ReedSmith

# MEMORANDUM

**Anthony E. DiResta**
Direct Phone: +1 202 414 9488
Email: adiresta@reedsmith.com

**Gina M. Cavalier**
Direct Phone: +1 202 414 9288
Email: GCavalier@reedsmith.com

Reed Smith LLP
1301 K Street, N.W.
Suite 1100 - East Tower
Washington, D.C. 20005-3373
+1 202 414 9200
Fax +1 202 414 9299
www.reedsmith.com

**Privileged & Confidential**[1]

**By Certified Mail**

**From:** Mark S. Melodia
Anthony E. DiResta
Gina M. Cavalier
Paul Bond
Andrew R. Boortz

**To:** Alain Sheer - Federal Trade Commission
Jerome Meites - Department of Health and Human Services

**Copy:** Loretta Garrison - Federal Trade Commission
Kristen Cohen - Federal Trade Commission
Christine Egan - CVS/Caremark Corporation

**Date:** April 7, 2008

**Subject:** **CVS Pharmacy, Inc.: Nonpublic Inquiry**

As you are aware, CVS Pharmacy, Inc. ("CVS") has been fully cooperating with a non-public inquiry into its compliance with specified laws and regulations in connection with the disposal of consumer information from June 1, 2005 to the present (for purposes of this document, the "relevant

---

1 This memorandum, the letters dated November 13, 2007, February 1, 2008, March 17, 2008, March 24, 2008, March 26, 2008, and April 3, 2008, and any other communications relating to this inquiry, as well as all documents accompanying or related to those communications, are intended to be highly confidential. The information contained in those letters, documents, or communications constitute sensitive and proprietary business information of CVS. All such materials are intended only for review by the staffs of the Federal Trade Commission and the Department of Health and Human Services. Accordingly, we request that they receive the highest level of protection for confidentiality available under the Commission's Rules of Practice, *e.g.*, 16 C.F.R. § 4.10, the Freedom of Information Act, *e.g.*, 5 U.S.C. § 552(b)(3)(B); 15 U.S.C. § 57b-2(f), the Federal Trade Commission Act, *e.g.*, 15 U.S.C. §§ 46(f); 57b-2, and any other applicable statutes, regulations, and rules.

period"). This inquiry has been jointly undertaken by the Federal Trade Commission ("FTC") and the United States Department of Health and Human Services ("HHS"), Office for Civil Rights ("OCR"). CVS submits that it has complied with all relevant laws and regulations promulgated by the FTC and OCR (collectively, "the Agencies"), and that the inquiry therefore should be closed.

CVS's Blue Bag Program, with its multi-million dollar annual costs and logistical challenges, has been a success. On a few occasions, the media has "discovered" and publicized unauthorized disclosures. In almost all instances, the reporters themselves caused and were the only audience to these disclosures. Unless identified, contacted, and singled out by these reporters, no CVS customers have complained that their information has been improperly disclosed because of CVS's PHI disposal policies.

Over the relevant period, CVS has always taken as its standard the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[12] the HIPAA regulation "Privacy of Individually Identifiable Health Information," ("Privacy Rule"),[13] and published OCR guidance on the same. In four iterations of the Privacy Rule over the course of more than three years, including more than 600 pages of explanatory preamble, OCR has never enumerated required disposal

---

12 Pub. L. 104-99 (1996).

13 45 C.F.R. §164.500 *et seq.*

methods.[14] Even with the benefit of hindsight and this intensive inquiry, CVS sees nothing in the history or current reality of its Blue Bag Program which fails to comply with HIPAA and/or the Privacy Rule, as explained by the OCR.

The FTC has promulgated a rule implementing a section of the Fair and Accurate Credit Transactions Act of 2003 entitled, "Disposal of Consumer Report Information and Records," ("FTC Disposal Rule").[15] The FTC Disposal Rule mandates, in disposal, "Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing *consumer information* so that the information cannot practicably be read or reconstructed."[16] However, "consumer information," as defined by the Disposal Rule, only includes information that "is a consumer report or is derived from a consumer report."[17] The Disposal Rule borrows its definition of "consumer report" from the Fair Credit Reporting Act ("FCRA").[18]

Therefore, the FTC Disposal Rule has no application whatsoever to this inquiry, which concerns pharmacy waste. No CVS document at issue constitutes a "consumer report." The PHI does not bear on the consumer's creditworthiness or any other factor enumerated by the FCRA.[19] The PHI was not collected for the purpose of determining the consumer's eligibility for credit,

---

14 See 64 Fed. Reg. 59,918 (Nov. 1999); 65 Fed. Reg. 82,462 (Dec. 2000); 67 Fed. Reg. 14,776 (Mar. 2002); 67 Fed. Reg. 53,182 (Aug. 2002).

15 16 C.F.R. Part 682.

16 16 C.F.R. §682.3(b)(1)(emphasis added).

17 16 C.F.R. §682.1(b).

18 See 16 C.F.R. §682.1(a); cf. 15 U.S.C.A. §1681 *et seq.*

19 15 U.S.C.A. §1681a(d)(1).

insurance, or employment.[20] And the PHI relates solely to transactions and experiences between the consumer and CVS.[21]

Indeed, the FTC has never suggested, in any of its rulemaking, statements, or enforcement actions, that it considers the regulation of PHI disposal within its bailiwick. To the contrary, in major addresses surveying the state of privacy law, both former Chairman Deborah Platt Majoras and Associate Director Joel Winston have suggested to Congress that HIPAA is one of the "federal laws not enforced by the Commission."[22]

Thus, CVS cannot be faulted for not establishing a company-wide shredding program. OCR, which enforces the HIPAA Privacy Rule, has jurisdiction over the disposal of PHI. It has never articulated nor suggested such a mandatory "must shred" disposal regime. While the FTC has imposed such a rule as to consumer reports, it has never suggested that rule would extend to pharmacy waste.

In the future, the OCR may well consider promulgating its own version of the disposal rule for pharmacy waste. Such a hypothetical "OCR Disposal Rule" might mandate a particular method or set of methods for disposal of PHI. Of course, any possible "OCR Disposal Rule" would first be subject to all of the safeguards inherent in rulemaking, including a notice and comment period,

---

20 Id.

21 15 U.S.C.A. §1681a(d)(2)(A)(i).

22 Deborah Platt Majoras, Chairman of the Federal Trade Commission, Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information, a prepared statement before the U.S. Senate, Committee on Banking, Housing, and Urban Affairs (Mar. 10, 2005), available at http://www.ftc.gov/os/testimony/050310idtheft.pdf. Accord, Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, Statement of Joel Winston, a prepared statement before the U.S. House of Representatives, Subcommittee on Social Security of the House Committee on Ways and Means (Mar. 30, 2006) available at:
http://waysandmeans.house.gov/hearings.asp?formmode=printfriendly&id=4790

inquiry into cost and benefit, and the possibility of Congressional rejection. CVS hopes that as one byproduct of this inquiry, OCR will have an appreciation of the nuts-and-bolts, practical difficulties encountered by covered entities in the conscientious disposal of pharmacy waste.

In summary, all documents and information submitted by CVS during the course of this inquiry demonstrate that CVS has complied with all presently-existing and applicable law and regulations. Accordingly, CVS submits that no further action is warranted, and that this inquiry should be closed.

## III. Argument

### A. No Further Action against CVS is Warranted under HIPAA's Privacy Rule.

The OCR enforces HIPAA's Privacy Rule.[82] OCR's stated approach to compliance is "cooperation". Indeed, before bringing any enforcement action, OCR must, "to the extent

82 45 C.F.R. §160.300 *et seq.*

practicable, seek the cooperation of covered entities in obtaining compliance[.]"[83] For example, OCR "may provide technical assistance to covered entities to help them comply voluntarily[.]"[84] To date, OCR has not provided CVS with any advice on achieving compliance, nor with any technical assistance.

The Privacy Rule requires that a covered entity, such as CVS, "must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of health information."[85] Further, a covered entity must "reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart."[86]

Unlike the FTC Disposal Rule, the Privacy Rule does not enumerate any concrete, specific safeguards a covered entity must employ with respect to disposal of PHI. For example, there is no requirement in the Privacy Rule that PHI be shredded before disposal, nor that waste containing PHI be stored inside a building, nor that dumpsters be locked in a certain way, nor that personnel attend a specific class dedicated solely to the disposal of PHI.

OCR has provided extensive educational and training materials ("Educational Materials") with respect to the Privacy Rule.[87] OCR has stated that these Educational Materials constitute

---

83 45 C.F.R. §160.304(a).

84 45 C.F.R. §160.304(b); accord, 45 C.F.R. §160.312 (requiring that when a compliance review indicates non-compliance, OCR "will attempt to reach a resolution of the matter satisfactory to [OCR] by informal means").

85 45 C.F.R. §164.530(c)(1).

86 45 C.F.R. §164.530(c)(2)(ii).

87 Office of Civil Rights, Medical Privacy – National Standards to Protect the Privacy of Personal Health Information: Educational Materials, at http://www.hhs.gov/ocr/hipaa/assist.html (all sites last visited Apr. 1, 2008)(hereafter, collectively, "Educational Materials").

reliable guidance as to how the Privacy Rule operates.[88] At the same time, OCR has cautioned covered entities against Privacy Rule explanations offered by third parties, such as vendors trying to sell a product. "In fact, HHS and OCR do not endorse any private consultants' or education providers' seminars, materials or systems, and do not certify any persons or products as 'HIPAA compliant.' The Privacy Rule does not require attendance at any specific seminars."[89]

Nowhere in the Educational Materials is there any list of specific administrative, technical, and/or physical safeguards that a covered entity is compelled to adopt with respect to disposal of PHI. Rather, the Educational Materials uniformly suggest that:

- covered entities are free to adopt any reasonable safeguards adapted to the covered entity's specific circumstances;
- reasonable safeguards may still result in some level of unintentional disclosure; and
- where modification to safeguards is needed, OCR will work with the covered entity if at all practicable.

The Educational Materials include a PowerPoint presentation from a 2003 OCR presentation at HHS's National Conference on the HIPAA Privacy Rule. The presentation describes the Privacy Rule as "flexible and scalable, workable, balanced."[90] The presentation has an "Administrative Requirements" section which lists no specific recommendations as to the disposal of PHI.[91] A

---

88 Office of Civil Rights, What You Should Know About OCR HIPAA: Be Aware of Misleading Marketing Claims, at http://www.hhs.gov/ocr/hipaa/misleadingmarketing.html.

89 Id.

90 Office of Civil Rights, HIPAA Privacy Rule, 2003 National Conferences, at http://www.hhs.gov/ocr/hipaa/conference/intro.pdf (page 8).

91 Office of Civil Rights, HIPAA Privacy Rule, 2003 National Conferences, at http://www.hhs.gov/ocr/hipaa/conference/adminreq.pdf.

review of this presentation suggests no reason a shredding program should be considered superior to the current Blue Bag Program.

Moreover, the section of this 2003 presentation marked "Compliance and Enforcement of the Privacy Rule" states again that OCR "with respect to the Privacy Rule" is committed to "promote voluntary compliance[.]"[92] The presentation poses the question, "Why Voluntary Compliance?", and answers that voluntary compliance is "Promoted by HIPAA Statute and Privacy Rule," which can consist of "Education, Cooperation, and Technical Assistance," and is "Permitted even after investigation commences," to seek the "most efficient way to promote privacy."[93] CVS agrees. CVS has sought and continues to seek attainment of voluntary compliance.

The Educational Materials also include an "OCR Privacy Brief" which serves as a "Summary of the HIPAA Privacy Rule."[94] Here, the OCR notes that "the flexibility and scalability of the [Privacy] Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources."[95] As to data safeguards, the OCR Privacy Brief only notes that such safeguards "*might* include shredding documents containing health information before discarding them"[96]

The Educational Materials include Frequently Asked Questions ("FAQ") and answers. In one such question, the provider asks, "Does the HIPAA Privacy Rule require hospitals and doctors'

---

92 Office of Civil Rights, HIPAA Privacy Rule, 2003 National Conferences, at http://www.hhs.gov/ocr/hipaa/conference/compli.pdf at p. 3.

93 Id. at p. 4.

94 Office of Civil Rights, OCR Privacy Brief: Summary of the HIPAA Privacy Rule, at http://www.hhs.gov/ocr/privacysummary.pdf.

95 Id. at p. 16 (emphasis added).

96 Id. (emphasis added).

offices to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard?"[97] The OCR answered, "No."[98] After all, "The Privacy Rule does not require that all risk of protected health information disclosure be eliminated."[99] "In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the potential effects on patient care, and any administrative or financial burden to be incurred from implementing particular safeguards."[100] With respect to the specific question:

> The Department does not consider facility restructuring to be a requirement under this [reasonable safeguards] standard. For example, the Privacy Rule does not require the following types of structural or systems changes: Private rooms; Soundproofing of rooms; Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners; or Encryption of telephone systems.[101]

Such "real world," practical realizations are key for CVS. CVS has already done everything possible to alert employees to the Blue Bag Policy. The bags themselves stand out due to their coloring and signage. Moreover, instructions regarding the Blue Bag Policy are posted in numerous places around the pharmacy. As noted above, not all CVS locations have room for an on-site shredding program. Nor are most CVS stores configured to allow for a self-contained trash system that would avoid the use of an outside dumpster.

OCR advised that it would not violate the Privacy Rule for a clinic to leave a patient's records in a box outside that patient's room unattended.[102] OCR suggested some measures the clinic

---

97 Office of Civil Rights, F.A.Q. at http://www.hhs.gov/hipaafaq/administrative/197.html.

98 Id.

99 Id.

100 Id.

101 Id.

102 Office of Civil Rights, F.A.Q. at http://www.hhs.gov/hipaafaq/administrative/201.html.

might take to mitigate the risk that an unauthorized person would steal those records. However, OCR further advised that "Each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances."[103]

Finally, the Educational Materials include a document entitled "OCR Guidance Explaining Significant Aspects of the Privacy Rule."[104] Under the title, "How the Rule Works," the guidance explains reasonable safeguards. "It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from any and all risks. Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business."[105] CVS's Blue Bag Program is appropriate to CVS's national, retail pharmacy environment, and constitutes reasonable safeguards.

### B. The FTC Act Does Not Have the Jurisdictional Authority to Address Issues Concerning the Disposal of PHI.

According to the September 27, 2007, letter to Tina Egan, the FTC staff seeks "to determine whether CVS's handling of sensitive information from or about consumers in connection with the preparation and sale of prescription medicines and supplies raises any issues under Section 5."[106] CVS respectfully submits that the issues presented by this inquiry are not within the jurisdictional scope of the FTC and are not designed to be addressed under the FTC Act. See FTC Operating Manual 3.3.7.4.1 (investigations should be closed "[a]s soon as it becomes apparent during an

---

103 Id. (emphasis added)

104 Office of Civil Rights, OCR Guidance Explaining Significant Aspects of the Privacy Rule, at http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf.

105 Id. at p. 5 (emphasis added).

106 (Letter at 1-2.)

investigation that no violation of the laws or regulations enforced by the Commission has occurred.") (emphasis added); see also, id. at 3.3.7.4.3(1) (closing warranted when there is insufficient evidence of jurisdiction).

While the jurisdictional grant provided by Congress to the Federal Trade Commission is broad, designed to address "unfair or deceptive acts or practices in or affecting commerce,"[107] this grant of power to the Commission is not unlimited. Where Congress has invested another body with specific authority over a subject matter, the FTC's broad mandate must often yield. Thus, these are times when the FTC must defer to another agency with primary jurisdiction.[108] Accordingly, when the FTC seeks to infringe on another agency's area of competence, it will be judicially rebuffed.[109]

These principles are clearly demonstrated when, like here, issues of medical privacy are contemplated. Simply put, the FTC should not act as a regulator of medical privacy. Former Chairman Majoras told Congress a few years ago that HIPAA and its Privacy Rule are not enforced by the Commission.[110] So did Associate Director Joel Winston about two years ago.[111]

---

107 15 U.S.C. § 45(a)(1).

108 See, e.g., "Memorandum of Understanding between Federal Trade Commission and Food and Drug Administration," 36 Fed. Reg. 18539 (September 16, 1971)(agreeing that, as to labeling of food and drug products, the FDA had primary jurisdiction).

109 See, e.g., Florida East Coast Ry. Co. v. U.S., 259 F.Supp. 993 (M.D. Fla. 1966), aff'd, 386 U.S. 544 (1967).

110 Deborah Platt Majoras, Chairman of the Federal Trade Commission, Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information, a prepared statement before the U.S. Senate, Committee on Banking, Housing, and Urban Affairs (Mar. 10, 2005), available at http://www.ftc.gov/os/testimony/050310idtheft.pdf.

111 Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, Statement of Joel Winston, a prepared statement before the U.S. House of Representatives, Subcommittee on Social Security of the House Committee on Ways and Means (Mar. 30, 2006) available at: http://waysandmeans.house.gov/hearings.asp?formmode=printfriendly&id=4790.

"The express provision of one method of enforcing [a statute] suggests Congress intended to preclude others."[112] "HIPAA limits enforcement of the statute to the Secretary of Health and Human Services."[113] That Congress expressly authorized OCR to enforce HIPAA's Privacy Rule strongly suggests that Congress did not intend HIPAA's Privacy Rule to be enforced by the FTC.

It is noteworthy that the FTC has not issued any regulations pertaining to disposal of PHI. The FTC issued a 28-page brochure entitled, "Protecting Personal Information: A Guide for Business," which does mention HIPAA, the Privacy Rule, or PHI.[114] OCR's guidance on OCR's Privacy Rule is not even mentioned in the Additional Resources section of the FTC pamphlet.[115]

The incongruity of FTC action in the medical privacy context has already been noted in the secondary literature. "[A]ny FTC action with regard to privacy for consumer health information would raise difficult issues of coordination, as the HIPAA privacy standards are already being implemented by the Department of Health and Human Services."[116]

CVS has fully cooperated in this joint FTC and OCR inquiry. However, a regulated entity like CVS is entitled to one consistent set of regulations and explicit guidance from one regulator so designated by Congress. The FTC should, accordingly, defer to HHS, which is the agency with direct statutory authority over this issue.

---

112 Alexander v. Sandoval, 532 U.S. 275, 286-87 (2001).

113 Acara v. Banks, 470 F.3d 569 (5th Cir. 2006)(finding no private consumer right of action exists for HIPAA violations).

114 Federal Trade Commission, Protecting Personal Information: A Guide for Businesses, available at http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf.

115 Id. at p. 29.

116 Privacy and the World Wide Web," George B. Delta and Jeffrey H. Matsuura, Law of the Internet §6.03 (Aspen Publishers, Inc. 2008).

### C. Even if the FTC Has Jurisdiction over the Disposal of PHI, CVS's Conduct Has Not Violated, and Does Not Violate, the FTC Act.

As noted in Appendix I, the FTC has brought multiple actions alleging that various data protection practices were unfair and/or that various data protection claims were deceptive. However, the nature of the conduct - - and the consequences that resulted from such conduct - - that forms the basis of such FTC jurisprudence are fundamentally distinguishable from the conduct and attendant consequences at issue in this inquiry. As former Chairman Majoras has noted, "No one need worry that the FTC is looking for 'perfect' security, or that we are developing a de facto strict liability standard for when a breach occurs, because the cases we have brought have not been close calls."[117]

The FTC Act does not permit prosecution for unfair acts "unless the act or practice causes or is likely to cause substantial injury to consumers[.]"[118] Accordingly, in almost every case where the FTC has taken action, there had been thousands or millions of consumers put in jeopardy of identity theft or unauthorized account access.[119] In this case, there are no criminal intruders or would-be identity thieves. The information at issue cannot easily be used for identity theft or unauthorized account access. In other words, no "injury," no "harm," or no "damage" can concretely be identified that is directly caused by CVS.

---

117 Deborah Platt Majoras, Chairman of the Federal Trade Commission, The FTC: Confronting New Security Challenges Through Enforcement, Education, and Research, remarks to the Exchequer Club (Sept. 20, 2006), available at: http://www.ftc.gov/speeches/majoras/060920exchequerclub.pdf.

118 15 U.S.C.A. §45(n).

119 See, e.g., In the Matter of DSW Inc., FTC File No. 052 3096 (arising from intruders stealing information on 1.4 million payment cards); see also In the Matter of CardSystems Solutions, Inc., FTC File No. 052 3148 (arising from intruders stealing information on millions of payment cards, committing millions of dollars in fraud).

Furthermore, many FTC actions arise from companies failing to avail themselves of obvious technical solutions. When a company refuses to do the bare minimum in protection, it could be argued that such a company has "a knowledge fairly implied on the basis of objective circumstances that such act is unfair[.]"[120] For example, many of the Consent Orders relate to situations where credit card information was stored in "clear text," i.e., unencrypted form, in clear violation of numerous prior warnings and industry best practices.[121] CVS has not been presented with any obvious, technical solution, or even a clearly superior and reasonable alternative to its already strengthened Blue Bag Program.

For obvious reasons, the FTC has pursued companies who derived income from privacy violations.[122] The incidents that gave rise to this inquiry were not motivated by income considerations; rather, these incidents have cost CVS millions in consumer goodwill, remedial compliance, and legal fees. They were not offset by any gains whatsoever.

The FTC has also pressed enforcement where a company promised something specific and failed to deliver.[123] CVS's privacy policies did not promise any specific measures on which CVS failed to deliver.

---

120 15 U.S.C.A. §45(m)(1)(A)(listing the requirements for a cease and desist order).

121 See, e.g., In the Matter of Guess?, Inc., and Guess.com, Inc., FTC File No. 022 3260, In the Matter of Petco Animal Supplies, Inc., FTC File No. 032 3221, In the Matter of Guidance Software, Inc., FTC File No. 062 3057.

122 See, e.g., In the Matter of ChoicePoint Inc., FTC File No. 052-3069 (arising from sale of subscriptions to consumer reporting agency database without adequate identity verification); In the Matter of Gateway Learning Corp., FTC File No. 042-3047 (arising from renting of consumer information in violation of privacy policy); In the Matter of Vision I Properties, LLC, FTC File No. 042 3068 (same).

123 See, e.g., In the Matter of ValueClick, Inc., et al., FTC File Nos. 072-3111 and 072-3158 (arising from a situation in which the company promised to encrypt payment card information, but instead merely replaced each digit with another).

In all of the FTC actions so far, only two have dealt with physical disposal of consumer information.[124] However, both of these cases fell squarely within the FTC's jurisdiction under the Gramm-Leach-Blilely Act ("GLBA").[125] As non-banking financial institutions, American United Mortgage and Nations Title fell under the Commission's Standards for Safeguarding Consumer Information Rule ("FTC Safeguards Rule"),[126] and Privacy of Customer Financial Information Rule ("FTC Privacy Rule").[127] Because later in time, American United was also subject to the FTC Disposal Rule.

CVS is not a financial institution, and is not subject to the FTC Safeguards Rule, the FTC Privacy Rule, nor the FTC Disposal Rule. None of these rules, and none of this guidance, applies to CVS and the disposal of medical waste. Accordingly, closing this inquiry is warranted. See Operating Manual 3.3.7.4.3(5), (7) (reasons for closing include insufficient evidence of violations and proceedings by another government agency).

CVS certainly acknowledges and applauds the prudent FTC leadership on data security issues. As always, CVS will continue to draw its understanding of best practices from all secondary sources available, giving thoughtful consideration to FTC rules and guidance. CVS also shares with the FTC and OCR the aspiration of privacy perfection. But as the leadership of both agencies has assured the public and the business community, perfection is not the legal standard. Developing reasonable safeguards is in part a process of determining what is practical in each specific

---

124 See, In the Matter of American United Mortgage Company, FTC File No.: 062 3103 and In the Matter of Nations Title Agency, Inc., FTC File No. 052 3117.

125 15 U.S.C.A. § 6801 et seq.

126 16 C.F.R. Part 314.

127 16 C.F.R. Part 313.

commercial environment, which necessarily is an ongoing process in which CVS welcomes all the help that can be offered.

## IV. Conclusion

For years, CVS has had in place a policy for protecting the disposal of PHI that was applicable to all of its employees. The Program and its revisions – which included the evaluation of options to determine the most appropriate approach to ensure confidentiality -- were adopted at great expense. There were constant reminders and reinforcements of the Program. Notwithstanding news reports that revealed vulnerabilities in the recognition of the "no dumpster policy" at several CVS locations, there is no evidence of consumer injury that can be directly attributed to these violations. In other words, no conduct has been identified that adversely impacts consumer welfare.

Perfection is not the standard. Reasonableness is. As the OCR has instructed, reasonableness varies according to the covered entity at issue, and depends upon several factors including the size of the entity and the nature of its business. A survey done about six weeks ago reported that almost all stores were using blue bags to line pharmacy trash receptacles.

Accordingly, CVS has complied with all applicable laws, regulations, and guidance. It has engaged in reasonable precautions and has reasonable safeguards in place to address the disposal of PHI. While CVS certainly looks forward to receiving additional technical advice, CVS respectfully requests that this joint inquiry be closed.