Medical Privacy Policies of Large U.S. Companies Have Major Deficiencies

Prepared for Rep. Henry A. Waxman
Ranking Minority Member

Minority Staff
Special Investigations Division
Committee on Government Reform
U.S. House of Representatives

April 6, 2000

Table of Contents

Executive Summary

I. Background 1

A. Growing Public Concerns about Medical Privacy 1

B. Contours of Sound Medical Privacy Policies 2

C. Objective of the Report 4

II. Methodology 5

III. Survey Responses 7

A. Overview 7

B. Privacy Protections in Company Policies and Contracts 8

C. Employee Rights Regarding their Own Health Records 11

D. Use or Disclosure of Employee Health Information for Employment Decisions, Marketing Activities, or Insurance Underwriting Purposes 12

E. Examples of Quality Policies 13

IV. Conclusion 14

V. Exhibits 16

EXECUTIVE SUMMARY

This report assesses the policies of major U.S. companies for protecting the privacy of employee health records. It finds that while most major U.S. companies state that they safeguard the privacy of employee health records, their policies frequently contain major deficiencies. The majority of the companies surveyed lack written policies that set forth basic privacy protections regarding employee health records, and lack written policies that provide employees with basic rights with respect to their own health records. In addition, many companies refused to state that they will not use or disclose employee health records for employment decisions, marketing activities, or insurance underwriting.

The U.S. Department of Health and Human Services, members of Congress, and independent experts have recently released proposals for protecting the privacy of medical records. These proposals describe a core set of policies for handling medical records. These include policies that:

- prohibit use or disclosure of health information without an individual's authorization unless for specified, limited purposes;
- require that use and disclosure of health information be limited to the minimum amount necessary;
- give individuals the right to review, copy, and request amendment of their own medical records; and
- establish an enforcement scheme to address failures to comply with medical privacy policies.

This report evaluates whether these recommended policies are being implemented in top Fortune 500 companies. It is based on a survey of the 48 largest Fortune 500 companies that provide "self-insured" health plans for their employees. Self-insured plans are those in which the employer assumes the risk for the health services provided to its employees and pays for claims directly from its income or assets. It is estimated that 43.4 million people in this country participate in self-insured private sector health plans.

Many of the companies surveyed stated that they take some steps to protect medical privacy. Some companies said that they allow only a limited number of individuals in their benefits departments access to employee health records. Further, a number of companies said that access to employee health records by individuals within the company occurs only for legitimate business or legal purposes, such as an appeal of a claims decision, on a "need-to-know" basis. The majority of the companies that responded said that they do not handle the processing of employee health claims, but rather contract with third party administrators to do this task and maintain the relevant records. Many of these companies said that they require the third parties that process the claims to maintain safeguards and precautions to ensure the confidentiality of employee medical records.

Most of the companies, however, failed to provide written documentation of their policies. With respect to those companies that did provide documentation, the written policies

often lacked critical details. For example, of the 48 companies surveyed, only 14 provided policies stating that disclosure or use of employee health information without an individual's authorization will be limited to specified purposes, and only four provided policies limiting use and disclosure of health information to the minimum amount necessary.

Most of the companies also fail to inform employees of their medical privacy practices, and virtually no companies have policies that give employees a right to review or amend their medical records. Of the 48 companies surveyed, only 21 said they provide employees with either a notice of their rights and protections relating to health records or a notice of employer information practices with respect to those records, and only 15 provided any documentation of such notice. Only one company provided a policy that gives employees the right to review and amend their own medical records.

Further, while many companies stated generally that they would take appropriate disciplinary action to address inappropriate disclosures of employee health records, only six provided documentation of company policies that set forth such a penalty scheme.

All the companies surveyed were asked specifically whether they would use or disclose employee health records for employment decisions, marketing activities, or insurance underwriting purposes. Many companies declined to state that they would not use employee health records for those purposes.

While most of the companies appeared to have substantial deficiencies in their policies for protecting medical privacy, a few companies stood out because of positive aspects of their privacy policies. Electronic Data Systems (EDS), which processes its own employees' health claims, provided documentation of company policies that include a number of essential components. Daimler-Chrysler and IBM, which contract with third parties to process employee health claims, also provided documentation of company policies that include essential privacy components.

The results of the survey do not mean that the companies surveyed have misused the medical records of their employees. However, the survey does indicate that many major companies in the United States that self-insure do not have adequate medical privacy policies in place. This failure creates conditions under which misuse of employee health records could occur.

I. BACKGROUND

A. Growing Public Concerns about Medical Privacy

With increasing computerization of medical records and integration of activities within the health care system, individuals' health information can be transmitted more rapidly to a wider range of recipients. Currently, however, there is no comprehensive federal law that ensures adequate privacy protections for medical records. Instead, a patchwork of state laws address medical privacy matters, and many provide only minimal protections.

As a result, many individuals are concerned about the confidentiality of their health records. According to a 1999 survey conducted by the California HealthCare Foundation, over half of all American adults believe that computerization of medical records increases privacy threats. Further, concerns about medical privacy invasions have led one out of every seven Americans to take steps such as withholding information from their physicians and even avoiding care altogether.[1]

The lack of essential legal protections leaves employees uncertain as to whether their employers will be able to access their medical records and make judgments or employment decisions based on the information in the records.[2] Press accounts of such situations underscore that employees have insufficient confidentiality assurances regarding employer access to their health information. For example, in one case recently in the news, a 30-year FBI veteran was put on administrative leave and his gun was taken away after pharmacy records released without his permission had been obtained by his employer. According to news reports, these records "showed, correctly, that he had sought treatment for depression. But they also showed, incorrectly, that he was taking multiple antidepressants." The agent, who had been respected for work on drug and organized crime activity, spent a year trying to regain his employer's trust and then retired.[3]

In some cases, an employee whose health records have been inappropriately accessed by an employer may be able to seek redress in court based on constitutional invasion of privacy claims, state invasion of privacy tort claims, or contract claims if the contract contains

---

[1]California HealthCare Foundation, *National Survey: Confidentiality of Medical Records* (Jan. 1999).

[2]Federal law prohibits employers from discriminating against employees on the basis of disability. 42 U.S.C. §12112 (known as the "Americans with Disabilities Act"). However, not every health condition is considered a "disability" under this law, and it can be difficult for an employee to prove that an employer based a particular employment decision on the individual's health condition as opposed to other factors.

[3]*Records No Longer for Doctors' Eyes Only,* Los Angeles Times (Sept. 1, 1998).

confidentiality restrictions and the employee is a party to the contract. Often, however, it can be difficult to succeed on such claims. For example, in one recent case, a court upheld the actions of an employer who reviewed records about the drugs individual employees were taking and conducted research to determine whether employees that were taking drugs used in AIDS treatment were HIV-positive.[4] Such decisions further reinforce the fears of employees that their health records lack adequate protections.

B. Contours of Sound Medical Privacy Policies

Recognizing growing public concerns, Congress in 1996 passed the Health Insurance Portability and Accountability Act (HIPAA). This law established an August 21, 1999, deadline under which Congress was to act to enact legislation providing privacy protections for medical records. HIPAA further provided that if Congress failed to act by the August 21, 1999, deadline, the Secretary of the U.S. Department of Health and Human Services (HHS) must issue regulations to protect medical privacy.

Several bills were introduced last year in Congress to protect medical records. The bill with the most cosponsors in the U.S. House of Representatives is the Health Information Privacy Act (H.R. 1941), which was introduced by Reps. Gary A. Condit, Henry A. Waxman, Edward J. Markey, and John D. Dingell. This legislation would provide comprehensive privacy protections for medical records by implementing the recommendations of HHS and other privacy experts. To date, however, no comprehensive medical privacy legislation has passed either House of Congress.[5]

---

[4]*Doe v. Southeastern Pennsylvania Transportation Authority*, 72 F. 3d 1133 (3rd Cir. 1995). Although this case involved claims based on the constitutional right to privacy, many courts also set standards for state privacy tort claims that are difficult for plaintiffs to surmount. For example, one common type of privacy tort claim relating to medical information disclosures is the tort called "publication of private facts." Courts in a number of jurisdictions hold that to prove the "publication" element of this tort, a plaintiff must demonstrate that private facts at issue were disclosed to a wide audience. Therefore, in these jurisdictions, disclosure of an employee's medical information to co-workers, even if the disclosure causes deep embarrassment and has a significant harmful impact on the plaintiff's life, would not constitute actionable conduct. *E.g., Stein v. Davidson,* 1996 Tenn. App. LEXIS 280 (Tenn. App. 1996) (employer's disclosure of employee's drug test results to two of the employee's peers was not actionable because disclosure was not to sufficient number of people); *Eddy v. Brown,* 715 P.2d 74 (Okla. 1986) (employer's disclosure to several co-workers of fact that employee was undergoing psychiatric treatment was not basis for a claim because disclosure was not to the general public).

[5]Congress considered including medical records provisions in the financial services modernization bill that was enacted into law last year, and medical records language was included in the House version of the bill (H.R. 10). The House-passed language, however, would have allowed an individual's medical information to be disclosed or sold without the consent of

As a result of Congress' failure to act, the Administration has proposed regulations as required by HIPAA to protect the privacy of medical records.[6] These proposed regulations govern the use of individually identifiable health information transmitted or maintained in electronic form, defined as "protected health information." They apply to health care providers and health insurers, including self-insured plans employers provide for their employees.

The proposed regulations include two general privacy rules. First, they prohibit use and disclosure of protected health information without individual authorization except in specified circumstances including treatment, payment, and health care operations, and for limited other purposes such as health research and law enforcement. Second, the proposed regulations provide that entities handling health records must limit the use and disclosure of protected health information to the minimum amount necessary.[7] These two ground rules create clear requirements that use and disclosure of individually identifiable health information will be limited and tailored to legitimate purposes.

In addition, the proposed regulations specify minimum rights that all individuals should have regarding their health records. These include the right of individuals to review, copy, and request amendment of their own health records, to obtain a history of disclosures of their health information, and to receive notice of their privacy rights. To help ensure enforcement of these privacy rules, the proposed regulations set forth penalties for privacy violations.

Other privacy experts have made recommendations that track the major principles in HHS's proposed regulations. For example, the Health Privacy Working Group, a broad coalition comprised of disability and mental health advocates, health plans, providers, employers, and experts in public health, endorsed many policies similar to those in the Administration's proposed regulations.[8] Similarly, the Consumer Coalition for Health Privacy, which represents

---

the individual, and was widely criticized by doctors, nurses, patient organizations, and privacy advocates. *See, e.g., House Approves Disclosure of Private Medical Records,* Los Angeles Times (July 2, 1999).

[6]*See Standards for Privacy of Individually Identifiable Health Information: Proposed Rule*, Fed. Reg. Vol. 64, 59918-60065 (Nov. 3, 1999).

[7]For example, the "minimum necessary" restriction helps ensure that an employer seeking to lower health care costs would not review employee health records to identify employees who are HIV-positive where non-identifiable data would be sufficient to conduct such cost control.

[8]For example, the Health Privacy Working Group recommended a general rule limiting disclosures of individually identifiable information without patient authorization to specific circumstances and a principle encouraging the use of non-identifiable information to the fullest extent possible. The group also recommended establishing individual rights of record access and supplementation, as well the right to notice, and penalties for privacy violations. Health Privacy

consumer, disability, and patient advocates, also recommends many policies similar to those in HHS's proposed regulations.[9] Together, HHS's proposed regulations and the recommendations of privacy experts provide the contours for sound medical privacy policies.

C. Objective of the Report

The goal of this report is to assess whether major U.S. employers have adopted privacy policies that comply with the goals of HHS's proposed regulations and the recommendations of privacy experts. In the absence of federal regulations or law, many employers currently have wide discretion in establishing medical privacy policies, especially in states with relatively weak state laws. This report evaluates whether these employers are voluntarily implementing sound privacy policies.

In particular, the report focuses on large Fortune 500 companies that provide self-insured health plans to their employees.[10] The structure of such plans provides opportunities for employer access to employee health information that raise privacy issues. Under self-insured plans, employers may be directly responsible for administering employee health claims, thereby having access to personal health information about employees.[11] In addition, even when a company contracts with a third party to administer employee health claims in a self-insured plan and the employee health records are not physically located on company premises, representatives of the company may request the third party to provide the company with information on individual health records so that the company can administer claims appeals, or conduct auditing

---

Working Group, *Best Principles for Health Privacy*, Health Privacy Project, Georgetown University (July 1999).

[9]*See* Consumer Coalition for Health Privacy, *Statement of Mission and Principles,* (March 22, 1999) (available at www.healthprivacy.org). While the recommendations of the Coalition have many elements in common with HHS's proposed regulations, the proposals differ on some points. For example, the Consumer Coalition recommends patient authorization be required for disclosures of health information for treatment, payment, and health care operations. The Coalition also recommends that individuals have a private right of action to seek redress for privacy violations, a remedy HHS states it did not have authority to provide.

[10]In contrast to self-insured plans, insured plans are those in which the employer pays a premium to purchase health insurance for employees from insurers that assume the risk for the health services.

[11]*E.g.,* National Journal, *Open Secrets,* at 2880 (Oct. 9, 1999) (quoting the chairman of the University of Massachusetts Medical School psychiatry department as saying, "It's Helen in personnel who's looking at all the forms, and knows whether you're seeing a psychiatrist, you just had your tubes tied, or you've just been diagnosed with cancer").

or other activities.[12] An estimated 43.4 million people in this country participate in self-insured private sector health plans.[13]

This report did not inquire about every component of a sound medical privacy policy. It did, however, ask companies about many of the most important components, such as whether they have adopted restrictions on the use and disclosure of individually identifiable health information without authorization; an enforcement scheme to address privacy violations; and policies that provide rights to individuals to access, copy, and amend their own health records.[14] This report is the first recent survey of medical privacy policies of large U.S. companies with self-insured health benefits plans.[15]

II. METHODOLOGY

On June 3, 1999, Rep. Henry A. Waxman, the ranking member of the House Committee on Government Reform, sent a survey to the 50 largest U.S. companies that offer fully or partially self-insured health plans to their employees. All of the companies surveyed were part of the Fortune 500. In fact, the smallest company surveyed was the 90th largest U.S. company according to *Fortune Magazine*.[16] Information on whether the company offers a self-insured health plan was obtained from the Department of Labor. The survey is attached as exhibit A, and

---

[12]*See id.*

[13]Employee Benefit Research Institute, *Employment-Based Health Care Benefits and Self-Funded Employment-Based Plans: An Overview*, 6 (Sept. 1998) (available at www.ebri.org/facts/1098fact.pdf).

[14]Other elements of a sound medical privacy policy that privacy experts have cited include technical practices and procedures to safeguard health records; the use of an objective and balanced process to review the disclosure of health information for health research purposes; and a rule prohibiting disclosure of health information to law enforcement officials without compulsory legal process such as a warrant. *See, e.g., Best Principles for Health Privacy, supra* note 8, at 4-7.

[15]In 1996, Professor David Linowes of the University of Illinois at Urbana-Champagne completed a survey of Fortune 500 companies that focused broadly on privacy practices relating to information the companies collect and maintain about employees. With respect to medical records, this survey found that 35% of the companies that responded said they use medical records in making employment decisions, among other findings. David F. Linowes, *A Research Survey of Privacy in the Workplace* (April 1996) (available at www.staff.uiuc.edu/~dlinowes/survey.htm).

[16]The list was derived from the annual survey of top companies by *Fortune Magazine* (April 1998).

the companies that received the survey are listed in exhibit B.

The survey included questions regarding (1) how companies ensure privacy protection for employee health records; (2) whether employees have essential rights with respect to their health information, such as the right to access, copy, and amend their records, as well as the right to notice about their rights and the information practices of the company; and (3) whether the company uses employee health information for employment decisions, marketing activities, or insurance underwriting. The survey also asked companies to discuss any additional privacy protections they provide regarding employee health information.

In addition, the survey asked for documentation of company policies that establish medical privacy protections and employee rights relating to health information. The survey sought this documentation because the existence of a written company policy demonstrates a company's commitment to the principles contained in the policy. Moreover, a written company policy provides clear and consistent rules to those employed by the company regarding acceptable conduct.

Two of the 50 companies surveyed informed Rep. Waxman that they do not currently provide self-insured plans for their employees, and therefore they are not considered in this report. With respect to the remaining 48 companies, the minority staff contacted each company at least once following the initial letter. Mr. Waxman also sent a second letter to virtually all of the companies that informed them of Mr. Waxman's plans to prepare a report analyzing the survey results.[17] These letters made clear that the report would include a discussion of whether companies surveyed were able to document privacy policies or contractual provisions with third parties that handle employee health information. In the case of companies that failed to provide documentation of privacy policies in response to the June 3, 1999, letter, Mr. Waxman's second letter stated:

> Based on your response to date to my June 3 letter, your company would be identified in my report as unable to provide documentation of either a written company policy in place that prohibits officers and employees from accessing or disclosing the health information of another employee or a specific contractual provision with any third party administrators that prohibits access by officers and employees of your company to employee health information maintained by the third party.
>
> If your company has such a written policy or contractual provision that you would like to

---

[17]A second letter was not sent to two of the 48 companies because, shortly before the second letters were sent, the minority staff discussed the content of the letter in phone conversations with representatives of the companies.

bring to my attention, please let me know by October 29, 1999.[18]

In total, companies had almost five months to provide Mr. Waxman with information relating to the survey questions. Thirty-seven of the 48 companies responded to at least some of the survey requests.

III. SURVEY RESPONSES

The information that companies provided in response to the survey indicates that the majority of major Fortune 500 companies have inadequate policies for protecting employee health information. The majority of the companies surveyed lack written policies containing essential privacy protections, and lack written policies ensuring employee rights to access, copy, and amend their health records. Further, many companies refused to state that they do not use employee health records for employment decisions, marketing activities, or insurance underwriting.

A. Overview

In total, 37 of the 48 companies responded to some or all of the questions in the survey. Many companies stated that they had in place policies or practices that protect the confidentiality of their employees' health information. Of the 48 companies surveyed, however, over half -- 28 companies -- did not provide documentation of either an existing written company policy or existing contractual provisions with third parties that administer their health plans concerning privacy protections or rights. Only 15 companies provided documentation of written company policies that address privacy protections for employee health information.[19]

The overwhelming majority of companies that responded -- 33 of 37 -- said that third party administrators process their employees' health claims. Many of these companies stated that they require the contractors to maintain appropriate safeguards to protect the confidentiality of employee health information, and that confidentiality contract provisions with third party administrators are in place. Of the 33 companies that stated they contract with third parties, however, only 12 provided documentation of confidentiality provisions in their contracts.

Eleven companies declined to respond to any of the survey questions. These eleven

---

[18]The letters also made clear that redaction of trade secrets or other proprietary information would be acceptable.

[19]The majority of the policies provided by companies in response to the survey did not address medical records specifically, but rather addressed personnel information generally. A few of these policies explicitly stated that employee health records are considered personnel information. This report considered documentation of a general company privacy policy concerning personnel information to be documentation of a policy on employee health records.

companies are:

American International Group
Caterpillar, Inc.
Chevron Corp.
Home Depot, Inc.
International Paper Company
Mobil Corp.
Morgan Stanley Dean Witter & Co.
Motorola
PepsiCo., Inc.
Proctor & Gamble Co.
Wal-Mart

B. Privacy Protections in Company Policies and Contracts

As discussed above in part I.B, HHS and other privacy experts have concluded that sound medical privacy policies include the following protections: (1) a prohibition on use or disclosure of individually identifiable health information without the individual's authorization except in limited, specified circumstances; (2) a requirement that use and disclosure of individually identifiable health information be limited to the minimum amount necessary; and (3) penalties for violations of privacy policies. The majority of companies surveyed failed to provide written documentation that they have these essential privacy protections in place.

Only 14 companies (29%) provided written policies that prohibit use or disclosure of employee health information without employee authorization except in limited circumstances. Moreover, many of these 14 policies stated that use or disclosure was permitted for "business purposes," a vague term that could be used to authorize a wide variety of disclosures. In addition, several of the policies only address disclosures outside of the company but not uses within the company. Only a few policies set forth permitted uses and disclosures with more specificity. For example, one policy provided that uses of personal employee information must be for "one or more specified purposes (and not for vague, undefined purposes)," such as when the particular use is required by employment law or for a legal claim. This policy also required that the purposes for which the data is used must be known to the data subject.[20]

Only four companies (8%) provided written policies that contain any sort of requirement limiting use and disclosure of identifiable employee health information to the minimum extent necessary to accomplish legitimate purposes. Although this requirement is considered a cornerstone of a sound privacy policy by privacy experts, the vast majority of companies have no

---

[20] *Outline of EDS Global Data Protection Policy: Personal Data Handling Requirements* (July 1999) (enclosure to letter from John D. Lacopo, Corporate Vice President, Office of Government Affairs, EDS, to Rep. Henry A. Waxman (Nov. 18, 1999)) (attached as exhibit I).

such policies. One example of a policy that did include this requirement stated that, where feasible the company should "use aggregate data" and access to medical information should be "narrowly tailored in terms of scope and detail to achieve intended business purposes."[21]

Further, only six companies (13%) provided written policies that state that penalties will be enforced against individuals that violate the companies' privacy policies.

A number of companies said that because they contract with third parties to process employee health claims and these third parties maintain the health records, questions about privacy restrictions regarding employee health information do not apply to the companies. These responses, however, often did not address whether the company could access employee health information maintained by third party contractors or whether the company restricts use and disclosure of this information upon access. Only eight companies (17%) provided contract provisions with third parties that place restrictions on company access to employee health information. Moreover, even if a company does not directly handle health records, its failure to insist on contractual privacy provisions with its third party administrators means that it has no assurance that appropriate privacy practices will be followed.

In a number of cases, companies that failed to provide documentation of their policies or contractual provisions with third parties nonetheless described in their responses policies and practices that appear to provide privacy protections for their employees' health information. For example, Johnson & Johnson stated that it does not maintain employee health records, nor does it access or review employee health data on an individual basis that is maintained by third party administrators.[22] Similarly, J.C. Penney said that employee health information is maintained by third parties and "is not accessible to any Company officer or employee."[23]

In other cases, however, company responses left wide leeway for companies to access employee health information. These responses stated broadly that companies may access the information for business purposes or by individuals with a "need to know." For example, AT&T's response stated:

> AT&T collects, retains, and discloses personally identifiable employee information only when required for valid business, legal, or regulatory reasons. Access to AT&T's records

---

[21]Letter from Daimler-Chrysler Corporation to International Union, UAW (Sept. 1999) (enclosure to letter from Donald L. Longnecker, Director, Strategic Planning and Healthcare Initiatives, Daimler-Chrysler, to Rep. Henry A. Waxman (Oct. 19, 1999)) (attached as exhibit J).

[22]Letter from Efrem B. Dlugacz, Vice President, WorldWide Benefits and Health Resources, to Rep. Henry A. Waxman (Sept. 13, 1999) (attached as exhibit G).

[23]Letter from Kathy Rattenbury, Benefits Development Project Manager, to Rep. Henry A. Waxman (July 6, 1999) (attached as exhibit H).

containing personally identifiable employee information is limited to authorized persons with a need to know (e.g. payroll, benefit, EO/AA representatives). Additionally, AT&T requires its insurance vendors to take all necessary safeguards and precautions to ensure confidentiality of employee information.[24]

Similarly, BellSouth's response stated that access to employee health information is limited to "company representatives who have a need to know," and cited a nonexclusive list of examples such as "company attorneys in regard to litigation, auditors reviewing the proper administration of the plan by carriers, administrators handling appeals, etc." The response further stated that "[d]isclosure of another employee's health information is not allowed unless it [is] appropriate and proper in regard to specific duties being performed by the employee or officer on behalf of the company."[25] Safeway's response said that the company's policy is "to limit access to an employee's personnel file to managers or staff who have a legitimate business need to access the information."[26]

Responses like those given by AT&T, BellSouth, and Safeway provide limited protection to employees. They allow disclosure for "valid business" reasons, which are undefined terms that could encompass a wide range of uses of employee health information. They also appear to place no limits on the amount of employee health information that may be accessed by company officials.

· Regardless of what the responses of companies said, the failure of the majority of companies to provide documentation of their privacy policies is a significant deficiency. Written privacy policies have substantial benefits. They provide employees with notice of their privacy rights, establish clear guidelines to employees regarding the limitations on access to and disclosures of other employees' health information, and demonstrate a company's commitment to the principles set forth.

---

[24]Letter from Susan C. Meholic, Division Manager, Health & Welfare Plan Administration, to Rep. Henry A. Waxman (Nov. 29, 1999) (attached as exhibit C).

[25]Letter from Justin Jordan, Director Benefit Planning, to Rep. Henry A. Waxman (June 25, 1999) (attached as exhibit D).

[26]Letter from Linda Watt, Vice President, Human Resources, to Rep. Henry A. Waxman (June 23, 1999) (attached as exhibit E). It is unclear from Safeway's response the extent to which employees have access to other employees' health information. Safeway's response noted that Safeway no longer processes health care benefit claims in-house and that this has "largely eliminated the need for Safeway to gather or maintain the information that employees must provide in order to receive or pay for health care benefits."

C. Employee Rights Regarding their Own Health Records

As discussed in part II.B, HHS and other medical privacy experts have concluded that individuals should have basic rights that enable them to have appropriate control over their own medical records, including the right to access, copy, and amend their own medical records. Further, the experts have recommended that individuals should receive notice from their health plan regarding their privacy rights.

Only one company (2%), however, provided a written policy that provides employees with essential rights concerning their health records relating to their benefits plan.[27] This policy provides that employees may access and amend their own data relating to the employer's self-insured health plan but does not specifically provide the right to copy records.[28] Four companies provided written policies that state that, with respect to health records maintained by the companies themselves, employees have rights of access, amendment, and (in the case of two of these companies) copying. None of those four policies, however, address whether employees have a right to access, copy, or amend health records maintained by the third parties with whom the company contracts to process health claims.

Only 21 companies (44%) said that they provide employees with notice of the protections and rights that apply to employee health information or company practices regarding employee health information. Only 15 companies (31%) provided written documentation of such notice.

Many examples of the types of notice provided were very general and brief. Four companies stated that the summary of the health plan that is required to be provided to employees under current federal employment law constituted such notice.[29] Others stated that general

---

[27]Some companies noted that employees have the rights of access to their records provided under an existing federal law known as the Employee Retirement Income Security Program (ERISA). Under ERISA, an employee has a right to review documents pertinent to an appeal of a denied benefits claim. 29 C.F.R. §2560.503-1(g). This ERISA right of access is significantly more limited than the access rights that privacy experts recommend individuals have with respect to their own health records. Therefore, this report does not consider compliance with existing ERISA requirements on records access as equivalent to having a policy on access that meets the standards recommended by privacy experts.

[28]*Outline of EDS Global Data Protection Policy: Personal Data Handling Requirements, supra* note 20.

[29]The federal law that establishes this requirement, and the Department of Labor's implementing regulations, however, do not specify that the summary plan must address an employee's privacy rights or the privacy protections that apply to the employee's health information, or describe all purposes for which the employer uses and discloses the information. *See* 29 U.S.C. §1022; 29 C.F.R. §2520.102-3.

confidentiality policies in company codes of conduct provided such notice as they are distributed to all employees. Further, a number of companies that responded to the survey stated that they do not believe that questions relating to notice to employees apply to them because they contract with third parties to handle employee health information relating to their self-funded plans.

D. Use or Disclosure of Employee Health Information for Employment Decisions, Marketing Activities, or Insurance Underwriting Purposes

The survey included three questions regarding specific potential uses and disclosures of employee health information: (1) Does the company use or disclose employee health information for the purpose of making employment decisions?; (2) Does the company use or disclose employee health information for marketing activities?; and (3) Does the company use or disclose employee health information for the purpose of conducting insurance underwriting? Many companies failed to state that they do not use or disclose employee health information for employment decisions, marketing activities, or insurance underwriting.

Only 13 companies stated explicitly that they do not use or disclose employee health information for employment decisions. In addition, five companies stated that they use or disclose such information in limited circumstances to make accommodations for job-related physical requirements or restrictions, or to determine eligibility for medical leaves of absence. Combining these two types of responses, only 18 (38%) responded that they do not use or disclose employee health information for employment decisions.[30]

Only 20 companies (42%) stated explicitly that they do not use or disclose employee health information for marketing activities.

Fifteen companies responded that they do not use or disclose employee health information for insurance underwriting. In addition, four companies stated there was a general prohibition on using or disclosing employee health information for insurance underwriting purposes, except in the aggregate or in de-identified form. Combining these two types of responses, only 19 companies (40%) responded that they do not use or disclose employee health information for insurance underwriting.[31]

---

[30]Two additional companies responded that they do not use employee health information for hiring decisions, but did not address whether they use the information for other types of employment decisions, such as promotion, demotion, or firing.

[31]Four additional companies stated in phone conversations with minority staff that their companies did not use employee health information for employment decisions, marketing activities, or insurance underwriting. They declined, however, to include this information in their written responses to the survey. Because oral representations in phone conversations do not establish binding corporate policies, this report does not include these four companies in the total number of companies that responded that they do not use or disclose employee health information for employment decisions, marketing activities, or insurance underwriting. Even if

Some companies did not directly respond to the questions on whether they use or disclose employee health information for employment decisions, marketing activities, or insurance underwriting, but described or provided policies that would appear to preclude such uses and disclosures. For example, Sprint stated in its letter response that it does not maintain any written or computerized records of employee health information. Further, Sprint said that it can request such information from a third party administrator "if requested by the employee to assist in a dispute," and that access to this information is then "limited to a small number of employee benefits professionals and attorneys within Sprint" on an "as needed basis" to resolve the claims dispute.[32] Thus, although Sprint did not directly respond to the questions on whether it uses or discloses employee health information for employment decisions, marketing activities, or insurance underwriting, its policy does not appear to contemplate such uses or disclosures.

This report does not, however, attempt to interpret whether each company's description or documentation of its policy or documentation precludes use or disclosure of employee health information. Companies could -- and many did -- respond directly to these questions, and the report credits those companies as having responded. With respect to those companies that did not respond expressly to these questions, in many cases it was not clear whether the language of a company's policy allowed or precluded use or disclosure of employee health information for employment decisions, marketing activities, and insurance underwriting. For example, as discussed in part III.B, AT&T's policy states that an AT&T discloses personally identifiable employee information for "valid business" reasons. It is not possible to determine from the face of this response whether AT&T would consider use or disclosure of employee health information for employment decisions, marketing activities, or insurance underwriting a "valid business" reason.

E. Examples of Quality Policies

Although the majority of companies surveyed failed to document existing company policies that reflect essential medical privacy principles, a few companies stood out as having existing privacy policies that contain crucial components. One of these companies was EDS, which self-administers employee health claims relating to its self-insured health benefits plan. EDS provided a written company policy concerning employee data, which includes health data. This policy restricts the use of employee data to specified purposes, contains minimum use restrictions, provides employees with the right to access and amend their own data, and states

---

these four companies were included, however, the findings of the report would not change substantially. Including the four companies that responded orally, only 46% of surveyed companies said they do not use or disclose employee health information for employment decisions, only 50% said they do not use or disclose such information for marketing activities, and only 48% said they do not use or disclose employee health information for insurance underwriting.

[32]Letter from J.E. Lewin, Jr., Vice President, to Rep. Henry A. Waxman (June 28, 1999) (attached as exhibit F).

that with respect to any company use of an employee's health data, the subject of the data must be informed about what data is being collected and by whom it is being used, and for what purposes it is being used, among other provisions.[33]

Daimler-Chrysler is another example of a company that has in place essential privacy policies. Daimler-Chrysler, which contracts with third parties to process employee health claims, provided a recent written agreement with the United Automobile Workers (UAW) that sets forth a number of privacy policies, including: access to employee medical information by the company and third party administrators will be narrowly tailored in scope and detail to achieve the intended business purpose, where appropriate and feasible; aggregate information will be used to the extent feasible; the company will establish internal safeguards regarding the exchange of employee medical information; and inappropriate exchange of medical information by employees will result in disciplinary action. This agreement also states that the company will "require third party administrators . . . to establish and enforce policies and procedures" consistent with the agreement.[34]

In addition, IBM, which also contracts with third parties to process employee health claims, provided documentation of a number of important privacy policies. IBM's policy provides that IBM will "only process Employee Information which is relevant to and necessary for the particular purposes" and requires that "consideration should be given (balanced against the effort involved) to aggregating or anonymizing Employee Information where there is no need to know individually identifiable Employee Information." IBM also provides that it will "instruct third parties processing Employee Information on behalf of IBM, if any, to implement appropriate measures to safeguard the Employee Information."[35]

IV. CONCLUSION

The survey results indicate that a few companies that provide self-insured health plans

---

[33]*Outline of EDS Global Data Protection Policy: Personal Data Handling Requirements, supra* note 20.

[34]Letter from Daimler-Chrysler to International Union, UAW, *supra* note 21.

[35]*IBM Guidelines For The Protection Of Employee Information* (enclosure to Letter from Harriet P. Pearson, Office of the Director of Public Affairs, to Rep. Henry A. Waxman (Oct. 29, 1999) (attached as exhibit K). While the three policies mentioned in this section contain numerous quality components, their inclusion in this section does not mean that each is without deficiencies. For example, Daimler-Chrysler's letter agreement with the United Automobile Workers contains a broad statement that access to medical information is "limited to persons having a need to use the information in the course of performing their job duties" but does not clearly define the "job duties" contemplated by the agreement. It is also worth noting that IBM's guidelines state explicitly that they are "not to be construed as a contract, either express or implied."

have taken substantial steps to protect the privacy of the health records of their employees. For example, some companies have established a written policy prohibiting the use or disclosure of employee health information except for specified purposes such as administration of the health plan. A few also have written policies containing "minimum necessary" requirements with respect to employee health information, or a penalty scheme for privacy violations. And a few companies provide employees with basic rights such as the right to access and amend their own records or notice of their privacy rights. These voluntary efforts underscore that sound privacy policies are practicable in the administration of employee health plans.

The survey results also indicate, however, that most employees that participate in their employers' self-insured health benefits plans do not have adequate assurances that their health records will be protected. The majority of companies surveyed failed to provide documentation of written company policies containing basic privacy protections, and many of the policies that were provided did not include key protections. The results also indicate that few employees are receiving sufficient information to understand how their employer handles and protects their health information and the extent of their rights with respect to their own health records. Finally, the results suggest that many employees cannot be confident that their employers will refrain from using or disclosing their health information for employment decisions, marketing activities, or insurance underwriting.

These results to do not mean that medical privacy abuses are occurring in the companies surveyed. They do indicate, however, that safeguards to prevent abuse are not in place.