Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

May 2012 - Issue 22

What's Inside?

Cloud Computing Study Reveals Data Security Flaws
Big Data, IT Risks and Privacy Meet in the Boardroom
Privacy & Security News

Cloud Computing Study Reveals Data Security Flaws

The adoption of cloud computing appears to be accelerating, especially with enterprise customers. The widespread availability of high speed internet access has resulted in the Internet no longer functioning solely as a communications network. It has become a platform for computing; the so-called "cloud". Rather than running software on your own computer or server, internet users reach to the "cloud" to combine software applications, data storage, and massive computing power. Not only can businesses save capital expenditure on in-house IT equipment, they can also benefit from the extra agility and flexibility that cloud services can deliver. However, many remain uncomfortable with the security and privacy ramifications of data in the cloud.

A British security company which conducted a research study involving four cloud service providers (CSPs), has revealed serious cloud computing data security problems. Context Information Security initially brought the issues to light a year ago when it tested the security of four CSPs. In March 2011, Context produced a white paper detailing the tests it carried out against Amazon EC2, Gigenet, Rackspace and VPS.net. Context outlined a range of security failings, including the virtual machines (VM) provided by all four CSPs lacked up-to-date security patches and antivirus protection. In addition, some CSPs had backdoors to allow their own administrators to access the VMs. But the most serious flaw, detected at the time in Rackspace and VPS.Net, was that data left by one customer was not deleted automatically and could conceivably show up on the VM belonging to the next customer.

The concept of transferring control of sensitive data to another company worries many people. Is data held somewhere in the cloud as secure as Data protected in user-controlled computers and networks? Privacy and security can only be as good as its weakest link. One of the issues with cloud computing is that technology is frequently light years ahead of the law.

Most importantly from a privacy standpoint, how does the cloud provider protect the user's data?
The research reveals a lack of maturity in the cloud service market; it emphasizes the need to perform due diligence including legal/regulatory review, before contracting with any cloud provider.

Frequently Asked Question

Q: Can I use Dropbox to store or transfer University of Miami sensitive information?

A: No, consumer based cloud storage vendors should not be used to store or transfer UM sensitive information. Information technology is currently evaluating various vendors for these services. Further information will follow.

Have a Question?

hipaaprivacy@med.miami.edu

Prior newsletters available online
http://www.med.miami.edu/hipaa

Big Data, IT Risks and Privacy Meet in the Boardroom

In three separate articles, Financial Times reports on large-scale privacy and security issues faced by organizations around the world. The rise of big data "poses a challenge for businesses" on "how to manage the ever-increasing and increasingly disparate data that we generate every day and how we use it." Utilizing consumer data is "business critical," but data management poses security risks. Several recent data breaches "underscore a key principle for boards: IT risks are business risks. Poorly managed, they can and will exceed corporate risk tolerances," the report states. In light of these recent breaches, chief financial officers "should be kept awake worrying about accountability at the business level." One report adds, "The key to data security is not what your IT department does, it is the policies you set in the boardroom."(Registration may be required to access this story.)

Office of HIPAA Privacy & Security
Professional Arts Center (PAC), Suite 409 (M-879)
http://www.med.miami.edu/hipaa
Phone: 305-243-5000
Fax: 305-243-7487

Insurer Pays $1.5 million fine Under HITECH

A Tennessee insurer will pay a $1.5 million settlement to the U.S. Department of Health and Human Services (HHS) for HIPAA violations related to its 2009 data breach. BlueCross BlueShield of Tennessee has already paid $17 million in costs related to the breach, and now must regularly train employees on HIPAA requirements and review and revise its privacy policies. The settlement is the first enforcement action taken under the HITECH Act and an HHS Office for Civil Rights (OCR) spokesman said it "sends an important message that OCR expects health plans and healthcare providers to have in place a carefully designed, delivered and monitored HIPAA compliance program."

Minnesota AG Brings HIPAA Enforcement Action Against Business Associate

On January19, 2012, following the theft of an unencrypted laptop computer containing approximately 23,500 patient records, the Minnesota attorney general brought the first formal enforcement action against a business associate, Accretive Health, Inc., for an alleged HIPAA violation, using her authority under the HITECH Act. Additionally, the attorney general appears deeply unsettled by the amount of information that Accretive Health collected about patients without the patients' knowledge, alleging that "this lack of transparency represents deceptive and fraudulent practices under Minnesota law". The Minnesota suit against Accretive Health is a reminder that the HITECH Act's statutory provisions are in effect and that state attorneys general (as well as the U.S. Department of Justice) are not bound by HHS' enforcement discretion when considering the exercise of their authority to enforce HIPAA.

Gartner: Corporate Privacy Policy Requirements Demand Urgent Review

Changes in technology and legislation are exposing weaknesses in the way organizations manage sensitive personal data, and as a result, many of them are now carrying out urgent reviews of their privacy policies. According to research group Gartner, 50% of all enterprises will revise their corporate privacy policy requirements before the end of 2012 in order to reflect changes in business practices, such as the use of cloud computing and location-based services available on smartphones. Gartner's forecast is based on interviews with its clients. Carsten Casper, privacy research director for Gartner, said changes to laws on privacy and mandatory breach disclosure are also forcing companies around the globe to review their security policies. He said it used to be enough for companies to tell customers their information was protected, but now the general public is much more aware of data breaches and the importance of privacy, and in turn require greater reassurance and information about how their data is managed.

IT Security's Scariest Acronym: BYOD, Bring Your Own Device

The torrent of smartphones and tablets entering companies has created challenges for information security. The new devices introduce new operating systems, new development environments and new security risks, but with no new controls. The scariest acronym in security might well be "BYOD," or "bring your own device." Some organizations believe that BYOD will allow them to avoid significant hardware, software and IT support costs. Even if cost-savings is not the goal, processing of company data on employee personal devices may be inevitable and unavoidable. Unfortunately, BYOD raises significant data security and privacy concerns, which can lead to potential legal and liability risk. Many companies are yet to adequately address these risks. To the extent a company's employees are unable or unwilling to implement particular security controls, the organization may be increasing its security risk. To reduce legal and liability risk, companies implementing a BYOD strategy need to carefully analyze their existing security and privacy policies, as well as implement new controls.

Related Links

- **Cloud Computing:** http://www.med.miami.edu/hipaa/public/documents/context.pdf
- **Big Data:** http://www.ft.com/intl/cms/s/0/ea1557de-7436-11e1-9e4d-00144feab49a.html#axzz1tvZSfgWV
- **Insurer Pays:** http://www.computerworld.com/s/article/9225170/Tennessee_insurer_to_pay_1.5_million_for_breach_related_violations
- **Minnesota:** http://www.dwt.com/Business-Associates-Beware-First-HIPAA-Enforcement-Action-Against-a-Business-Associate-And-the-Plot-Thickens-with-Transparency-Demands-02-06-2012/
- **Gartner:** http://searchsecurity.techtarget.co.uk/news/2240039467/Gartner-Corporate-privacy-policy-requirements-demand-urgent-review
- **IT Security:** http://www.cio.com/article/703185/The_BYOD_Troubleshoot_Security_and_Cost_Savings

Office of HIPAA Privacy & Security
Professional Arts Center (PAC), Suite 409 (M-879)
http://www.med.miami.edu/hipaa
Phone: 305-243-5000
Fax: 305-243-7487