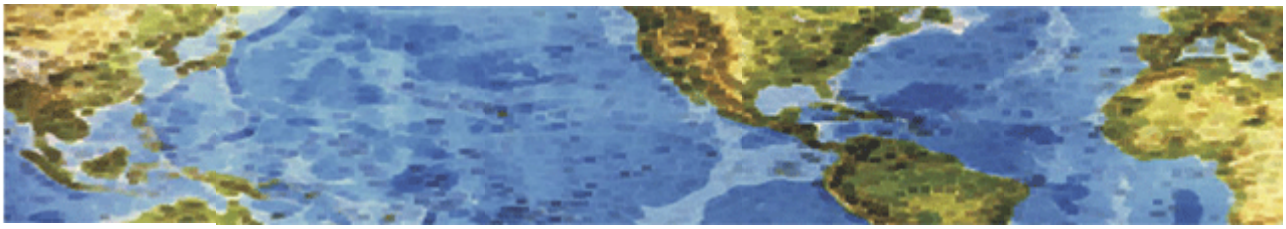
HALL ASSOCIATES



Risk-Based Decision Making Commentary
22 April 2013 Newsletter

HIPPA Requirements for Business Associates

If your company handles one or more "personal health records" it would be **VERY** prudent for you to fully comprehend the severity of the legal impact. The following is a very brief example of some of the concerns. The penalties for mishandling even one record can be very costly.

The new HIPAA expanded "business associate" definition to include health information organizations, e-prescribing gateways **or others** that provide data transmission services for protected health information (PHI) to a covered entity and that require routine access to the health information. Companies that offer a personal health record to one or more individuals on behalf of a covered entity **are also now** considered business associates.

In the past month, eight out of 15 breaches added to the Department of Health and Human Services' "wall of shame" tally have involved business associates. And business associates have been implicated in about 21 percent of the 571 breaches affecting 500 or more individuals that HHS has tracked since September 2009. Business associates have been involved in many of the largest incidents, including, for example:

- A September 2011 breach affecting 4.9 million individuals involving SAIC, a business associate of TRICARE, the military health program;
- A December 2010 incident affecting 1.7 million patients involving New York City Health and Hospitals Corp. and it's business associate, GRM Information Management;
- A March 2012 breach that compromised data of 780,000 individuals and involved the Utah Department of Health and its business associate, the Utah Department of Technology.

With the enforcement date of Sept. 23 for HIPAA Omnibus less than five months away, it's possible that even more business associate-related breaches will appear on the tally. That's because under HIPAA Omnibus, not only are business associates and **their subcontractors** for the first time **directly liable** for HIPAA compliance, but also the definition of business associates has been expanded to include more kinds of vendors, including many cloud service providers.
http://www.healthcareinfosecurity.com/breaches-business-associates-role-a-5709

Have you evaluated what data you have and whether or not it is "protected"? There are now numerous types of "protected" data with onerous legal liabilities if compromised.

HALL ASSOCIATES

Android Malware

The amount of malware (malicious software) aimed at infecting Android devices (mostly mobile phones and tablets) more than doubled in 2012. The number of pieces of malware targeted against an Android platform rose from less than 25,000 in 2011 to **over 65,000 in 2012**. A report published by a mobile security company, estimates that nearly **33 million** devices were infected in 2012 – an increase of over 200% from 2011.

The most popular way of infecting Android devices is through application repackaging – taking popular applications from the Google Play Store, adding malicious code and than uploading the corrupted application to an "unofficial" application market site. Such infections occur when Android users download cut-rate applications from "unofficial" sites to avoid paying the full price at the Google Store. Such malware can provide cybercriminals access to any data stored on your mobile device, including account information and passwords. (***You do encrypt your data on all your mobile devices, don't you?***).

Cybercriminals can also steal Android user's personal (and business) data through malicious websites. Subtle changes in URLs redirect users to criminal clones of the sites you think you are accessing. Once there, you are prompted to provide personal or account information. Based on some research, people are less likely to be suspicious or security-minded on mobile devices than they are on their PCs.

Smishing (a combination of SMS and phishing) involves sending an unsolicited text message (SMS) to a target and getting them to click on a link in the message. This in turn downloads and installs the malware application. Some of this malware accesses premium text message services in the background, sends messages and causes your phone bill to skyrocket.

You can avoid becoming malware victims by being **very careful** about clicking on links and installing applications. Access the internet on your Android device with the same level of concern for security that you do on your Windows PC. Don't click on any links or open attachments in e-mail messages without scanning for viruses and malware and if you do not recognize who sent them. Make sure you are really on the web page you seek before filling out any personal information or passwords. Small screens make it harder to see the full URL, but taking a moment to check could be **extremely** useful. Download applications only from Google Play store. Google does try to keep malicious code from apps there. Finally, install one of the available Android anti-virus applications, keep it updated and use it.

http://www.technewsdaily.com/17817-android-malware-doubles.html