# An Analysis of Web Site Privacy Policy Evolution in the Presence of HIPAA

Annie I. Antón[1], Julia B. Earp[2], Matthew W. Vail[1], Neha Jain[1], Carrie Gheen[2], Jack M. Frink[1]

[1]College of Engineering, North Carolina State University, Raleigh, NC 27695-8207, USA (919.515.5764)
[2]College of Management, North Carolina State University, Raleigh, NC 27695-7229, USA (919.513.1707)

[1]{aianton, mwvail, njain, jmfrink}@eos.ncsu.edu, [2]{julia_earp, cmgheen}@ncsu.edu

**Abstract**

*The U.S. department of Health and Human Services' (HHS) Privacy Rule requires healthcare institutions to notify their customers about the institution's privacy practices. Privacy practices are typically posted online in the form of privacy policy documents, which are intended to help consumers develop an understanding of how their sensitive information is used. We investigate the online privacy practices of three categories of healthcare Web sites — pharmaceuticals, health insurance companies and online drugstores — and present our analysis of 24 online privacy documents from nine institutions. Our study provides a unique perspective on the state of privacy practices before and after HIPAA's enactment, by comparing our current results to our pre-HIPAA (Health Insurance Portability and Accountability Act) study of these same institutions' privacy practices. We discuss how HIPAA's introduction has resulted in more descriptive and detailed privacy policies but has not necessarily improved the online privacy practices of these organizations. The results of this analysis may be helpful for forecasting how future legislation will affect the state of online privacy in other domains.*

## 1. Introduction

Approximately eighty percent of adult Internet users consult online healthcare services for health information, making healthcare research the third most popular online activity behind email and researching a product before buying it [Fox03]. The Pew Project surveyed 2,038 adults in 2002 to examine the kinds of information Internet users seek online; this survey revealed that people searching for health information use the Internet to become informed, share information, seek and provide support, as well as schedule appointments [Fox03]. The evolving trend toward Internet supported healthcare services has resulted in increased information sharing among providers, pharmacies and insurers. However, according to recent studies [AER02, GHS00], inconsistencies exist between privacy policies and the actual privacy practices of healthcare-related Web sites.

The Privacy Act of 1974 protects medical records held by federal agencies, but not those held by private groups where most medical records are actually created and stored[1]. The 1996 Health Information and Portability Accountability Act (HIPAA)[2] mandated that the U.S. Government Administration introduced regulations for health information privacy. The Department of Health and Human Services (HHS) published the final Privacy Rule[3] that took effect on April 14, 2001, requiring healthcare providers and health plans to comply by April 14, 2003. The new regulations specify several procedures regarding PII (Personally Identifiable Information) disclosure that should be reflected in healthcare Web site privacy policies [BEP00]. However, our previous work shows these Web sites are inconsistent in their treatment of PII [AER02], and these findings led us to examine whether the enactment of HIPAA's Privacy Rule has resulted in improved online healthcare privacy policies.

---

[1] 5 U.S.C. 552a (1994)

[2] Health Insurance Portability and Accountability Act of 1996, 42 U.S.C.A. 1320d to d-8 (West Supp. 1998).

[3] Federal Register 59918 et seq., Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160 through 164, Standards for Privacy of Individually Identifiable Health Information, (December 28, 2000).

This paper discusses a unique longitudinal study that examines the effects of HIPAA's enactment on a collection of privacy policy documents for a fixed set of organizations over the course of four years. Specifically, we present our analysis of 24 healthcare privacy policy documents from nine healthcare Web sites, analyzed using a content analysis technique called goal-mining. Goal-mining is an analysis method that supports extraction of useful information about institutions' privacy practices from documents. We compare our results to a pre-HIPAA study [AER02] of these same institutions' online privacy practices and evaluate their evolution in the presence of privacy laws.

## 2. Analyzing Healthcare Privacy Policies

For this study, we analyzed 24 online privacy documents from nine healthcare institutions using goal-driven requirements engineering and text readability metrics [AER02]. Our sample consists of Web sites from three pharmaceutical companies (GlaxoSmithKline, Novartis and Pfizer Inc.), three health insurance companies (Aetna, AFLAC and CIGNA) and three online pharmacies (DestinationRx, Drugstore.com and HealthCentral). Each of these healthcare institution's privacy statements had been previously analyzed using the same goal-driven approach during the summer of 2000 prior to HIPAA's enactment [AER02]. The 24 privacy policy documents examined for this study were in force on September 4, 2003.

### 2.1 Using Goals to Analyze Policies

We employed a content analysis technique, goal-mining, to derive the privacy-related goals of various Internet healthcare websites. As previously mentioned, *goal-mining* refers to the extraction of goals from data sources by the application of goal-based requirements analysis methods [AE04]. The extracted goals are expressed in structured natural language [AEB04]. Analysts begin the goal-mining process by first exploring any available information sources, in this case privacy policies, to identify goals. Goals are then organized according to goal class (privacy protection or vulnerability) as well as according to keyword and subject (e.g. browsing patterns, personalization, cookies, etc.). These goals are documented and annotated with auxiliary information, including the responsible agents, in a Web-based Privacy Goal Management Tool (PGMT) [AEB04] developed at North Carolina State University.

Goals are extracted from source documents by identifying action verbs in policy statements. Every statement is examined and analyzed by asking, *"What goals does this statement or fragment exemplify?"* and/or *"What goal(s) does this statement obstruct or thwart?"* Consider the following example from Drugstore.com's privacy policy:

> *"We may enter into an agreement with other companies or individuals to perform functions on our behalf. These functions may include sending promotional e-mails on our behalf to such company's customers; serving advertisements on our behalf, providing marketing assistance; processing credit card payments; and fulfilling and delivering orders."*

By asking the goal identification questions, we identify the following goals contained within the PGMT goal repository:

$G_{867}$: USE customer email address for marketing and promotional purposes

$G_{642}$: SHARE CI (Customer Information) w/ subsidiaries to recommend services to customer

$G_{1166}$: SHARE CI w/ 3rd parties to perform marketing services on our behalf

$G_{1167}$: SHARE CI w/ 3rd parties to provide valuable financial services we do not offer (e.g. credit card)

Identified goals are classified in several ways: as privacy protections or vulnerabilities and according to subject matter. *Privacy protection goals* express ways in which sensitive information is protected.

*Privacy vulnerabilities* reflect ways in which sensitive information may be susceptible to privacy invasions. Goals not relevant to privacy or privacy-related functionality are marked as unclassified.

There are five kinds of privacy protection goals: notice and awareness, choice and consent, access and participation, integrity and security, and enforcement and redress. *Notice and awareness* goals reflect ways in which customers are notified and/or made aware of an organization's information practices before any information is actually collected from them. *Choice and consent* goals reflect ways in which a Web site ensures that consumers are given options as to what personal information is collected, how it may be used and by whom. *Access and participation* goals reflect ways in which consumers access, correct and challenge any data about themselves; for example, by providing a means for consumers to ensure their data is accurate and complete. *Integrity and security* goals reflect ways in which a Web site ensures that data is both accurate and secure. Finally, *enforcement and redress* goals reflect ways in which a Web site enforces its policies.

There are seven kinds of vulnerabilities: information collection, monitoring, personalization, storage, transfer, aggregation and contact [AER02]. *Information collection* addresses how and what information is being collected from the consumer by an institution, either by directly requesting information or by collecting information without consent. *Information monitoring* reflects ways in which organizations may track when consumers use their site (e.g., via cookies) often times with the expressed intent of providing benefits to the consumer, such as a customized online experience. *Information personalization* reflects Web site customization and tailoring of the functionality and content offered to individual users. *Information storage* refers to what and how information is maintained in an institution's database. *Information transfer* concerns any transfer of information from one entity to another. *Information aggregation* concerns the combination of previously gathered PII with data acquired from other sources. *Contact* concerns how, and for what purposes, an organization contacts a consumer.

As previously mentioned, goals are also classified according to subject matter (e.g., browsing patterns, personalization, cookies, etc.). Once goals are classified in the PGMT, they must be further refined. Goal refinement entails removing synonymous and redundant goals and resolving any inconsistencies that exist within the goal set. Consider the following two goals:

$G_{1187}$: AVOID disclosing names, address, email to 3rd party w/o consent

$G_{1183}$: AVOID sharing sensitive PII with 3rd parties w/o customer consent.

These goals are synonymous and thus redundant because names, addresses and email addresses are all considered forms of PII. Thus, these goals were merged by eliminating goal $G_{1187}$ and replacing it with goal $G_{1183}$. The objective here is enable goal reuse by capturing the high level intent of the goal. The goal refinement process helps create a standardized, non-redundant goal set in the PGMT repository. Given this understanding of goal analysis, we now discuss our pre-HIPAA case study.

### 2.2 Evaluating Privacy Documents for Readability

Natural language policies are difficult for average Internet users to read and understand [AEB04]. Several of the analyzed privacy documents were unclear and difficult to comprehend. To quantify the readability of these documents, we employed the Flesch Reading Ease Score (FRES) and Flesch-Kincaid Grade Level (FGL) score methods [Fle49]. The FRES and FGL methods provide a standardized and statistical metric to objectively analyze the text contained in documents. The Flesch metrics give an approximate measure of a text's difficulty. The FRES is often used to evaluate legal documents and is used to regulate the complexity of insurance policies in more than 16 states [AEB04]. The FGL is a number that estimates the number of years of schooling required for an individual to be able to read and understand a document; for example, a score of 9.0 means that a ninth grader would be able to understand a document. These two readability metrics (see Table 1) are based on a formula that considers the sentence length and word choice (based upon number of syllables) to determine the overall readability of

a document. The FRES is a scale from 0 to 100, with 0 representing a difficult document to read, and 100 representing an easy document to read. Average sentence length for a score of 0 is 37 words and for a score of 100 is 12 words or less [Gno04].

| |
|---|
| **Flesch Reading Ease Score:** |
| 206.835 – 84.6 * (total syllables / total words) – 1.015 * (total words / total sentences) |
| **Flesch-Kincaid Grade Level:** |
| (0.39 * average sentence length (in words)) + (11.8 * average number of syllables per word) – 15.59 |

**Table 1: Flesch Metrics Formulas**

The FRES and FGL scores for each analyzed privacy document are shown in Table 2. The FGL reading difficulty scores were calculated using Microsoft Word[4], which returns correct grade levels for values less than 12. For values greater than 12, the average syllables per word were extracted from the Flesh Reading Ease score returned by Word, and then used in the Flesch-Kincaid grade level formula; 206.835 – (1.015 x average sentence length) – (84.6 x average syllables per word).

The pre-HIPAA scores were calculated for privacy policy documents that were in effect during the summer of 2000 before HIPAA went into effect. Table 2 also provides an average score for all the post-HIPAA privacy documents for a given site, including Legal Disclaimers and Terms of Use.

### 2.3 Process Support

As previously mentioned, this post-HIPAA study replicates a portion of the previous pre-HIPAA study, allowing us to compare the privacy practices that were in place prior to the HIPAA Privacy Rule effective date with those that were in place after April 14, 2003. Both studies were conducted in a similar fashion; however, the PGMT was not available during the pre-HIPAA study. Instead, spreadsheets were used to keep a list of the goals and the number of times the various goals occurred. Using the PGMT in the post-HIPAA analysis allowed more policies to be analyzed in a shorter time period. Additionally, the goal-mining heuristics and analysis process are now much more refined, having been validated on several different case studies [AER02, AEB04, AHB04]. The pre-HIPAA study took 180 person-hours to extract goals from 23 privacy documents using spreadsheets. In contrast, the PGMT greatly improved our efficiency, as reflected by it taking only 34 person-hours to extract goals from the 24 post-HIPAA documents.

## 3. Post-HIPAA Findings

Our longitudinal study yielded several lessons learned that we believe to be of interest to policy makers, consumers, government agencies, e-service providers and policy enforcement agencies such as the HHS and the Federal Trade Commission.

***Information transfer practices are more common post-HIPAA.***

To gain a better understanding of how privacy statements evolved, we examined changes in the specific categories within protection goals and vulnerabilities. As shown in Figure 1, the vulnerability category with the most significant increase was *Information Transfer*. This is not surprising given that HIPAA requires institutions to inform consumers of those privacy practices that may result in the transfer

[4] http://www.microsoft.com/office/word/

of their PII to another entity. This sizeable increase in information transfer practices suggests that HIPAA has caused companies to disclose more information, but it is also concerning because it implies that these companies are exchanging large amounts of sensitive information while consumers may not understand the ramifications of such transfers.

***Some practices may still be concerning to consumers.***

HIPAA requires organization to "make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request" [HHS03]. Unfortunately, as we observed in our study, many of the self-governed business transactions that result in the sharing of sensitive data seem questionable. For example, Drugstore.com's Terms of Use document states that they "may disclose any content, records, or electronic communication of any kind ... if such disclosure is necessary or appropriate to operate the site." Because HIPAA allows organizations to self-govern what a reasonable effort is to protect data, a consumer would find it difficult, if not impossible, to discern what constitutes an "appropriate" disclosure. Additionally, although both the number of protection goals and vulnerabilities increased within the nine companies' policy documents, the number of vulnerabilities increased by 6 times in contrast to an increase in the number of protection goals of 3.5 times (see Table 2). This differs from the pre-HIPAA study in which we identified more protection goals than vulnerabilities. Thus, it suggests that consumers' sensitive information is more susceptible to privacy breaches now than prior to HIPAA's enactment.

***Notice & awareness as well as integrity & security practices are more common post-HIPAA.***

In the protection goals category, as illustrated in Figure 2, the two protection goal categories in which the number of occurrences increased the most (post-HIPAA) were the *Notice and Awareness* and *Integrity and Security* categories. With the enactment of new legislation, organizations are conveying more information to consumers regarding their privacy practices. In contrast, pre-HIPAA organizations were not required to convey this information to consumers. The increase in privacy statements related to notice and awareness is encouraging, as it illustrates organizations' attempts to notify consumers of their business practices and possible compromises to consumers' sensitive data.

***Consumers still have very little control over their personal/sensitive information.***

The increase in *Choice/Consent* goals was not dramatic, suggesting that consumers now have no more control than before over how their information is used. Even though consumers appear to be receiving more information, they still have little control over how their sensitive information is being used, stored and disclosed. This lack of control is exacerbated by the fact that consumers often provide implicit consent to these terms and organizations' privacy practices by simply using an organization's Web site.

***HIPAA has yielded a greater number of unique privacy statements, making it more difficult to compare different organizations' practices.***

Another interesting metric to examine is the extent to which we were able to reuse goals from the pre-HIPAA study in this study. The ability to reuse goals indicates some stability in the way some privacy practices are expressed. In a sense, these goals survived the introduction of HIPAA. In contrast, when few goals are reused it suggests that the introduction of HIPAA required a fundamental change in the way privacy practices are now expressed or the need for organizations to express a broader range of privacy practices.

In this study, although the total number of goals increased, the percentage of goal reuse dropped from 69% (pre-HIPAA) to 43% (post-HIPAA) and the total number of unique/new goals increased from 133 (pre-HIPAA) to 366 (post-HIPAA). We observed that prior to HIPAA, healthcare privacy documents were strikingly similar, and in some cases several privacy policy sections were even identical across different organizations. Given that HIPAA now requires more detailed notices about an organization's

privacy practices, it is reasonable to see more detailed, company-specific information expressed in these policy documents. To the benefit of consumers, this has resulted in more complete and unique privacy documents. At the same time, this increase in uniqueness makes it more difficult for consumers to compare the practices of different organizations as is the case with financial privacy documents [AEB04].

The types of vulnerabilities that appear to have survived HIPAA's introduction are those that reflect liability disclaimers and general information collection (such as cookies). The types of protection goals that appear to have survived HIPAA's introduction are the inform goals (e.g., `INFORM customer of intended use of PII`) and the security goals (e.g., `MAINTAIN procedural safeguards to protect PII`).

***Healthcare privacy policy documents are now more difficult to comprehend.***

The introduction of HIPAA has made healthcare privacy policy documents more difficult to comprehend. The readability of the all the privacy documents within the examined organizations decreased as shown in Table 2. The average FGL for all privacy documents increased from 13.3 (pre-HIPAA) to 14.2 (post-HIPAA), and the average FRES decreased from 39.6 (pre-HIPAA) to 34.9 (post-HIPAA). The increase in the FGL is the equivalent of almost an entire grade level of education, making the already difficult to understand documents less comprehensible to a large percentage of the general population. An FGL score of 14.2 is the equivalent of 2 years of college education or an associate's degree. Studies have shown that only 52.1% of the general population has obtained this level of education [NTI02].

The average FGL score for an organization's main "privacy policy" document increased from 13.3 (pre-HIPAA) to 13.87 (post-HIPAA) and the FRES also increased from 36.86 (pre-HIPAA) to 38.3 (post-HIPAA). However, the newly added privacy related documents (e.g. Terms of Use, Legal Disclaimers, Privacy Facts, etc.) received significantly higher FGL scores (see Table 2: Novartis's terms of use yields a FGL of 16.7 compared to a FGL of 13.8 for its privacy policy) and lower FRES scores (Novartis' Terms of Use FRES score is 27.2, whereas the Privacy Policy FRES score is 38.2), making them the most difficult to understand. Interestingly, these documents also generally contain a higher ratio of vulnerabilities to protection goals. This is alarming because consumers should not be burdened with having to read complex documents to uncover these possible compromises to their sensitive information. Moreover, these documents seem to convey a misleading sense of protection to consumers with promising statements at the beginning of the document. For example, HealthCentral.com stated, "HealthCentral is deeply committed to preserving your privacy" in the first paragraph of their Privacy Policy. However, their legal disclaimer contains only six protection goals and 18 vulnerabilities. Additionally, HealthCentral's Privacy Policy yielded a FGL score of 14.2, implying that only less than 30% of the general population can comprehend its content [NTI02]. This, combined with the fact that there are three vulnerabilities to each protection goal in this document, seems to contradict the organization's expressed commitment to their customers.

***Healthcare institutions are employing deeper linking post-HIPAA.***

In the summer of 2000, each of the analyzed organizations had a single privacy policy document posted on their Web site. At this time, healthcare institutions generally only provided a single link but this link was not always available from the organization's main homepage. Most company homepages now display at most two links: a privacy policy link and a legal disclaimer link. From these pages, some companies provide links to several additional Web pages containing more privacy practice-related information. We found this "deep linking" inconvenient because it requires one to continue clicking on links to ensure all privacy related information has been located. Moreover, although these documents contain some redundant information, much of the information differs across the multiple documents. Therefore, consumers must read all of the privacy documents in their entirety to fully understand the

privacy practices of a given healthcare organization. We observed an increase of up to seven privacy policy documents per organization in our post-HIPAA study.

***Lengthier and more numerous privacy policy documents have increased the burden on consumers.***

Not only has the number of policy documents increased but their readability has also decreased. The documents in the post-HIPAA study were lengthier and contained more information about the privacy practices of the institutions than the pre-HIPAA documents. Thus, consumers are now burdened with having to read lengthier documents that are more difficult to comprehend in order to properly evaluate how an institution's privacy practices may affect him or her. On average an institution's main privacy policy document is now approximately two times the length of the same pre-HIPAA privacy document. For instance, Health Central's privacy policy contains 1,278 words compared to its pre-HIPAA version, which contained only 683 words. The total number of policy documents for the nine analyzed institutions also increased from nine (pre-HIPAA) to 24 (post-HIPAA). The addition of 15 new documents yielded a significant increase in goal occurrences from 153 goals (pre-HIPAA) to 656 goals (post-HIPAA). This increase suggests that the introduction of HIPAA has caused online healthcare organizations to be more comprehensive in describing their online privacy practices.

***HIPAA has caused a shift in the content emphasis in the policies of different healthcare Web site categories.***

Our pre-HIPAA study suggested that the number of privacy goals extracted from a privacy policy document depends on the type of Web site as well as the content of the given policy. For example, health insurance sites tend to yield the least number of goals because they are more regulated and have less flexibility in how they manage personal information. Our post-HIPAA study also suggests that the number of privacy goals extracted depends on the type of website. However, in the post-HIPAA study, health insurance sites tended to yield the most number of goals. For example, the health insurance sites yielded 42% more goals than online drugstores and 73% more goals than pharmaceutical companies. This seems to be due to the myriad of different insurance plans offered by the health insurance companies, each of which had its own privacy document associated with it. This resulted in the increase of total posted privacy documents, and thus an increase in the total number of goals on health insurance-related websites.

**4. Summary**

Privacy concerns are a serious impediment to expanded growth of Internet commerce and provision of online healthcare services. Often times, the only guide users have as to how an institution will use, disclose and store sensitive information is via an institution's online privacy policies. For this reason, one should expect these privacy policy documents to be both descriptive about an institution's privacy practices and presented in a manner that conveys these practices to consumers with ease and clarity. Whereas HIPAA's enactment has resulted in more detailed and descriptive policies to the benefit of consumers, this study also reveals an increased lack of readability and clarity of the same policies.

Most Web sites display a privacy policy that describes the site's privacy-related information practices. However, in spite of the many guidelines for the content and layout of these policies, privacy policy content inevitably differs from site to site, even in the presence of laws which would be expected to lead to some form of standardization. Because of the lack of standardization and the varied use of terms by each institution, the process of comprehending the meaning of the privacy policies proved challenging and tedious. While most Internet users are concerned with their privacy and how their PII is being used, the effort one must expend to fully discern the privacy practices of the nine institutions we examined is plainly unrealistic. For example, it took experienced analysts with the aid of well-defined heuristics and the PGMT an average of 1.5 hours to analyze each privacy document. For some institutions, it even required an entire day to fully understand how that institution handles sensitive information.

The main objective of this study was to evaluate the evolution of privacy policies in the presence of HIPAA. The availability of our pre-HIPAA analysis data and the introduction of HIPAA offer a unique opportunity to evaluate how nine institutions' privacy policy documents evolved in response to a new Federal law. To our knowledge, we are the first to conduct a longitudinal study of this kind, which allowed us to examine a collection of privacy policy documents for the same organizations over the course of four years. This study thus provides a unique perspective on the state of privacy practices in nine online healthcare organizations before and after HIPAA's enactment. We believe the results of this analysis may be helpful for forecasting how future legislation will affect the state of online privacy in other domains. Additionally, our findings suggest that law makers need to do a better job of considering how the introduction of law can benefit, or adversely affect, not only the ways in which sensitive information is handled but also how it affects the ways in which organizations choose to express these practices online. Moreover, the United States needs additional non-domain-specific legislation that broadly regulates online privacy and which protects the consumer rather than institutions.

**Acknowledgements**

The authors wish to thank Qingfeng He and William Stufflebeam for their assistance throughout this study and Hai Yuan for his comments on this paper.

**References**

[AEB04] A.I. Antón, J. B. Earp, D. Bolchini, Q. He, C. Jensen and W. Stufflebeam. "The Lack of Clarity in Financial Privacy Policies and the Need for Standardization," *IEEE Security & Privacy*, 2(2), pp. 36-45, March/April 2004.

[AER02] A.I. Antón, J.B. Earp and A. Reese, "Analyzing Web Site Privacy Requirements Using a Privacy Goal Taxonomy, 10th Anniversary IEEE Joint Requirements Engineering Conference (RE'02), Essen, Germany, pp. 605-612, 9-13 September 2002.

[AHB04] A.I. Antón, Q. He and D. Baumer. "Inside JetBlue's Privacy Policy Violations," To Appear: *IEEE Security & Privacy*, August/September 2004.

[AE04] A.I. Antón and J.B. Earp. "A Requirements Taxonomy to Reduce Web Site Privacy Vulnerabilities," To Appear: *Requirements Engineering Journal*, Springer-Verlag, 2004.

[BEP00] D. Baumer, J.B. Earp and F.C. Payton. Privacy of Medical Records: IT Implications of HIPAA. *ACM Computers and Society*, 30(4), pp.40-47, December 2000.

[Fle49] R. Flesch, *The Art of Readable Writing*, Macmillan Publishing, 1949.

[Fox03] S . Fox, "Internet Health Resources," Pew Internet and American Life Project, July 2003, Washington D.C.

[GHS00] J. Goldman, Z. Hudson and R.M. Smith. Privacy Report on the Privacy Policies and Practices of Health Web Sites, Sponsored by the California Health care Foundation, Jan. 2000.

[Gno04] "Usability and Readability Considerations For Technical Documentation," http://developer.gnome.org/ documents/usability/usability-readability.html. Accessed June 2004.

[HHS03] United States Department of Health and Human Services. http://www.hhs.gov/news/facts/privacy.html. Posted April 2003. Accessed May 2004.

[NTI02] National Telecommunications and Information Administration. A Nation Online: How Americans Are Expanding Their Use of the Internet http://www.ntia.doc.gov/ntiahome/dn/ Washington, D.C. February 2002.

| | Policy Document | Protection Goals | | Vulner-abilities | | Un-classified | | Total Goals | | FRES | | FGL | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pre / Post HIPAA | | Pre | Post | Pre | Post | Pre | Post | Pre | Post | Pre | Post | Pre | Post |
| **Health Insurance** | | | | | | | | | | | | | |
| AETNA | Privacy Policy | 5 | | 5 | | | | 10 | | 42.8 | | 13.4 | |
| | Web Privacy Stmt | | 8 | | 12 | | 1 | | 21 | | 39.8 | | 13.8 |
| | Legal Statement | | 0 | | 9 | | | 0 | 9 | | 28.4 | | 18.0 |
| | Health | | 16 | | 34 | | | 0 | 50 | | 28.7 | | 14.8 |
| | Student | | 17 | | 36 | | | 0 | 53 | | 39.8 | | 13.6 |
| | Long Term | | 4 | | 29 | | | 0 | 33 | | 34.5 | | 10.2 |
| | Large Pension Case | | 6 | | 12 | | 1 | 0 | 19 | | 28.7 | | 14.8 |
| | Life Disability | | 15 | | 28 | | | 0 | 43 | | 35.1 | | 10..6 |
| | **Subtotal** | 5 | 66 | 5 | 160 | 0 | 2 | 10 | 228 | 42.8 | 33.6 | 13.4 | 14.2 |
| AFLAC | Privacy Policy | 1 | | 1 | | | | 2 | 0 | 30.4 | | 15.0 | |
| | Conditions | | 9 | | 22 | | | 0 | 31 | | 32.3 | | 14.7 |
| | Web Site Priv. Notice | | 14 | | 31 | | 2 | 0 | 47 | | 35.1 | | 13.7 |
| | **Subtotal** | 1 | 23 | 1 | 53 | 0 | 2 | 2 | 78 | 30.4 | 33.7 | 15.0 | 14.2 |
| CIGNA | Notices of Priv. Practices | 6 | 18 | 5 | 13 | | | 11 | 31 | 43.9 | 43.6 | 10.9 | 11.4 |
| | Legal Disclaimers | | 0 | | 7 | | | 0 | 7 | | 27.8 | | 16.6 |
| | **Subtotal** | 6 | 18 | 5 | 20 | 0 | 0 | 11 | 38 | 43.9 | 35.7 | 10.9 | 14.0 |
| **Online Drugstores** | | | | | | | | | | | | | |
| DestinationRX | Privacy Policy | 16 | 21 | 18 | 19 | | 2 | 34 | 42 | 40.0 | 39.0 | 12.9 | 13.9 |
| | Terms of Use | | 7 | | 13 | | 3 | 0 | 23 | | 31.8 | | 15.5 |
| | **Subtotal** | 16 | 28 | 18 | 32 | 0 | 5 | 34 | 65 | 40.0 | 35.4 | 12.9 | 14.7 |
| Drugstore.com | Privacy Policy | 15 | 21 | 14 | 38 | | | 29 | 59 | 39.1 | 40.9 | 13.6 | 13.7 |
| | Terms of Use | | 8 | | 22 | | 3 | 0 | 33 | | 35.8 | | 15.1 |
| | **Subtotal** | 15 | 29 | 14 | 60 | 0 | 3 | 29 | 92 | 39.1 | 38.4 | 13.6 | 14.4 |
| HealthCentral | Privacy Policy | 13 | 13 | 12 | 14 | | | 25 | 27 | 39.5 | 41.0 | 12.5 | 13.0 |
| | Terms of Use | | 6 | | 18 | | | 0 | 24 | | 24.9 | | 16.3 |
| | **Subtotal** | 13 | 19 | 12 | 32 | 0 | 0 | 25 | 51 | 39.5 | 33.0 | 12.5 | 14.7 |
| **Pharmaceuticals** | | | | | | | | | | | | | |
| Glaxo | Privacy Policy | 5 | | 7 | | | | 12 | | 39.5 | | 12.5 | |
| | Internet Priv. Stmt. | | 10 | | 6 | | 2 | | 18 | | 41.9 | | 12.7 |
| | Legal Notices | | | | 5 | | | 0 | 5 | | 28.8 | | 16.0 |
| | **Subtotal** | 5 | 10 | 7 | 11 | 0 | 2 | 12 | 23 | 39.5 | 35.4 | 12.5 | 14.4 |
| Novartis | Privacy Policy | 18 | 24 | 5 | 9 | | 4 | 23 | 37 | 27.4 | 41.4 | 16.7 | 13.1 |
| | Legal Disclaimer | | 3 | | 12 | | | 0 | 15 | | 27.4 | | 16.7 |
| | **Subtotal** | 18 | 27 | 5 | 21 | 0 | 4 | 23 | 52 | | 34.4 | 16.7 | 14.9 |
| Pfizer | Privacy Policy | 4 | 7 | 3 | 6 | | | 7 | 13 | 41.8 | 41.4 | 11.8 | 11.8 |
| | Terms of Use | | | | 10 | | | 0 | 10 | | 37.8 | | 12.9 |
| | **Subtotal** | 4 | 7 | 3 | 16 | 0 | 0 | 7 | 23 | 41.8 | | 11.8 | 12.4 |
| **Totals** | | **83** | **227** | **70** | **405** | **0** | **18** | **153** | **650** | | | | |
| **Averages** | | | | | | | | | | **39.6** | **34.9** | **13.3** | **14.2** |

**Table 2:** Pre-HIPAA vs. Post-HIPAA Analysis of Privacy Policies: Goal Classification and Flesch Readability. Grey cells indicate cases in which there was no Pre-HIPAA data because the documents were introduced Post-HIPAA or cases in which the Pre-HIPAA documents were replaced with newly-titled documents. Blank cells indicate null data.

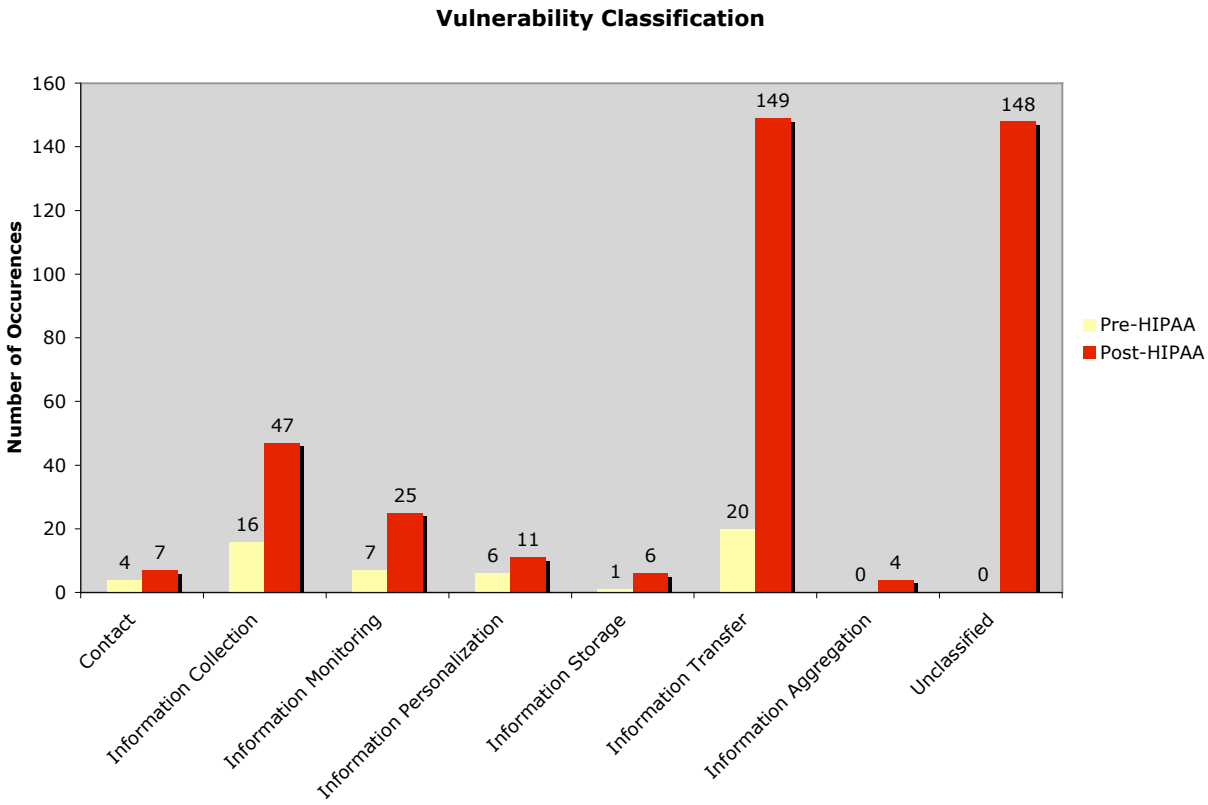


**Figure 1.** Comparison of the number of privacy vulnerabilities identified in privacy policy documents pre-HIPAA and post-HIPAA.

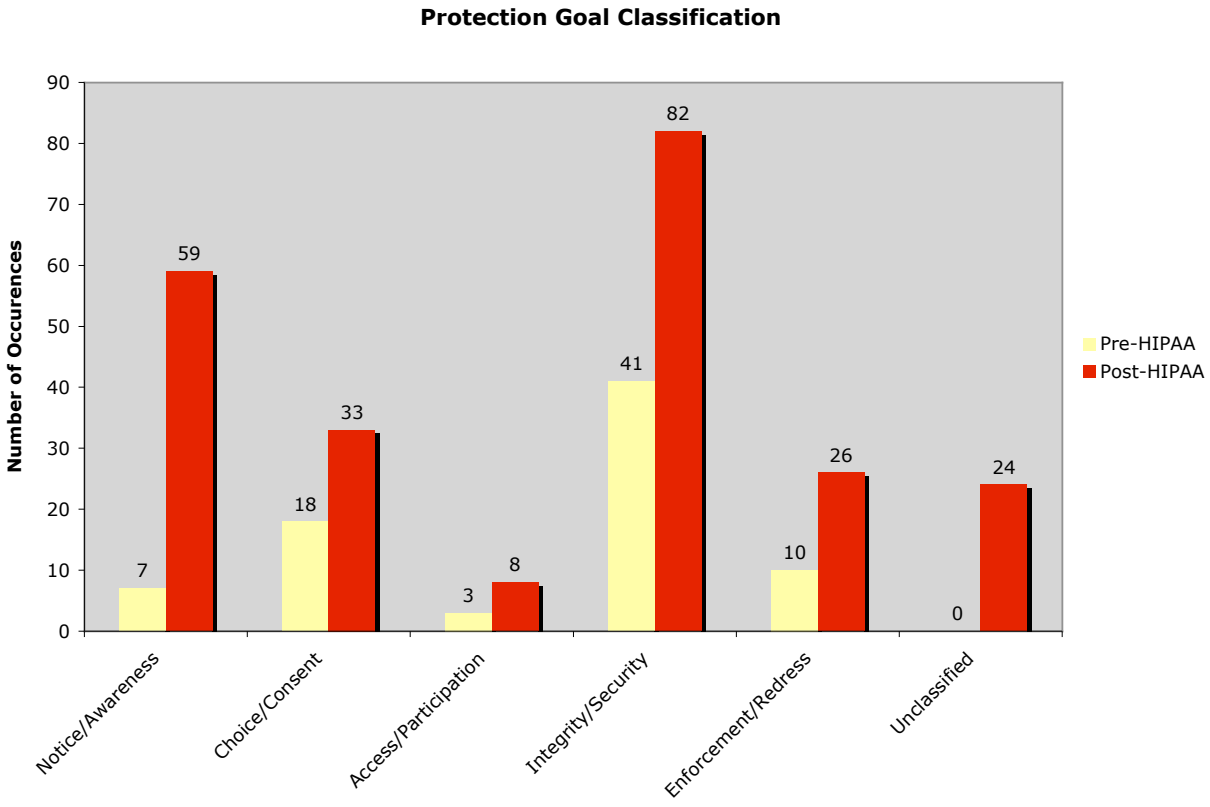


**Figure 2.** Comparison of the number of privacy protection goals identified in privacy policy documents pre-HIPAA and post-HIPAA.