HIPAA Compliance and Patient Privacy Protection

Tyrone Grandison[a], Rafae Bhatti[b]

[a] *IBM Almaden Research Center,650 Harry Road, San Jose, California 95120, USA*
[b] *Oracle Corporation, 500 Oracle Parkway, Redwood Shores, California 94065, USA*

Abstract

Recent prosecutions of violations of the Health Insurance Portability and Accountability Act (HIPAA), and the amendments currently in process to strengthen the Act of 1996, has led many companies to take serious notice of the measures they must take to be in compliance. A company's privacy policy states the business' privacy practices and embodies the firm's commitments to its users and is normally a mandatory step in reaching legislative compliance. In the face of this, the patient has to decipher if the company's privacy practices are congruent with their thoughts on the level of privacy protection they should be receiving. This is the core of our investigation. In this paper, we explore the question "Is a healthcare entity's compliance with regulation sufficient to provide the patient with adequate privacy protection?" in the context of the United States of America.

Keywords: Patient Data Privacy, Compliance, Legislation

Introduction

There is a significant body of evidence that shows that privacy breaches of healthcare data occurs far more often than patients believe [1]. The prevailing perception, by most non-corporate healthcare stakeholders, is that the current measures in place (i.e. legal, social, technological and business safeguards) are weak and not effective [2]. In recent times, enforcement of the legal mandates articulated for covered entities[1] has been on the rise [3].

Though not as prolific as many would like, the record of convictions under HIPAA [4] provides hope. In the first HIPAA-related criminal case (2004) [5], a phlebotomist, Richard W. Gibson, employed by the Seattle Cancer Care Alliance, obtained a cancer patient's personal information from the health record and used that to fraudulently obtain four credit cards, charging $9,000 to the patient's name. That patient, Eric Drew, tracked down the perpetrator on his own, while fighting leukemia. Gibson pled guilty and was sentenced to 16 months in prison.

In Delaware, Linda Danyell Williams, an insurance representative employed by Hospital Billing and Collection Services in New Castle, was indicted in November 2006 for allegedly conspiring to steal the identities of more than 400 of the billing company's clients and selling the data to Richard Yaw Adjei, who used 163 of the stolen identities to file false and fraudulent tax returns, seeking refunds from the Internal Revenue Service. Williams pled guilty to two counts [6].

In 2007, Liz Arlene Ramirez, an employee at a doctor's office in Texas, pled guilty and was convicted of selling confidential medical information belonging to a Federal Bureau of Investigation Special Agent to someone she believed was working for a drug trafficker. She was sentenced to six months in prison [7].

In that same year, the U.S. Attorney Southern District of Florida obtained the first medical privacy criminal conviction after a trial [7]. In that same, Isis Machado, a front desk office coordinator at The Cleveland Clinic in Weston, Florida, improperly obtained Medicare information and other demographic information about Cleveland Clinic patients in Naples, Florida, and sold that information to her cousin, co-defendant, Fernando Ferrer, of Naples, for $5 to $10 each. Machado improperly obtained the patient information of approximately 1,130 patients. That data led to $7 million in fraudulent Medicare claims. Machado pled guilty to conspiracy and testified at trial against Ferrer. Machado was sentenced to three years probation, including six months of home confinement, and ordered to pay restitution of $2.5 million. Ferrer was sentenced to 87 months in prison, three years supervised release and ordered to pay $2.5 million in restitution.

In February 2008, CVS Caremark Corp. ("CVS" for short) agreed to pay $2.25 million to settle a federal investigation into allegations that it violated HIPAA privacy regulations when pharmacy employees threw items such as pill bottles with patient information into the trash [8].

Most recently (in May 2009) [9], California health regulators fined Kaiser Permanente's Bellflower Hospital to the tune of $250,000 due to the unauthorized access, by 23 workers, of the medical records of Nadya Suleman, after she gave birth to octuplets in January 2009.

[1] Covered entities refer to health plans, health care providers and health care clearinghouses.

This stream of legal activity is slowly bolstering patients' confidence in the protection of their data, i.e. insofar as the activities of regulators are concerned. Is this phenomenon encouraging healthcare firms to elevate patient protection in their own business functions? In this paper, we explore the legislative and technical sides of this patient privacy discourse.

Method

The baseline for regulatory compliance in the American healthcare industry is thought to be HIPAA [4], the new security and privacy requirements imposed by the Health Information Technology for Economic and Clinical Health (HITECH) Act [10] and the changes to HIPAA mandated by the American Reinvestment and Recovery Act (ARRA) [11]. We used these to measure legislative compliance.

However, as the HITECH [10] and ARRA [11] Acts are still open for public comment and no one has implemented them in their organizations yet, there were removed from our study. A high-level summary of the five key principles in the HIPAA Privacy Rule are:

1. *Notification* - Patients should receive a notice of a covered entity's privacy practices.
2. *Authorization and Consent* - Written authorization is required for disclosures not permitted under the Privacy Rule.
3. *Limited Use and Disclosure* - Covered entities must use or disclose the minimum necessary PHI for a specific purpose and ensure the development and implementation of policies and procedures governing access and use.
4. *Auditing and Accounting* - Patients have the right to an accounting of all disclosures of their PHI for non-allowed HIPAA operations.
5. *Access* - Patients have the right, under most circumstances, to access the covered entity's designated record set. Covered entities must amend information that is inaccurate or incomplete.

The full descriptions of the principles can be found at the U.S. Department of Health and Human Services' website [4]. For completeness, we have to define *Protected Health Information* (PHI) as individually identifiable health information held or transmitted by a covered entity or its business associate, electronically, on paper, or orally.

For this project, a sample of 78 patients, commissioned from Amazon's Mechanical Turks [12], were selected and provided their expectations of privacy protection with regards to the principles above. The study population ranged from 23 to 68 and their county of residence covered 31 states. Each participant was given five options for each principle and asked to indicate the choice they associated most with their expected level of privacy protection.

As stated previously, a healthcare entity creates and publishes privacy documents, which describe their behavior (and implicitly establishes an agreement between themselves and their patients). A typical covered entity in our study provided an electronic copy of their HIPAA Notice of Privacy Practices[2], as required by regulation. Most organizations in our study also posted a separate Website Privacy Policy[3]. For our purposes, we use the terms "policy" and "privacy policy" to mean the virtual combination of both.

In order to answer our initial question, "Is a healthcare entity's compliance with regulation sufficient to provide the patient with adequate privacy protection?" we analyzed a sample set of privacy policies from twenty healthcare companies (chosen from the Thomson Reuters Top 100 Hospitals list [13]) with respect to patient expectations (obtained from our Amazon Mechanical Turks survey [12]). The companies in our study included Norton Healthcare, CIGNA Healthcare, West Virginia University, Interim Healthcare, Mount Auburn hospital, OSF Healthcare System, PharmaCare, Oakwood Healthcare, St Joseph's Hospital, AETNA, Blue Cross Blue Shield, Kaiser Permanente, Kindred Healthcare, United Healthcare, Camino Medical Group, Veterans Health Administration, Thomas Jefferson University Hospital, University of Michigan Health System, University of Chicago Hospital and St. Louis University Hospital. Table 1 shows the locations of the policies used.

Table 1: Companies and their Policy Locations (Accessed October 15, 2009)

#	Company	Online Policy	Notice of Privacy Practices
1	Norton Healthcare	*http://www.nortonhealthcare.com/services/services/privacypolicy.aspx*	*http://www.nortonhealthcare.com/services/services/hipaa.aspx*
2	CIGNA Healthcare	*http://www.cigna.com/privacy/privacy_statement.html*	*http://www.cigna.com/privacy/standard.html*
3	Healthcare at West Virginia University		*http://www.health.wvu.edu/privacy.htm*
4	Interim Healthcare	*http://www.interimhealthcare.com/about/privacypolicy.aspx*	*http://www.interimhealthcare.com/about/hipaa_policy.aspx*
5	Healthvision (Mount Auburn Hospital)		*http://www.mountauburn.caregroup.org/body.cfm?id=89*
6	OSF Healthcare System	*http://www.osfhealthcare.org/hipaa/*	*http://www.osfhealthcare.org/hipaa/*
7	Pharmacare	*http://www.pharmacare.com/footer/privacystatement.jsp?ms=corporate*	*http://www.pharmacare.com/footer/privacystatement.jsp?ms=corporate*
8	Oakwood Healthcare	*http://www.oakwood.org/?id=147&sid=1*	*http://www.oakwood.org/?id=147&sid=1*
9	St. Joseph's Hospital	*http://www.sjhlex.org/body.cfm?id=49*	*http://www.sjhlex.org/body.cfm?id=49*
10	Aetna	*http://www.aetna.com/about/privacy.html*	*http://www.aetna.com/about/information_practices.html*
11	Blue Cross Blue Shield	*http://www.empireblue.com/wps/portal/ehpfooter?content_path=shared/noapplication/f0/s0/t0/pw_ad068128.htm&label=HIPAA%20Privacy%20Notice*	*http://www.empireblue.com/wps/portal/ehpfooter?content_path=shared/noapplication/f0/s0/t0/pw_ad068128.htm&label=HIPAA%20Privacy%20Notice*
12	Kaiser Permanente	*http://members.kaiserpermanente.org/kpweb/privacystate/entrypage.do*	*http://members.kaiserpermanente.org/kpweb/privacystate/entrypage.do*
13	Kindred Healthcare	*http://www.kindredhospitalnola.com/privacy.asp*	*http://www.kindredhospitalnola.com/PrivacyPractices.asp*
14	United Healthcare	*https://www.unitedhealthcareonline.com/b2c/CmaAction.do?channelId=064985642192b010VgnVCM100000c520720a___*	*https://www.unitedhealthcareonline.com/b2c/CmaAction.do?channelId=c42985642192b010VgnVCM100000c520720a___*
15	Camino Medical Group	*http://caminomedical.org/privacy/index.html*	*http://caminomedical.org/privacy/npp.html*
16	Veterans Health Administration (VHA)	*https://www.vha.com//portal/server.pt/gateway/PTARGS_0_0_268_0_0_47/public/aboutvha/privacy.asp*	*http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1089*
17	Thomas Jefferson University Hospital	*http://www.jeffersonhospital.org/about/article5070.html*	*http://www.jeffersonhospital.org/about/article5071.html*
18	University of Michigan Health System	*http://www.med.umich.edu/prmc/privacy.htm*	*http://www.med.umich.edu/hipaa/npp_official.htm*
19	University of Chicago Hospitals		*http://www.uchospitals.edu/visitor/privacy/notice.html*
20	St. Louis University Hospital	*http://www.sluhospital.com/CWS/PrivacyPolicy.aspx?hostName=sluhospital#privacy*	*http://www.sluhospital.com/CWSContent/sluhospital/aboutUs/JointNoticeOfPrivacyPractices.htm*

Results

Generally, the surveyed companies structured their policies to convey information on the following areas: Collection of In-

[2] The HIPAA Notice of Privacy Practices (NOPP) is a document that specifies how the organization maintains the privacy of members' medical information. An electronic copy of this notice is posted on their website.

[3] The Website Privacy Policy only applies to information collected, used and or disclosed through the company's website.

formation, Information Types, Information Use and Changes to Information. There were slight differences in terminology amongst the policies, but the higher level concepts were equivalent. We found the policies clear in their articulation of the information that they collect. This information falls into one of three classes: 1) *Protected Health Information*, which includes name, address, social security number, email address, licensure, certifications, education and employment history, etc. and is normally assumed critical for the delivery of care and the company's normal business functions, 2) *Derived Information*, which includes individual access history and usage patterns, which is gathered through cookies in order to improve their site and allow personalization or customization, and 3) *Aggregate Information*, which is statistical information, consolidated from IP addresses, computer information and locations (amongst other things), for promotion and marketing.

From the Mechanical Turks study, the top choices for each of the principles in the HIPAA Privacy Rule were:

1. *Notification* - Patients expect notifications sent to them of privacy practices' changes within days of the change.
2. *Authorization and Consent* - Patients expect authorization and consent for each non-authorized disclosure.
3. *Limited Use and Disclosure* - Patients expect healthcare payers and providers to enforce rules that ensure their business partners do not abuse their information.
4. *Auditing and Accounting* - Patients expect timely (a few days) response when they request an accounting of who touched their PHI.
5. *Access* - Patients expect to be able to see the information a healthcare entity has on them and they expect to be able to quickly correct any inaccurate information.

When analyzing each privacy policy, we examined the policy stipulations against the requirements of the HIPAA Privacy Rule and the expectations of patients. The results show that a majority of the policies were in a satisfactory compliance state with regards to legislation and that they all fell short of patient expectations.

Each of the following sections goes into more detail on our findings.

Notification, Authorization and Consent

At the start of their policies, the healthcare companies either stated (1) that they do not collect personal information from web page visitors, but do collect web usage statistics in the aggregate form and if one wishes to register with them, then personal information will be collected or (2) that by accessing the companies' web pages you have consented to their privacy policy. Both cases lead to a situation where the patient is assumed to have implicitly consented to the privacy policy through the action of browsing the companies' web pages. It is debatable if this is in the spirit of the HIPAA Privacy Rule. However, it is clearly outside of patient expectations.

There was also an interesting trend present in the statements about the communication of policy updates to the patients. From the companies' policies, a majority of the organizations were content with simply updating the policy on the website, and making it the responsibility of the user to check for policy changes. It is a general theme that privacy policy changes are communicated with very little concern for the patient. There were a few exceptions to the rule which actually indicated that they would alert the patient (via email, etc.) in case of a policy update.

Limited Use and Disclosure

For all the firms in the study, use and disclosure of information are associated with a purpose and specific purposes are defined for information. However, we found that many organizations defined very broad and all encompassing purposes, which may be used to exploit exceptions in the HIPAA Privacy Rule. For example, quite a few policies mention collecting information for the purpose of "administering healthcare". They settled for a granularity so coarse that it could subsume a huge category of uses and disclosures of information. As a result, a whole host of activities, which the patient may not be in agreement with, could be interpreted as included within these purposes.

For disclosures to third parties and affiliates, it is common to see the phrase "we require the third parties to comply with Policy". However, there are two significant hurdles here. Firstly, a proposition to either "comply with policy" or to have "use limited by policy" is only meaningful if the policy is not broadly defined and implicitly inclusive of a wide range of business functions. Secondly, apart from business associate contracts with the third parties that perform services, requiring PHI, for them, there are no guarantees of the actual enforcement of policy on the third party. Ideally, covered entities should proactively monitor third parties to assure that they comply with the business associate agreements. However, the policies make no mention of the (general) terms and ramifications of such agreements.

None of the privacy policies surveyed provided a fine-grained list of roles or employee categories who have the authorizations to view specific categories of patient data. For internal use, the collected information is available to all "members of medical staff". This is the only requirement for being an "authorized" employee. Nowhere are the precise conditions for being "authorized" stated, nor is there any criteria specified under which any exception-based accesses may be granted (such as in "break the glass" scenarios). Overall, the counsel or consent of the patient is not incorporated in assigning more specific access privileges to employees.

Audit and Accounting

The privacy policies of all organizations advise that patients can obtain audit records for information disclosures. Most policies mention that protected health information may be disclosed to government and regulatory authorities for compliance with law. Although not explicitly stated on the websites, the literature from the medical community [14] suggests that most organizations advocate the use of audit trails of all actions pertaining to patient medical records to meet the audit

reporting and accounting requirement. Our experience with clients indicates that audit trails do not record all the necessary context information, such as purpose and recipient amongst other attributes. More alarmingly was the tendency of corporate executives to turn off audit systems because of the storage and performance burden incurred when they ran.

Access

The privacy policies posted on all the websites in our survey indicated that patients have the right to access or update their personal information maintained by the company through phone or email or an online account. However, the response time was in the order of weeks and normally in written form.

Discussion

For each of the principle areas examined in our study, there was useful insight that we gained while examining the policies. Here we share some of these lessons.

Notification, Authorization and Consent

Current practices around issuing a notice and obtaining consent are not sufficient unless they provide the patient an opportunity to clearly and easily understand the policy and negotiate any objectionable provisions. This will continue to be a manually intensive task unless the policies are presented to the patient in a format that not only highlights the key segments in the policy, but also allows reasonable modifications to be made by the patient at his/her discretion. The use of P3P[4] and APPEL technology, for example, may facilitate this task. Though recent studies have shown that privacy policies are unreadable by their target audience, irrespective of their format, [15] and that less than 26% of Internet users read privacy policies [16], we assert that the codification of policy would enable computer to analyze them and visualize potential problems, perhaps based on a specification of the user's concerns or hot buttons.

We also noticed that very few websites actually published a policy in machine-readable form, e.g. P3P, or any similar electronic privacy language, and only the natural language version is available online for manual review. The fact that no P3P policy is available on the website precludes anyone from performing automated interpretation and analysis.

Limited Use and Disclosure

While HIPAA requires organizations to obtain unambiguous authorization of the patient before use or disclosure of information for a purpose other than what it was collected for, and recommends adoption of the principle of minimum necessary disclosure, HIPAA-compliant policy can be constructed that allows organizations to design policies with broadly defined purposes. This concern has also been highlighted in the public media [17]. For instance, while "marketing" is identified as a purpose that requires authorization, various sub-categories are defined, such as "communications for treatment of patient", that are exempt from the rule, making it possible to disclose patient data for marketing under the assumed purpose. Therefore, it may be assumed that the levels of disclosure post-HIPAA will not necessarily shrink, and in fact a data disclosure previously considered a breach may now fall within the folds of the policy to which the patient has consented. Anton et. al. [18] observe a similar phenomenon, where the number of information disclosures increased post-HIPAA.

Audit and Accounting

The fact that current healthcare audit systems do not capture the required context information in order to provide an accounting was the most striking observation. Even though HIPAA requires organizations to account for all activity (including data disclosures) and provide detailed reporting for audit purposes, fulfilling this requirement by itself would still not be effective in improving levels of privacy protection unless measures are taken to compensate for shortcomings in the data disclosure and access rules in the privacy policy.

When the purpose or authorization is not established at a fine granularity before any disclosure or access is allowed, the burden falls on the audit mechanism to be able to capture any action that may actually constitute as a violation of the policy. Additionally, when an exception-based mechanism is in place that allows users to override normal access controls, the need for audit-based controls is further accentuated. While an argument can be made that the deterrent factor of audits is more suited to the healthcare sector because of the critical nature of the services provided, it should certainly not become an excuse for failing to do better.

Access

Meeting this requirement may not translate to adequate privacy protection for patient. There are several reasons for this. First, the ability of a patient to access or update personal information maintained by the organization provides no measure of how much information is actually protected unless the patient is also in control of the use and disclosure rules, and, based on our preceding discussion, this is not the case. Second, navigating the processes of information access and update can be simple or laborious for the patient depending on the organization. In some cases, data retrieval may be a matter of few mouse clicks online. In others, one may have to wait up to 60 days to receive a paper copy of one's information.

Further Observations

From our analysis, the language used in the privacy policies appears to be unnecessarily convoluted. This is corroborated by other researchers in the field [19, 20] for healthcare and finance. Given this, it will likely not be understandable by the average patient. In other cases, the language was clearly ambiguous. For example, one policy in the study states "……will not sell, license or transmit to anyone any personal information that members or practitioners provide to us online. We may

[4] Platform for Privacy Preferences (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents, which can be machines or humans.

disclose information obtained online to our partners involved in administering or providing services for our health benefits plans". These are possibly two seemingly contradictory, yet consistent statements that seem to have a nullifying effect on each other.

Conclusion

The overall message from our study was that even though the privacy policies cover enough ground to enable healthcare organizations to claim regulatory compliance, they are not adequate to communicate understandable privacy practices to the patient or provide adequate privacy safeguards. Even more importantly, current privacy policies do not reflect what patients think are in their best interest.

We believe that, while using artifacts such as broadly-defined purposes, exception-based accesses and umbrella authorizations may still allow the organizations to claim regulatory compliance, organizations should strive to do better. It is only a matter of time before gaining customer confidence and trust with regards to privacy concerns plays a more significant role.

References

1. Privacy Rights Clearinghouse. A chronology of data breaches. ttp://www.privacyrights.org/ar/ChronDataBreaches.htm.
2. RAND and the Institute for Health Policy Solutions. "Effectiveness of HIPAA and state laws in ensuring access to health insurance in the small group and individual markets". Report to Congress. Article date: March 22, 2001. http://www.allbusiness.com/finance/3585318-1.html Accessed October 15, 2009.
3. Marsan, CD. "Health privacy undermined: Worst breaches of 2009". Network World, 09/02/2009. http://www.networkworld.com/slideshows/2009/090209-health-breaches.html. Accessed October 15, 2009.
4. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability (HIPAA) Act, http://www.hhs.gov/ocr/hipaa/.
5. Shukovsky, P. "Hospitalized man catches identity thief". Seattle PI. August 20, 2004. http://www.seattlepi.com/local/187126_identitytheft20.html Accessed October 15, 2009.
6. O'Sullivan, S. "ID Thief gets prison time in tax fraud". Delaware Online - THe News Journal. April 18, 2007. http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20070418/NEWS/704180354/1006/NEWS Accessed October 15, 2009.
7. Sorrel, AL, "3rd HIPAA criminal case hints at federal tactics". American Medical News. Oct 16, 2006. http://www.ama-assn.org/amednews/2006/10/16/gvsb1016.htm Accessed October 15, 2009.
8. US Department of Health & Human Services (HHS) Press Office. "CVS Pays $2.25 Million and Toughens Practices to Settle HIPAA Privacy Case". News Release. February 18. 2009 http://www.hhs.gov/news/press/2009pres/02/20090218a.html Accessed October 15, 2009.
9. Collins, E. "California Hands Down Maximum $250,000 Penalty for Employee Snooping Into Patient Records at Kaiser Permanente Bellflower Medical Center". AIS's Health Business Daily. June 10. 2009. http://www.aishealth.com/Bnow/hbd061009.html Accessed October 15, 2009
10. U.S., Health Information Technology for Economic and Clinical Health (HITECH) Act, http://waysandmeans.house.gov/media/pdf/110/hit2.pdf
11. U.S., American Recovery and Reinvestment Act (ARRA), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf
12. Amazon Mechanical Turks, https://www.mturk.com Accessed October 15, 2009.
13. Thomson Reuters. "100 Top Hospitals: 2009". March 30, 2009. http://www.modernhealthcare.com/section/lists?djoPage=product_details&djoPid=10537&djoTry=1249923457 Accessed: October 15, 2009.
14. Blobel, B. "Authorization and Access Control for Electronic Health Records". International Journal of Medical informatics, 73(3), 2004.
15. McDonald, A., Reeder, R., Kelley, P., Cranor, L. Comparative Study of Online Privacy Policies and Formats. The Proceedings of the 9th Annual Privacy Enhancing Technology (PET) Symposium (PETS 2009). August 5-7, 2009. Seattle, WA, USA
16. Jensen, C., Potts, C. and Jensen, C. Privacy practices of Internet users: Self reports versus observed behaviour. International Journal of Human-Computer Studies 63 (July 2005), 203-227.
17. Pear, R. Warnings over privacy of us health network. New York Times, February 18, 2007.
18. Anton, AI, Eart, JB, Vail, MW, Jain, N, Gheen, CM, and Frink, JM. HIPAA's effect on web site privacy policies. IEEE Security and Privacy, 5(1):45–52, Jan/Feb 2007.
19. Hochhauser, M. Lost in the fine print: Readability of financial privacy notices, July 2001. http://www.privacyrights.org/ar/GLB-Reading.htm.
20. Graber, M. A., D'Alessandro, D. M., Johnson-West, J. Reading level of privacy policies on internet health web sites. Journal of Family Practice (July 2002).