Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

Assessments of Security and Privacy Risks of Google Health Portal

by

Verma, Vivek

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: May 2009

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, Associate Professor, MISSM

Assessments of Security and Privacy Risks of Google Health Portal

by

VERMA, Vivek

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, Associate Professor, MISSM

Reviews Committee:

Andy Igonor, Assistant Professor, MISSM
Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

Assessments of Security and Privacy Risks of Google Health Portal

Vivek Verma
Dale Lindskog (Primary research advisor)
Pavol Zavarsky (research advisor)
Ron Ruhl (reserch advisor)

Information Systems Security Management
Concordia University College of Alberta
7128 Ada Boulevard, Edmonton, Alberta, Canada T5B 4E4
http://infosec.concordia.ab.ca

Abstract

The use of Google Health patient portal raises security and privacy concerns for the users. Since the portal stores sensitive personal and health information, it raises questions on security and privacy risks. The objective of this research is to identify those security and privacy risks of the Google Health portal which could affect the user. This paper analyzes how the risks identified affect the security and privacy of users' personal health information. It will be argued that Google Health does have certain inherent security and privacy risks. In particular risks related to: third party access to health records, HIPAA non compliance, advertising by third-party service providers, single sign-on, access control, health record linkage and data storage. Based on the risks identified, this paper recommends the measures to overcome the privacy and security risks identified.

1. Introduction

The intention of this research paper is to assess the security and privacy risks associated with the use of Google Health portal. Google Health users store their personal and health information within the portal. I will identify and describe various security and privacy risks of Google Health and would also suggest practical measures for Google to implement so as to mitigate the risks identified. The rest of the paper is structured as follows. The next section provides a brief overview of how Google Health functions. In Section 3, privacy and security risks of Google Health are identified and discussed. The risks identified are based both on material available on risks to patient managed portals, along with some of my own proposed solutions to those risks and suggestions to improve the privacy and security practices of Google Health. Finally, section 4 presents the conclusion for this paper and points out directions for future work.

2. Overview of Google Health

Patient portals are healthcare related online applications that allow patients to interact and communicate with their healthcare providers, such as physicians and hospitals [1]. There are two models of patient portals: patient managed and provider managed patient portals. In provider managed patient portals, provider grants Electronic medical record and/or Electronic health record access to the patient. Depending on the provider it could be view-only, or patients could be allowed to make limited contributions. In patient managed patient portals, patients maintain their own record and invite providers to participate. Google Health portal is a patient managed portal. The rest of this section is devoted to certain details about Google Health that are relevant to the risks identified in section 3.

Use of Google Health is only meant for the residents of United States [24]. To use Google Health, users have to register with Google Accounts, creating a single sign-on login account to use Google services, of which Google Health is a part. Google Health is a depository of health information in which users build their online health profile. Besides adding their personal information, users can add history of their personal health details like medical conditions, medications, test results, procedures and immunizations.

Users can share their profile with family members, friends, doctors or anyone in the users care network. Users enter email addresses of the individuals they want to share information with, and those individuals will be provided read-only access. Users can revoke the access at any time and will always be able to see who has access to their profile [34]. In addition, users can also use different personal health services provided by third party service providers, like importing medical records, exploring different medications and treatments with third party healthcare providers, converting paper records into e-records, using different personalized tools, and copy and sharing user health records with healthcare providers.

Third party service providers who can access user data after the user links their profiles with the third party; they have to subscribe to Google Health integration policies, which govern data use policy for the third party service providers [28]. When users link their health profile with third parties, the information is shared with the third party authorized by the user. Users cannot control what information they want to share, thus the complete health profile of the user is shared with the third parties. When users sync their Google Health profile with a third party service provider like a healthcare provider or pharmacy, users are informed about the kind of access the third party service will have. There are basically two types of access the third party service can have, i.e., write-only access and read/write access [3]. Access controls to the health information lie in the hands of the users. Users can revoke third party access to their health profile by revoking access anytime. Third parties will not have access to the user information once access is revoked [3]. In addition, there are no ads in Google Health, but it does allow third party service providers to provide for advertising once a user links his profile with third party service [28].

Google Health follows a cloud computing model for storing users' personal health information. Thus, users' information is stored in the United States and other countries [19]. Google Health is a depository of the users' health information, but it is not regulated by Health Insurance Portability and Accountability Act (HIPAA), a federal law that establishes data confidentiality standards for patient health information [16]. In addition, to protect confidentiality and integrity of user health information, Google Health uses SSL (Secure Socket layer) encryption and firewalls during information transmission and storage. Google Health also does regular backup of the system to ensure information availability of the user information [3].

With this background material on the working of Google Health and its privacy policies described above, I can now proceed to discussion of various security and privacy risks related to these workings.

3. Security and privacy risks of Google Health

By simply using Google Health, the user is exposed to different security and privacy risks. In addition, users share their Google Health profile with third party service providers, further exposes user information to risk. Google Health has some inherent security and privacy risks like sharing of users' personal health information

with third-party developers, third party access controls, issues concerning data storage outside of US, linking of users' health records with third party service providers, single sign on risk, Ad targeting by third party service providers, and HIPAA non-compliance.

3.1 Google Health Integration Policies

Users intending to use third party services link their health profiles with third party service providers. When users link their health profile with third party service providers, they provide these third parties with access to their personal health information. Thus, Google Health has created its "Google Health Integration Policy" for these third party service providers to follow [28]. The Google Health Integration Policy consists of guidelines on how third parties collect, use, share and handle users' personal health information. The Google Health Integration policy is applicable to all third party service providers which are listed in the Google Health directory.

Under this policy, there is one section entitled "Data Use Policy", which lays guidelines on how third parties should handle user data [28]. In the "Data Use Policy" section Google Health describes under what circumstances third parties can share Google Health user data with additional parties' without explicit consent from the user [28]. It states, "*You have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a)satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable terms of service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of your users or the public as required or permitted by law.*"

Based on this statement, third party service providers can share users' health data with additional third parties, like government agencies or any other investigating agency, without the user being aware of it. This raises privacy issues about the handling of users' personal health information by these additional parties. There is a risk of mishandling users' personal information. In addition, these additional parties are under no obligation to inform the user, so that user cannot take legal recourse to block access. Thus, there is a risk of mishandling of users personal information, which is a confidentiality risk.

To mitigate the risk, whenever these third parties with whom the user shares the personal information, themselves share information with additional parties, those third parties should notify the user. Thus, it would help the user in taking any legal measures if the user does not want the information to be disclosed. Since, the user information is being shared without opt-in consent of the user; it raises another issue of access controls, regarding sharing of user information.

3.2 Google Health access controls

According to the Google Health privacy policy [3], users control access to their health information. Users choose who can read or write information to their Google Health profile and can revoke access at any time, and the third party will not be able to read or write information to and from the users Google Health profile. When users sync their Google Health account with third party service providers, like a pharmacy or healthcare provider, they are informed about the kind of access that third party service provider will have, i.e., write-only access or read/write access [3].

Users cannot control whether a third party can or cannot retain the copy of users' personal health records. For example, suppose a user shares his

profile with a diagnostic service, which has read-only access. After a while user revokes access to the third party diagnostic service. But since the diagnostic service already had access to the user's personal health information, it may have retained a copy of that information before the user revoked access. In this way multiple copies of the user's personal health information can be generated when the user shares his health profile with a third party service provider. Thus, multiple copies can be generated even after access has been revoked. Despite the privacy and security controls of Google Health, records are thus duplicated in multiple locations, which is a privacy risk. The records leaked could be used for marketing purposes. The leaked information could also get into the hands of malicious people and can lead to identity theft.

Though risk cannot be mitigated completely, e.g., in case of a pharmacy which has read-only access to the user's health profile, and the pharmacy needs this read-only access to know the medication details. There is no point in hiding this information from the pharmacy. But in other cases it can be minimized by restricting the flow of users' personal health information. For example, if a third party service provider's job is to provide diagnostic reports to the user and to update the record of the user in its health profile, there is no logic in giving the diagnostic service read access rights.

3.3 Google Health profile linkages

Independent healthcare providers often maintain separate healthcare records about the patients. One set of records, say, is with an eye specialist, and another with a family doctor. Thus, there are two different set of records with each doctor. Thus, in all probability these two separate records will never be linked or shared unless in some extreme circumstances [29].

In Google Health users maintain centralized health records. When a user links his centralized health records with the third party healthcare service provider, he has to share his centralized health care record with the physician. Thus, an eye specialist will have the same record health record as the family doctor [29].[1]

Patients may not like to share their medical history about other health problems unrelated to his vision problems. For example, a patient is being treated for depression and would not like his eye specialist to know about it. There are other sensitive pieces of medical problems that a patient may not like to share [29]. For example, a patients company is paying for the treatment that a patient is receiving from a particular healthcare provider. But the patient would also like that certain sensitive information about his health condition should not reach his employer, since it could affect his position in company [29]. In addition, if certain sensitive pieces of information reach his insurance company it could affect his premiums. Also, if someone is being treated for some particular health condition that he hadn't shared with his family members, this could be later leaked out because the patient couldn't control what information he wanted to share.[2]

To mitigate the risk Google Health should provide a certain degree of control in such a way that a user could control access depending on time, people and information. Google Health should allow the user maneuverability in such a way that he should be able to share certain information and be able to hide other information which he does not want to share.

This also raises other related issue of compliance issues like what protections are available to the

[1] The seed for this idea came from reference [29], in the section 'PHRs and Linkage.'

[2] The idea for this came from reference [29], in the section 'PHRs and Linkage.'

users if their information gets leaked, which of turn to next.

3.4 Google Health and HIPAA

According to Administrative Simplification standards adopted by Health and Human Services (HHS), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) covers three basic groups (as defined in 45 C.F.R. Part 160; HIPAA Privacy Regulations): health plans, health care providers and healthcare clearing houses [35]. Google Health is not a covered entity under HIPAA because Google Health does not provide health care services [6]. By not subscribing to HIPAA, Google Health exposes users' health information to privacy risks which would otherwise have been taken care of under HIPAA since HIPAA provides statutory protections. Two such risks are addressed in the following two subsections.

3.4.1 Google Health and Business Associate agreement

Under HIPAA, a business associate is an individual who works on behalf of a covered entity (e.g. Google Health) which involves the use or disclosure of individually identifiable health information. Under HIPAA, the covered entity is required to have a written agreement with individuals/entities (third parties) such that personal health information is safeguarded appropriately (as defined in 45 C.F.R. Part 164.314(a)(1), (b)(1), ; Organizational Requirements) [36]. Thus, any covered entity under HIPAA cannot share PHI (Protected health information) without this agreement. The individual (business associate) cannot be a member of covered entity's workforce [30].

It is the responsibility of the covered entity to initiate the business associate agreement with the third party entity. Although the covered entity is not liable if the third party violates terms of agreement, if and when the violation of the agreement is discovered, the covered entity must terminate the agreement [30]. Thus it ensures the privacy of the users' personally identifiable health information.

With the help of Business Associate agreements, users' information handled by third parties comes under the preview of the covered entity. Thus, it becomes the responsibility of the Business Associate appointed by the covered entity to take care of third-party handling of users' personal information. Since Google Health is not a covered entity under HIPAA, there is no oversight available over the use of personal health information by third parties, and Google cannot be held responsible for any misuse.

3.4.2 Google Health and subpoenas

Health records of the users stored in Google Health can be subpoenaed. HIPAA provides protections to the users health records in case records are summoned under subpoenas (as defined in 45 C.F.R. Part 160.314; Investigational subpoenas and inquiries) [37]. HIPAA requires that person seeking the records should provide notice to the users in advance. Thus it gives the user a chance to contest the subpoena or take any other legal measure that the user wants to undertake.

Google Health is not required to provide advance notice to the user. Thus the records in Google Health do not have basic procedural protection which is otherwise provided by HIPAA for subpoenas. Notice for subpoena is not a legal requirement for non-HIPAA covered Google Health. Besides, Google Health is not likely to be spending money on behalf of consumers to protect their personal health information. Although Google Health states that whenever possible it will try to give user a notice [16], it is not legally binding. Thus, there

is a privacy risk to the users' personal health information.

This also raises other related issues of data stored outside of US, where HIPAA compliance may not work. The following section concerns data storage.

3.5 Google Health and data storage

Google Health stores users' personal health information in servers in the United States and other countries [19]. Google follows the cloud computing storage model to store the users' personal health information. Thus, users' information is stored in a distributed environment. This means some information in part or in whole may be stored in the servers outside of United States [19]. In case of data breach, the physical location of the server where the data is stored will affect the recourse that will be available to the users. E.g. a user in United States can face legal complications in case of data breach because the data is stored somewhere outside of United States, thus exposing users' personal health information to confidentiality risk.

Since a lot of sensitive personal health information is stored in the servers and use of Google Health is restricted to United States residents only [24], Google should try to keep the personal health information of the users in a data centre located in United States itself. It would provide users necessary statutory safeguards and will increase confidence among the users regarding their handling of personal health information by Google. Storing personal health information in US will make Google more accountable to the users.

3.6 Ad targeting by third party service providers

There are many ways information could get leaked, affecting the privacy of the users' health information. One of them is advertising by third party service providers. Google Health does not provide any ads on the user's profile. However, Google Health allows third party service providers [28] to provide ads or promotional targeting. By allowing third party advertising, users' personal health information faces privacy risk such that personal information gets leaked into marketing system [29]. For example, if a user clicks on an ad for an online pharmacy and shops for medicines related to his particular health condition, the advertiser would be able to get personal health information about the user. The advertiser may then use the information, disclose it to others, share it with commercial data brokers, or do anything it pleases because no privacy law typically applies and Google Health is not typically subject to any privacy policy [29]. Thus, third party ads are a confidentiality risk to the users' personal health information.[3]

Third party advertising could facilitate disclosure of the information, albeit indirectly. E.g.: An advertiser wants to target a particular category of users. Based on the profile of the user, the third party vendor can make sure that the ad only appears on pages viewed by women, and it can do so without disclosing any personal information about the women who see the advertisement. The advertiser knows that anyone who saw the ad or clicked on it is registered on the website as a female [29]. Thus, through ad targeting based on the users profile, without having access to personal information, the advertiser already has some information about the user.[4]

In addition, if the third party service provider is using Google Ad-Words, there is additional

[3] The idea for this came from reference [29], under the section 'PHRs and Consents for Disclosure'.

[4] The idea for this came from reference [29], under the section 'PHRs and Consents for Disclosure'.

threat to users' personal health information. When the third party having access to the user's personal health information combines it with Google Ads, it raises a host of privacy issues, since Google Ads are keyword/ context generated [33]. If the third party service provider, anyone with malicious intent, or a marketing company wants to compile a database of people suffering from cancer, they could trigger an ad with the keyword "Cancer". When a user accesses the third party service integrated with Google Ads, based on the keyword cancer, the ad would show up. If a user clicks the ad and he could then be asked to provide some personal details (so that he would receive some gifts say). Thus the ad provider has the detail about the user including his personal health information and personal identifiable information. Therefore, allowing ads by third party service providers pose a risk to the privacy of the users' health information. [5]

To mitigate these risks, Google Health should consider providing the user the option of choosing advertisement based third party service or advertisement free service for which user actually pays some fees for using that particular third-party service. Google Health could make arrangements with third parties in respect to that. Thus, if a user chooses third party advertisement based service, he would be accepting the risk that accompanies that service. For example, Gmail provides advertisement free service in the form of Gmail Premier Edition [39]. For this paid Gmail service, Google charges user an annual fee.

3.7 Single Sign on risk

Beside privacy risks, there are security risks that could affect the integrity and availability of the user's health information. Single sign on is a method of access control to gain access to the multiple systems using one username and password. Google provides single sign on to the users, i.e., users having a Google Account who use services like Gmail, Google Docs and many other Google products need have just one simple account. If a user is using Gmail and he is also using Google Health, the user would be using a single Google Account to log in into any Google service, e.g., Gmail and Google Health. Thus, if one account is compromised all the other accounts are compromised.

Any hacker could exploit any vulnerability in any other Google service to gain unauthorized entry to the Google Account. For example, a hacker is able to exploit any vulnerability in any available Google service like Gmail to gain unauthorized access. Since Google Account uses the same login credentials for any Google service, the hacker could gain unauthorized entry to the users Google Health account. Since Google Health contains lot of sensitive information, it is exposed to security and confidentiality risk concerning users' personal health information.

Although Google is making things lot easier for the user by providing them with single login credentials, it is also exposing users to the single sign on risks. A hacker who gains unauthorized access to the Google Health account can steal the information of the user. The stolen information could be used for identity theft. Since, Google Health contains personal details of the user, it would be easier for any unauthorized person who has access to the Google Health to build a profile of the user and sell it to marketers, insurance companies and in extreme cases maybe to the employers of the user. In fact, Google Health provides any unauthorized user a complete repository of users' minute personal details including health information.

[5] The idea for this came from reference [33].

To mitigate the risk, Google should think of delinking Google Health from other services. Thus, if any Google account is hacked, Google health will remain immune to that risk. Google Health could also let the users have different password parameters with the same user id of other Google services. Since Google health contains lot of sensitive personal health information, having different and strong password parameters would prevent the Google Health account from being exposed to risks that other Google services face.

4. Conclusion and Future Work

In this research paper I have highlighted the security and privacy risks of the Google Health patient portal, and how those risks could affect the privacy and security of users' personal health information. I have also offered suggestions as to how it would be possible for Google Health to mitigate the risks identified. While implementing these suggestions, Google Health may have to do a trade-off between ease of use and managing security and privacy risks.

Web based user managed patient portals like Google Health are a new concept. This research could serve as a base for identifying security and privacy risks of other web based patient portals, like WebMD or Microsoft Health Vault. In fact, another interesting area of research could be a comparison of security and privacy risks of Google Health with other web based user managed patient portals like WebMD or Microsoft Vault or both.

5. References

1. Patient Portals: Retrieved from Wikipedia, http://en.wikipedia.org/wiki/Patient_portals on 25th March, 2009.

2. Benefits of a patient portal: Retrieved from, Health Technology Review (October 10, 2007). Retrieved from http://www.healthtechnologyreview.com/viewarticle.php?aid=10 on 25th March, 2009,

3. Google Health privacy policy: Retrieved from, http://www.google.com/intl/en-US/health/privacy.html on 25th March, 2009.

4. Aksel Tjora, Privacy vs Usability: A Qualitative Exploration of Patients' Experiences with Secure Internet Communication with Their General Practitioner (2005). Retrieved from, http://www.jmir.org/2005/2/e15/ on 25th March, 2009.

5. Sharma S.K, Huinan Xu, Nilmini Wickramasinghe, Electronic healthcare: issues and challenges (2006). Retrieved from, http://inderscience.metapress.com/media/59dkvnwtrqcaacj2cb9q/contributions/a/3/5/g/a35g9g5xbx8qamcf.pdf on 25th March, 2009.

6. Google Public Policy Blog (May 19, 2008): Retrieved from Google Health, privacy and HIPAA http://googlepublicpolicy.blogspot.com/2008/05/google-health-privacy-and-hipaa.html on 25th March, 2009.

7. Google Health: Retrieved from Wikipedia, http://en.wikipedia.org/wiki/Google_Health on 25th March, 2009.

8. Google Health: Retrieved from About Google Health, http://www.google.com/intl/en-US/health/about/index.html on 25th March, 2009.

9. Google Helps Organize Medical Records: Retrieved from Wall Street Journal, http://online.wsj.com/article/SB121123806355705253.html on 17th January, 2009.

10. Google Health Blog (28th February, 2008): Retrieved from, http://googleblog.blogspot.com/2008/02/google-health-first-look.html on 25th March, 2009.

11. Jacqui Cheng, Google Health beta launches with security issues looming (19th May, 2008). Retrieved from http://arstechnica.com/news.ars/post/20080519-google-health-beta-launches-with-security-issues-looming.html on 25th March, 2009.

12. Google Health frequently asked questions. Retrieved from http://www.google.com/intl/en-US/health/faq.html on 25th March 2009.

13. Patient Portals: Brian Hamilton, Portfolio Officer, Office of the Information and Privacy Commissioner, Edmonton, Alberta, Access Privacy Conference, 2008. Retrieved from http://www3.extension.ualberta.ca/accessandprivacy/presentations/Hamilton-sessionB.ppt on 23rd November, 2008.

14. Information security: Retrieved from Wikipedia, http://en.wikipedia.org/wiki/Information_security on 25th March, 2009.

15. Towards the Security and Privacy Analysis of Patient Portals. Retrieved from http://www.cs.virginia.edu/sigbed/archives/2007-04/Mathe_sec.doc on 25th March, 2009.

16. Google Health and HIPAA: Retrieved from: http://www.google.com/intl/en-US/health/hipaa.html on 25th March, 2009.

17. Jessica Young and Annie I. Anton Are Google Health's Privacy Practices Healthy (20th June, 2008). Retrieved from http://theprivacyplace.org/2008/06/are-google-healths-privacy-practices-healthy on 25th March, 2009.

18. Information security awareness and privacy training programs: Retrieved from http://www.nativeintelligence.com/ni-programs/ni-benefits.asp on 25th March, 2009.

19. Google privacy centre, privacy policy: Retrieved from http://www.google.com/privacypolicy.html on 25th March, 2009.

20. Leigh A. Zaykoski, Google Health issues and concerns (Sep 15, 2008). Retrieved from http://www.brighthub.com/health/technology/articles/7254.aspx on 25th March, 2009.

21. Google accounts help: Retrieved from https://www.google.com/support/accounts/bin/request.py?ara=1&hl=en on 25th March, 2009.

22. Google privacy question: Retrieved from http://www.google.com/support/websearch/bin/request.py?contact_type=privacy on 25th March, 2009.

23. Larry Dignan, Google Health launches; Read the terms of service (May 19, 2008): Retrieved from: http://blogs.zdnet.com/BTL/?p=8866 on 25th March, 2009.

24. Google Health terms of service: Retrieved from: http://www.google.com/intl/en-US/health/terms.html on 25th March, 2009.

25. Nathan McFeters, RSnake picks on Google Health… yes, Google wants your medical records, too! (May 22, 2008): Retrieved from:

http://blogs.zdnet.com/security/?p=1166 on 25th March, 2009.

26. Simon Peyton Jones,Microsoft research, Cambridge, How to write a great research paper. Retrieved from http://research.microsoft.com/en-us/um/people/simonpj/papers/giving-a-talk/writing-a-paper-slides.pdf on 25th March 2009.

27. Google Health launched. Can we Entrust our Health to Google (22nd May, 2008): Retrieved from http://www.bluelinerny.com/blog/2008/05/22/google-health-launched-can-we-entrust-our-health-to-google/ on 25th March 2009.

28. Google Health Integration Policies: Retrieved from: http://www.google.com/intl/en-US/health/about/devpp.html on 25th March 2009.

29. Robert Gellman, February 20, 2008, Personal Health Records: Why many PHRs Threaten Privacy. Retrieved from http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf on 25th March 2009.

30. HIPAA "Business Associate" Agreements: Knowing When and How to Enter into Them. Retrieved from: http://www.nixonpeabody.com/linked_media/publications/HIPAALA_03152003.pdf on March 25, 2009.

31. Business Associate (HIPAA), Retrieved from: http://privacy.med.miami.edu/glossary/xd_business_associate.htm on 25th March, 2009.

32. HIPAA and Business Associate Puzzle: Retrieved from http://www.oandp.com/articles/2003-07_11.asp on 25th March, 2009.

33. Online PHR + Google Ad Words/Ad Sense = A Privacy Disaster (March 8, 2008): Retrieved from http://gunther-eysenbach.blogspot.com/2008/03/google-health-google-adwordsadsense.html on 25th March, 2009.

34. Google Health, What's new in Google Health: Retrieved from http://www.google.com/intl/en-US/health/whatsnew.html on 25th March 2009.

35. HIPAA Privacy Regulations, 45 C.F.R. Part 160. Retrieved from, http://www.medlawplus.com/library/legal/hipaaprivacyreg.htm?#160103 on 25th March, 2009.

36. Security Standards: Organizational, Policies and Procedures and Documentation Requirements. Retrieved from: http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsOrganizationalPolicies.pdf on 25th March 2009.

37. HIPAA Administrative Simplification, 45 C.F.R. Parts 160, 162 and 164, (February 16, 2006). Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf on 25th March 2009.

38. Excerpt from Senate Bill S. 1389. Retrieved from http://www.therapistsforsocialresponsibility.org/pdfs/Articles/Senate_B._1389.pdf on 25th March, 2009.

39. Google Apps: Retrieved from: http://www.google.com/apps/intl/en/business/editions.html on 25th March, 2009