security Rule contains 42 implementation specifications (table 2) that are sufficiently broad and complex to elicit the publication of multiple articles and books that attempt to explain and simplify them.[21 22] They include guidelines that relate to security administration (conducting risk analyses and implementing policies and procedures to address vulnerabilities; assigning responsibility; screening and educating the workforce; limiting access to PHI; developing incident response plans), physical safeguards (protecting and limiting access to servers, storage media, and workstations), and technical safeguards (user identity management; encryption; activity audits; data integrity verification; transmission security).

Movement of EHR applications and data outside the healthcare establishment's corporate perimeter involves implementation of many of the HIPAA-required security processes and technologies by the cloud provider. The actual implementation

Table 2 Cloud provider business associate contract stipulations needed to ensure compliance with the HIPAA Security Rule

HIPAA Security Rule specification	Cloud provider business associate contract stipulation
1. Conduct risk analysis	Cloud provider agrees to produce periodic server-side risk analyses for use by the client
2. Implement risk management policies to reduce vulnerabilities	Cloud provider agrees to implement the server-side risk management policies required by the risk analysis
3. Apply sanctions to non-compliant workforce members	Cloud provider agrees to subject its workforce to sanctions for compliance violations
4. Implement policies to periodically review information system activities	Cloud provider agrees to give client a simple means to review its information system activities
5. Assign a security official	Cloud provider identifies a security official responsible for overseeing ePHI security
6. Supervise workforce members who work with ePHI	Cloud provider agrees to be responsible for supervising its workforce for security policy compliance
7. Clear workforce members for access to ePHI	Cloud provider agrees to perform a security clearance before workforce members have access to ePHI
8. Terminate workforce members' access to ePHI appropriately	Cloud provider agrees to implement policy to terminate its workforce members' access to ePHI appropriately
9. Isolate healthcare clearinghouse functions from the larger organization	Cloud provider agrees to ensure client's ePHI is isolated from its larger organization, and from ePHI of other clients (multitenancy of applications and databases may not be an option)
10. Implement policies for granting user access to ePHI	Cloud provider agrees to implement policies for granting workforce access to ePHI
11. Implement policies for review and modification of user access to ePHI	Cloud provider agrees to implement policies for reviewing and modifying its workforce's access to ePHI
12. Periodically remind users of security policies	Cloud provider agrees to implement mechanisms to remind users of security policies
13. Protect system from malicious software	Cloud provider agrees to keep antivirus software, operating system, and software patches up to date. Cloud provider operates intrusion detection system and firewall
14. Monitor login attempts	Cloud provider agrees to monitors login attempts, makes information available to client, and locks out users who exceed failed login attempt limit
15. Manage passwords	Cloud provider's software platform gives client administrator functionality to manage passwords
16. Identify and respond to security incidents	Cloud provider utilizes tools like an intrusion detection system to prevent attacks, and reports incident details, impact, and response to client
17. Backup data	Cloud provider agrees to back up data with tape, internet, redundant drives, or any means necessary to allow full recovery from incidents
18. Establish data recovery plan	Cloud provider develops, tests, and publishes a detailed procedure for emergency operations
19. Establish emergency operation mode plan	Cloud provider develops, tests, and publishes its plan for emergency operation, including backup power supplies and offsite failover facilities
20. Periodically test and revise contingency plans	Cloud provider agrees to periodically test and revise contingency plans for smooth transition to emergency operation mode
21. Assess relative criticality of applications and data	Client reports relative criticality of applications to cloud provider so emergency operations can be designed to provide at least the most important applications
22. Perform periodic security evaluation	Cloud provider agrees to perform periodic security evaluation and report any changes to client
23. Obtain assurances from business associates that security requirements will be met	Cloud provider agrees to all HIPAA-required SLA stipulations, as do any of the provider's business partners who handle ePHI
24. Establish procedure for facility access in emergency mode operation	Cloud provider develops, publishes, and tests procedure for facility access in emergency operation mode
25. Protect data facility and equipment from unauthorized access, tampering, and theft	Cloud provider agrees to implement sufficient physical safeguards to prevent unauthorized persons from entering data facility
26. Control and validate person's access to data facilities and software programs	Cloud provider agrees to screen, authorize, validate, and log all personnel accessing data facilities and their activities while there
27. Document repairs and modifications to data facility's physical components	Cloud provider agrees to document and report data facility repairs and modifications
28. Control use and location of workstations that can access ePHI	Cloud provider has software that allows client administrator to limit access to ePHI by certain devices identified by MAC or client certificate
29. Implement physical safeguards and control access to workstations that can access ePHI	(Client controls access to workstations)
30. Properly dispose of electronic media that stored ePHI	Cloud provider implements policies to properly dispose of electronic media
31. Properly remove ePHI from electronic media before re-use	Cloud provider agrees to implement policies to properly remove ePHI from electronic media
32. Maintain record of hardware and electronic media that store ePHI	Cloud provider agrees to maintain record of hardware and electronic media that store ePHI
33. Backup ePHI before moving equipment	Cloud provider agrees to back up ePHI before moving equipment
34. Assign unique name or number to users	Cloud provider's software platform ensures users are uniquely identifiable
35. Establish procedure for obtaining ePHI during an emergency	Cloud provider agrees to develop, test, and publish procedures for accessing ePHI during an emergency
36. Automatically log-off users after a period of inactivity	Cloud provider's software platform automatically logs users off after inactivity
37. Encrypt ePHI when appropriate	Cloud provider agrees to encrypt stored ePHI whenever necessary
38. Record and audit ePHI system usage	Cloud provider's software platform logs user access to ePHI and makes it available to client's administrators
39. Implement mechanisms to ensure that stored ePHI has not be been altered or destroyed in an unauthorized manner	Cloud provider implements policies to protect ePHI from alteration or destruction with encryption, PKI
40. Authenticate persons or entities seeking access to ePHI	Cloud provider's software platform authenticates users before granting access to ePHI
41. Implement measures to ensure transmitted ePHI is not modified in transit	Cloud provider's software platform implements data integrity controls such as digital signatures, MD5 one-way encrypted file hashes
42. Encrypt transmitted ePHI when appropriate	Cloud provider's software platform ensures transmitted ePHI is encrypted with strong passphrases, 128-bit or higher encryption algorithm, PKI or SSL/TLS

ePHI, electronic protected health information; HIPAA, 1996 Health Insurance Portability and Accountability Act; MAC, media access control address; PKI, public key infrastructure; SLA, service level agreement; SSL, secure sockets layer; TLS, transport layer security.

of many of the security measures remains essentially the same, regardless of who applies them, although there are some issues that are specific to the cloud architecture.

Security measures common to traditional and cloud architectures

Most of the HIPAA-specified controls listed above can be directly transferred from a traditional in-house system to an outside provider of simple EHR hosting or of cloud architecture services (table 2). The provider must conduct risk analyses, implement policies and procedures to address vulnerabilities, assign responsibility to a security officer, screen and educate its workforce, limit workforce access to PHI, develop incident response plans, protect and limit access to servers, storage media, and workstations, manage user identity, encrypt data both at rest and in transit, monitor and audit system activity, and verify data integrity. The provider can accomplish this with standard security controls like physical plant security, firewalls, intrusion detection/prevention systems, anti-virus software, patch maintenance, encryption, activity monitoring, identity and access management, and with governance-risk management-compliance policies and processes.[26]

Security concerns specific to cloud architectures

If the third-party provider offers cloud services, rather than simple EHR hosting, then there are specific privacy and security issues that must be addressed in addition to those listed above.[27–29] Many of the cloud-specific issues relate to multitenancy, which refers to cloud architectural designs that allow multiple customers to share infrastructure, services, and applications in order to enable the economies of scale and operational efficiency. Degrees of isolation can range from the entire data center, to the physical server, to a virtual server, to an application, a database, a database table, or to data elements (ordered from most to least isolated). Generally, the higher the degree of isolation between different customers' assets that a cloud architecture offers, the higher the cost.[30] In the case of EHR, a high degree of isolation should be used to ensure that ePHI is not commingled with that of other patients or cloud clients, since commingling complicates data security, data destruction, encryption, and geo-location restrictions. Some of the security concerns relating to multitenancy for cloud-based EHRs could be ameliorated by exploiting the 'community clouds' design, so computing resources are only utilized by EHR systems. The cloud provider could then apply HIPAA-compliant data management and disposal techniques to all the clients in its EHR cloud community.

Approaches to the problems arising from multitenancy and other cloud-specific problems like encryption key management are detailed in the Cloud Security Alliance's Guidance.[9] Much of the CSA's Guidance focuses on ensuring that the client understands the cloud provider's security controls, confirming that they are transparent, consistent with and supportive of the cloud client's own security framework, and defining contractual responsibilities and liabilities with a detailed business associate contract.

Business associate contract

Contracts between EHR data owners and cloud providers should stipulate compliance requirements, service levels, and legal liability.[31] Federal law requires that third parties handling PHI enter into a 'Business Associate Contract' with the client, stipulating that they will adhere to Privacy Rule guidelines.[32 33] As such the contract must specify that the cloud provider will not use or disclose PHI other than permitted or required by the contract or by law, use appropriate safeguards, report illegal use or disclosure of PHI, document its internal practices, books, and records relating to the use PHI, agree to turn this documentation over to the HHS Secretary if requested, and return or destroy all PHI upon termination of the contract.

The contract should also detail service levels, including which security controls of the entire EHR system are the responsibility of the client versus the provider, what security metrics the provider must meet, and how performance will be audited. The contracts should include constraints on how the provider's business associates will handle the client's data, procedures for electronic discovery and other litigation activities, and limitations on the geographic locations where data and backups can be stored.[34] The provider should detail its incident detection and response plan, and a formal arrangement for return or disposal of the client's data and other assets upon termination of the business relationship with the provider.

The contract with the cloud provider should also establish legal liability for breaches. Since liability assignment can be contentious and the negotiations complicated, the HITECH Act of 2009 clarified the responsibility for issues relating to misuse of PHI by business associates. Federal law privacy and security provisions that previously applied only to covered entities have been also assigned to business associates. Business associates now have both contractual and HIPAA liability, and are subject to mandatory periodic audits by the Office of Civil Rights.[35] Civil and criminal liability now extends to business associates for violations of HIPAA and HITECH security provisions. The CSA recommends that cloud clients negotiate penalties payable by providers in the case of a breach

The federal incentives in the HITECH Act constitute a strong temptation for healthcare groups to enroll in online EHR applications that offer rapid, low-cost startups like those offered by cloud providers. Lists of their security features and claims of HIPAA compliance by online EHR providers are comforting, but do nothing to alleviate practitioners from liability for damages resulting from compromised patient privacy. A worst case scenario for the healthcare provider could result by clicking through a series of friendly EHR sign-up screens and unwitting agreeing to release the provider from all financial responsibility for a security breach. Far better for the EHR client to have legal counsel negotiate a detailed, meaningful business associate contract with the cloud provider as described by the CSA before any ePHI is sent.

THE OTHER SIDE OF CLOUDS

Beyond security there are other issues that must be examined before migrating to the cloud platform. An economic analysis should be conducted to ensure net savings are not overestimated, especially after considering potential hidden costs.[30] Some of these could include legal fees for writing contracts and defending disputes with the cloud provider, salaries of security staff to monitor the provider's performance and compliance, costs of in-house IT support for custom-built PAAS applications, and the expense of data migration at the beginning and end of the contract's lifetime. There are also concerns about the maturity of the service model itself, and whether it is compatible with the high standards that must be maintained in a complex and sophisticated IT environment like that found in healthcare.[36 37]

CONCLUSIONS

Traditional in-house EHR applications are hampered by many unsatisfactory features that could be improved by re-designing them with modern computing architectures. EHR hosting by cloud computing providers could potentially promote acquisition and modification of sophisticated EHR applications through improved efficiency and pricing plans. Implementation of the privacy and security standards that are currently under development within the cloud community, including business associate contracts that specify auditable, enforceable performance metrics and sharing of liabilities, should allow such a system to achieve compliance with federal privacy and security regulations. By enabling easy adoption of feature-rich EHR systems, modern IT architectures can facilitate the federal government's expressed goals of enhancing patients' access to their medical records, improving data exchange, and reducing healthcare costs.

Competing interests Yes, I will upload an HREF http://www.icmje.org/coi_disclosure.pdf - ICMJE conflicts of interest form for each author of this manuscript.

Provenance and peer review Not commissioned; externally peer reviewed.

REFERENCES

1. **DesRoches CM,** Campbell EG, Rao SR, *et al*. Electronic health records in ambulatory care — a national survey of physicians. *N Engl J Med* 2008;**359**:50—60.
2. **Jha AK,** DesRoches CM, Campbell EG, *et al*. Use of electronic health records in U.S. hospitals. *N Engl J Med* 2009;**360**:1628—38.
3. **Fox A.** Cloud computing — What's in it for me as a scientist? *Science* 2011;**331**:406—7.
4. **Doukas C,** Pliakas T, Maglogiannis I. Mobile healthcare information management utilizing cloud computing and android OS. *Conf Proc IEEE Eng Med Biol Soc* 2010;**2010**:1037—40.
5. CONNECT Community Portal. Available from: http://www.connectopensource.org/ (accessed 31 Jan 2011).
6. **Rittinghouse JW,** Ransome JF. *Cloud Computing: Implementation, Management, and Security*. Boca Raton: CRC Press, 2010.
7. **Katzan H Jr.** On an ontological view of cloud computing. *Communications of the Association for Computing Machinery* 2010;**3**:1.
8. **Mather T,** Kumaraswamy S, Latif S. Cloud security and privacy. Beijing, Cambridge [Mass.]: O'Reilly, 2009.
9. **Brunette G,** Mogull R. Security guidance for critical areas of focus in cloud computing v2.1. http://www.cloudsecurityalliance.org (accessed 10 Dec 2010).
10. **Smith R.** Computing in the cloud. *Res Technol Manage* 2009;**52**:65.
11. **Armbrust M,** Fox A, Griffith R, *et al*. A view of cloud computing. *Association for Computing Machinery Communications of the ACM* 2010;**53**:50.
12. *Cloud Computing*. http://www.nist.gov/itl/cloud/index.cfm (accessed 14 Dec 2010).
13. *Practice Fusion*. http://www.practicefusion.com (accessed 26 Nov 2010).
14. *Centricity Advance*. http://www.gehealthcare.com/centricityadvance/index.html (accessed 26 Nov 2010).
15. *MedScribbler*. http://www.medscribbler.com/Internet-Based (accessed 26 Nov 2010).
16. *EMR in the Cloud*. http://www.emritc.com/about.html (accessed 26 Nov 2010).
17. *Sevocity*. http://www.sevocity.com/index.php/blog/technical-qstuffq-made-easy/140-cloud-computing-and-ehremr&template=sevocity_blog (accessed 26 Nov 2010).
18. *Centricity Advance 24/7 Secure Data Center*. http://www.gehealthcare.com/centricityadvance/features-data-center.html (accessed 26 Nov 2010).
19. *EHR Incentive Program*. http://www.cms.gov/ehrincentiveprograms (accessed 2 Feb 2011).
20. **Moore J.** *HIEs, Future PaaS for Healthcare?* http://chilmarkresearch.com/2009/11/02/hies-future-paas-for-healthcare (accessed 31 Jan 2011).
21. **Wu SS,** ed. *Guide to HIPAA Security and the Law*. Chicago: ABA Section of Science & Technology Law, 2007.
22. **Beaver K,** Herold R. *The Practical Guide to HIPAA Privacy and Security Compliance*. Boca Raton: Auerbach Publications, 2004.
23. *Health Insurance Reform: Security Standards; Final Rule. Fed Reg 8334: Health Insurance Reform: Security Standards; Final Rule*. 2003.
24. *Health Information Privacy*. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule (accessed 2 Nov 2010).
25. *Health Information Technology for Economic and Clinical Health (HITECH) Act. Fed Reg 160: Health Insurance Reform: Security Standards; Final Rule*. 2009.
26. **Rai S,** Chukwuma P. Security in a cloud. *Internal Auditor Magazine* 2009;**66**:21.
27. **Katzan H Jr.** On the privacy of cloud computing. *Int J Manag Inform Syst* 2010;**14**:1.
28. **Barnes FJ.** Putting a lock on cloud-based information. *J Inform Manag* 2010;**44**:26.
29. **DeFelice A,** Leon JC. Cloud computing: what accountants need to know. *J Accountancy* 2010;**210**:50.
30. **Rhoton J.** *Cloud Computing Explained*. [City not specified]. Recursive Press, 2010.
31. **Ryan W,** Loeffler C. Insights into cloud computing. *Intellect Property Tech Law J* 2010;**22**:22.
32. **Health Information Policy.** *Business Associate Contracts*. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (accessed 16 Apr 2011).
33. **Health Information Policy.** *Business Associates*. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (accessed 16 Apr 2011).
34. **Gatewood BC.** Clouds on the information horizon: How to avoid the storm. *J Inform Manag* 2009;**43**:32.
35. *HITECH Act Updates to the Business Associate Agreements*. www.ihs.gov/ihimc/documents/4IHITECHActUpdateBusAssocAgrmts.pdf (accessed 19 Apr 2011).
36. **Lewis B.** *ITIL vs The Cloud: Pick One*. http://www.weblog.keepthejointrunning.com/?p=3927 (accessed 21 Feb 2011).
37. **Lewis B.** *ITIL vs The Cloud: Pick Both — Just Not at the Same Time*. http://www.weblog.keepthejointrunning.com/?p=3936 (accessed 21 Feb 2011).