



---

**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.<sup>1</sup>

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.<sup>2</sup> 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.<sup>3</sup>

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

---

<sup>1</sup>California HealthCare Foundation, *National Survey: Confidentiality of Medical Records* (Jan. 1999).

<sup>2</sup>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.

<sup>3</sup>*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.<sup>4</sup> 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.<sup>5</sup>

---

<sup>4</sup>*Doe v. Southeastern Pennsylvania Transportation Authority*, 72 F. 3d 1133 (3<sup>rd</sup> 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).

<sup>5</sup>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.<sup>6</sup> 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.<sup>7</sup> 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.<sup>8</sup> 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).

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

<sup>7</sup>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.

<sup>8</sup>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.<sup>9</sup> 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.<sup>10</sup> 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.<sup>11</sup> 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).

<sup>9</sup>See Consumer Coalition for Health Privacy, *Statement of Mission and Principles*, (March 22, 1999) (available at [www.healthprivacy.org](http://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.

<sup>10</sup>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.

<sup>11</sup>*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.<sup>12</sup> An estimated 43.4 million people in this country participate in self-insured private sector health plans.<sup>13</sup>

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.<sup>14</sup> This report is the first recent survey of medical privacy policies of large U.S. companies with self-insured health benefits plans.<sup>15</sup>

## 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 90<sup>th</sup> largest U.S. company according to *Fortune Magazine*.<sup>16</sup> 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

---

<sup>12</sup>*See id.*

<sup>13</sup>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](http://www.ebri.org/facts/1098fact.pdf)).

<sup>14</sup>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.

<sup>15</sup>In 1996, Professor David Linowes of the University of Illinois at Urbana-Champaign 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](http://www.staff.uiuc.edu/~dlinowes/survey.htm)).

<sup>16</sup>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.<sup>17</sup> 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

---

<sup>17</sup>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.<sup>18</sup>

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.<sup>19</sup>

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

---

<sup>18</sup>The letters also made clear that redaction of trade secrets or other proprietary information would be acceptable.

<sup>19</sup>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.<sup>20</sup>

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

---

<sup>20</sup>*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.”<sup>21</sup>

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.<sup>22</sup> Similarly, J.C. Penney said that employee health information is maintained by third parties and “is not accessible to any Company officer or employee.”<sup>23</sup>

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

---

<sup>21</sup>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).

<sup>22</sup>Letter from Efreem B. Dlugacz, Vice President, WorldWide Benefits and Health Resources, to Rep. Henry A. Waxman (Sept. 13, 1999) (attached as exhibit G).

<sup>23</sup>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.<sup>24</sup>

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."<sup>25</sup> 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."<sup>26</sup>

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.

---

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

<sup>25</sup>Letter from Justin Jordan, Director Benefit Planning, to Rep. Henry A. Waxman (June 25, 1999) (attached as exhibit D).

<sup>26</sup>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.<sup>27</sup> 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.<sup>28</sup> 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.<sup>29</sup> Others stated that general

---

<sup>27</sup>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.

<sup>28</sup>*Outline of EDS Global Data Protection Policy: Personal Data Handling Requirements*, *supra* note 20.

<sup>29</sup>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.<sup>30</sup>

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.<sup>31</sup>

---

<sup>30</sup>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.

<sup>31</sup>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.<sup>32</sup> 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.

<sup>32</sup>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.<sup>33</sup>

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.<sup>34</sup>

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."<sup>35</sup>

#### IV. CONCLUSION

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

---

<sup>33</sup>*Outline of EDS Global Data Protection Policy: Personal Data Handling Requirements, supra* note 20.

<sup>34</sup>Letter from Daimler-Chrysler to International Union, UAW, *supra* note 21.

<sup>35</sup>*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 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.

# **EXHIBITS**

# **EXHIBIT A**

STANCE A. MORELLA, MARYLAND  
STOPHER SHAYS, CONNECTICUT  
JA RQS-LEHTINEN, FLORIDA  
I M. McHUGH, NEW YORK  
HEN HORN, CALIFORNIA  
I L. MICA, FLORIDA  
AAS M. DAVIS III, VIRGINIA  
D M. MCINTOSH, INDIANA  
C E. SOUDER, INDIANA  
SCARBOROUGH, FLORIDA  
TEN C. LATOURETTE, OHIO  
SHALL "MARK" SANFORD, SOUTH CAROLINA  
BARR, GEORGIA  
MILLER, FLORIDA  
HUTCHINSON, ARKANSAS  
TERRY, NEBRASKA  
BIGGERT, ILLINOIS  
G WALDEN, OREGON  
G OSE, CALIFORNIA  
RYAN, WISCONSIN  
T T. DOOLITTLE, CALIFORNIA  
EN CHENOWETH, IDAHO

# Congress of the United States

## House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

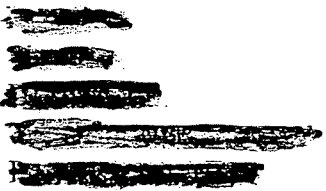
WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074  
MINORITY (202) 225-5051  
TTY (202) 225-6852

ROBERT E. WISE, JR., WEST VIRGINIA  
MAJOR F. OWENS, NEW YORK  
EDOLPHUS TOWNS, NEW YORK  
PAUL E. KANJORSKI, PENNSYLVANIA  
FATSY T. MINK, HAWAII  
CAROLYN E. MALONEY, NEW YORK  
ELEANOR HOLMES NORTON  
DISTRICT OF COLUMBIA  
CHAKA FATTAH, PENNSYLVANIA  
ELIJAH E. CUMMINGS, MARYLAND  
DENNIS J. KUCINICH, OHIO  
ROD P. BLAGOJEVICH, ILLINOIS  
DANNY K. DAVIS, ILLINOIS  
JOHN F. TIERNEY, MASSACHUSETTS  
JIM TURNER, TEXAS  
THOMAS H. ALLEN, MAINE  
HAROLD E. FORD, JR., TENNESSEE  
JANICE D. SCHAKOWSKY, ILLINOIS

BERNARD SANDERS, VERMONT,  
INDEPENDENT

June 3, 1999



Dear [Redacted] :

I am writing to seek information regarding the privacy protections your company provides the health information of employees.

I understand that your company offers a self-insured health plan or plans for its employees. As you know, self-insured plans are those in which the employer pays for the health care claims of employees directly out of the employer's income or assets, as opposed to plans in which the employer purchases health insurance coverage for employees by paying a premium to a health insurer that assumes the risk for health care services to the employees. In administering self-insured health care plans, including performing functions such as processing payment claims, employers often must obtain some health-related information from their employees.

I am interested in learning about your policy regarding the privacy of information that employees provide to receive or pay for health care under your self-insured plan or plans (hereafter "health information"). Specifically, I would appreciate your responding to the following requests for information:

1. Record keeping.

- (a) Does your company maintain any written or computerized records of employee health information?
- (b) If so, does your company keep such records separate from personnel files that are maintained on these same employees?
- (c) How is such separation accomplished?

2. Employee Access to Information. Please describe any restrictions the company places on access by an officer or employee of the company to the health information of other employees.

3. Penalties for Improperly Accessing Information.

(a) Please describe what, if any, penalties apply if an officer or employee of the company accesses health information in violation of access restrictions the company placed on that information.

(b) Please describe the process under which any such penalties are imposed.

4. Disclosure and Use of Information.

(a) Please describe any restrictions you place on disclosure by an employee or officer of the company of another employee's health information.

(b) Does the company use or disclose employee health information for the purpose of making employment decisions?

(1) If so, please describe those decisions.

(c) Does the company use or disclose employee health information for marketing activities?

(1) If so, please describe the marketing activities for which the company has used or disclosed employee health information.

(d) Does the company use or disclose employee health information for the purpose of conducting insurance underwriting?

(1) If so, please describe the insurance underwriting activities for which the company has used or disclosed employee health information.

5. Penalties for Improper Information Disclosure.

(a) Please describe what, if any, penalties apply if an officer or employee of the company discloses health information of another employee in violation of any disclosure restrictions that the company placed on that information.

(b) Please describe the process under which any such penalties are imposed.

6. Other Protections. Please describe any other ways in which the company protects the confidentiality of employee health information.

7. Record Review, Copying, and Correction. Please describe any rights the company provides employees regarding review, copying, or correction of records of their own health information that the company maintains as part of administering the plan or plans.

8. Disclosure History.

(a) Does the company maintain records of disclosures of health information that occur after an employee provides the information to receive or pay for health care under the plan or plans?

(b) If so, please describe any right the company provides its employees regarding reviewing any such disclosure histories that concern their own health information.

9. Notice of Protections and Rights.

(a) Does the company provide its employees with a description of the protections and rights that apply to employees' health information?

(b) If so, please describe when such a description is provided and in what form.

10. Notice of Information Practices.

(a) Does the company provide its employees with a description of how the company uses and discloses employee health information?

(b) If so, please describe the information contained in such a description, when such a description is provided, and in what form it is provided.

11. Opportunity to Limit Uses and Disclosures.

(a) Does the company provide its employees with an opportunity to request limitations on the use and disclosure of employee health information by the company?

(b) If so, please describe when and how the company provides such an opportunity.

12. Redress for Violations. Please describe any process available to employees for seeking redress for improper disclosure of the employee medical information or violation of the employee's rights with respect to that information.

13. Written Policies.

(a) Does the company have a written policy that addresses any of the following matters: 1) privacy protections relating to health information, 2) employee rights

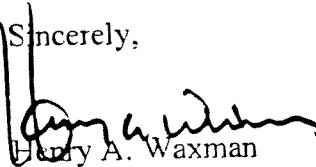


relating to health information, or 3) use and disclosure by the company of employee health information?

(b) If the answer to (a) is yes, please provide me with a copy of such policy or policies.

Please respond to these inquiries by June 25, 1999. Thank you very much for your attention to this matter. If you have any questions, please contact Kristin Amerling of my staff at (202) 225-5420.

Sincerely,



Henry A. Waxman  
Ranking Member

**EXHIBIT B**

## COMPANIES SURVEYED

American Express Company  
American International Group  
AMR Corporation  
Atlantic Richfield Co.  
AT&T Corporation  
Bell Atlantic Corp.  
BellSouth Corporation  
Caterpillar, Inc.  
Chase Manhattan Corp.  
Chevron Corporation  
CIGNA Corporation  
Compaq Computer Corp.  
ConAgra, Inc.  
Daimler-Chrysler  
Electronic Data Systems  
Federated Department Stores  
Fleming Companies, Inc.  
General Motors Corp.  
Hewlett-Packard  
Home Depot, Inc.  
Intel Corp.  
International Business Machines  
International Paper Co.  
J.C. Penney Company, Inc.  
Johnson & Johnson, Inc.  
J.P. Morgan & Co.  
Kmart Corp.  
Kroger Company  
Lehman Brothers  
Lockheed Martin Corp.  
MCI Worldcom, Inc.  
Merck & Co., Inc.  
Merrill Lynch & Co., Inc.  
Minnesota Mining & Manufacturing  
Mobil Corp.  
Morgan Stanley Dean Witter & Co.  
Motorola Corp.  
NationsBank Corp. (Bank of America)  
New York Life Insurance Company  
PepsiCo, Inc.  
Phillip Morris Companies

Phillips Petroleum Co.  
Procter & Gamble Co.  
Safeway, Inc.  
SBC Communications  
Sprint Corporation  
Supervalu, Inc.  
United Parcel Service  
Wal-Mart Stores  
Xerox Corporation

# **EXHIBIT C**



Susan C. Meholic  
Division Manager  
Health & Welfare Plan Administration

Room 603 East Tower  
One Speedwell Avenue  
Morristown, NJ 07962-1954  
973 898-2356  
FAX 973 898-2358  
EMAIL meholic@att.com

November 29, 1999

Mr. Henry A. Waxman  
Ranking Minority Member  
House of Representatives  
Committee on Government Reform  
2157 Rayburn House Office Building  
Washington, DC 20515-6143

**Re: Health Information Privacy**

Dear Representative Waxman:

This letter is in response to your 10/28/99 letter to C. Michael Armstrong requesting information on company policy for accessing employee health information.

AT&T maintains a culture and policies that respect the privacy of individual information, and safeguards sensitive, personally identifiable employee information. The importance of this is captured in the AT&T Code of Conduct and the Personal Guide. 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 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.

AT&T is reviewing the Health and Human Service Regulations for Protection of Individually Identifiable Health Information published November 3, 1999 in the Federal Register and will provide feedback, either directly or through participation in one of our industry groups, to HHS prior to the January 3, 2000 deadline.

Please feel free to contact me or Leanne Fosbre of my staff at 973-898-2915 with any question.

Sincerely,

A handwritten signature in black ink that reads "Susan C. Meholic".

**EXHIBIT D**

BellSouth Corporation  
Room 13C09  
1155 Peachtree Street, N.E.  
Atlanta, Georgia 30309-3610

Benefits

June 25, 1999

The Honorable Henry A. Waxman  
Ranking Member Congress of the United States  
House of Representatives  
2157 Rayburn House Office Building  
Washington, D. C. 20515-6143

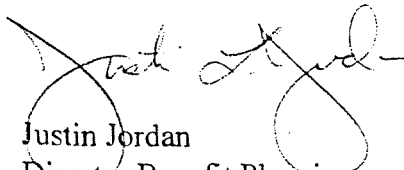
Dear Congressman Waxman:

In a letter dated June 3, 1999, you asked Duane Ackerman, President and Chief Executive Officer, BellSouth Corporation, to provide you with information about the company's policy on employee privacy of health information. Mr. Ackerman asked me to respond to your request since BellSouth's health and welfare program falls under my responsibilities as BellSouth's director of benefit planning.

BellSouth is committed to protecting the privacy rights of employees as it relates to personal information about their health care. We believe that employees must have security that personal information gathered through medical history and other plan resources is confidential and that access to their data is limited. Otherwise, employees won't feel comfortable using the health plans offered by the company.

Attached you will find a summary of responses to your questions. Please contact me if you have any questions or if you need additional information related to the privacy of employee health information.

Sincerely,



Justin Jordan  
Director Benefit Planning

Attachment



BellSouth's response to your questions is as follows:

1. Record keeping.

(a) Does your company maintain any written or computerized records of employee health information?

**Response:** BellSouth does not maintain records of employee health information. Rather, such records are maintained by third party administrators who are responsible for the adjudication and processing of health related claims under BellSouth's medical plans. While BellSouth does not physically maintain this information, we consider it BellSouth property.

(b) If so, does your company keep such records separate from personnel files that are maintained on these same employees?

**Response:** Yes, please see 1 (a) response.

(c) How is such separation accomplished?

**Response:** Please see 1 (a)

2. Employee Access to Information. Please describe any restrictions the company places on access by an officer or employee of the company to the health information of other employees.

**Response:** BellSouth limits access to employee health information to company representatives who have a need to know. Examples: company attorneys in regard to litigation, auditors reviewing the proper administration of the plan by carriers, administrators handling appeals, etc.

3. Penalties for Improperly Accessing Information.

(a) Please describe what, if any, penalties apply if an officer or employee of the company accesses health information in violation of access restrictions the company placed on the information.

**Response:** Disciplinary action up to and including dismissal may be taken.

(b) Please describe the process under which any such penalties are imposed.

**Response:** Once reported or discovered, the company would conduct an investigation. Any violation of policy would be reported to the employee's Department Head, Legal and Human Resources to determine the appropriate disciplinary action to be taken.

4. Disclosure and Use of Information.

(a) Please describe any restriction you place on disclosure by an employee or officer of the company of another employee's health information.

**Response:** Disclosure of another employee's health information is not allowed unless it appropriate and proper in regard to specific duties being performed by the employee or officer on behalf of the company. Please see the response to question 2.

(b) Does the company use or disclose employee health information for purpose of making employment decisions?

**Response:** Yes

(1) If so, please describe those decisions.

**Response:** If restrictions are placed on an employee by the employee's physician as a result of an illness or an injury that affect the employee's ability to perform his/her job, consideration would be given to the employee's medical condition in attempting to determine whether the employee can be accommodated in his/her current job or in a another open position.

(c) Does the company use or disclose employee health information for marketing activities?

**Response:** No

(d) Does the company use or disclose employee health information for the purpose of conducting insurance underwriting?

**Response:** No

5. Penalties for Improper Information Disclosure.

(a) Please describe what, if any, penalties apply if an officer or employee of the company discloses health information of another employee in violation of any disclosure restrictions that the company placed on that information.

**Response:** Disciplinary action up to and including dismissal may be taken.

(b) Please describe the process under which any such penalties are imposed.

**Response:** Please see 3 (b) response.

6. Other Protections. Please describe any other ways in which the company protects the confidentiality of employee health information.

**Response:** The company has established and enforces policies that prohibit the unauthorized use or disclosure of employee health information.

7. Record Review, Copying and Correction. Please describe any rights the company provides employees regarding review, copying or correction of records of their own health information that the company maintains as part of administering the plan or plans.

**Response:** Health information other than restrictions placed by a physician (see 4, (b) 1 response) is not maintained by the company. Employees may request access to health information in accordance with the procedures provided under the Employee Retirement Income Security Act of 1974.

8. Disclosure History.

(a) Does the company maintain records of disclosures of health information that occur after an employee provides the information to receive or pay for health care under the plan or plans?

**Response:** With respect to disclosures made to authorized BellSouth representatives, no records are maintained. A record would be maintained when disclosures are made (see response to question 2) to third parties, e.g., pursuant to an authorization signed by the employee, in compliance with a subpoena, or pursuant to a discovery request during litigation.

(b) If so, please describe any right the company provides its employees regarding reviewing any such disclosure histories that concern their own health information.

**Response:** The information would only be disclosed outside the company as result of a written release by the employee or if legally required in connection with litigation.

9. Notice of Protection and Rights.

(a) Does the company provide its employees with a description of the protections and rights that apply to employee's health information?

**Response:** No

10. Notice of Information Practices.

(a) Does the company provide its employees with a description of how the company uses and discloses employee health information?

**Response:** Yes

(b) If so, please describe the information contained in such a description, when such a description is provided, and in what form it is provided.

**Response:** Information is provided in the medical plan Summary Plan Description Booklet (SPD). The SPD advises that medical information may be released to the plan administrator or a designated auditor.

11. Opportunity to Limit Uses and Disclosures.

(a) Does the company provide its employees with an opportunity to request limitations on the use and disclosure of employee health information by the company?

**Response:** No

12. Redress for Violations. Please describe any process available to employees for seeking redress for improper disclosure of the employee medical information or violation of the employee's rights with respect to that information.

**Response:** The employee can report any situation in which he/she believes that an improper disclosure of medical information has occurred. If substantiated, proper disciplinary action against the offender will be taken as well as any necessary corrective action needed as result of the improper disclosure.

13. Written Policies.

(a) Does the company have a written policy that addresses any of the following matters: 1) privacy protections relating to health information, 2) employee rights relating to health information or 3) use and disclosure by the company of employee health information?

**Response:** No

**EXHIBIT E**

June 23, 1999

Rep. Henry A. Waxman  
U. S. House of Representatives  
Committee on Government Reform  
2157 Rayburn House Office Building  
Washington, D.C. 20515-6143

Re: Privacy of Employee Health Information

Dear Representative Waxman:

This responds to your letter of June 3, 1999 inquiring about Safeway's policy regarding the privacy of information that employees provide in order to receive or pay for health care under our self-insured health plan. The specific questions set forth in your letter are in large measure inapplicable to Safeway, because we do not do any in-house processing of health care benefit claims. Nevertheless, we appreciate the opportunity to address this important subject.

Safeway recognizes the need to safeguard the confidentiality of employee health information. Our 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. Our policy goes on to further limit access to employee health information by mandating that "all information concerning the medical condition or history of an applicant or employee . . . be held in separate, confidential files." We are not aware of any instances of unauthorized access to or disclosure of employee health information, but such conduct would certainly result in disciplinary action.

Your letter notes that employers often must obtain health-related information from employees in the course of administering self-insured health care plans. Prior to 1996, Safeway processed health care benefit claims in-house and, thus, the company did routinely receive health-related information from employees. Our practice at that time was to require all personnel involved in the claims administration process to sign forms confirming their understanding that they were required to maintain employee health information in strict confidence. Since 1996, however, Safeway has contracted with a third-party, Connecticut General Life Insurance Company, to receive and process participant claims for health plan benefits and services. Our administrative services

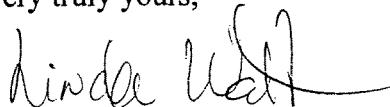
Rep. Henry A. Waxman  
June 23, 1999  
Page 2.

agreement obligates Connecticut General to maintain health information received from Safeway employees in confidence.

Safeway's decision to utilize a third-party claims administrator 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. Indeed, we regard the diminished potential for any inadvertent disclosure of employee health information to be one of the advantages of discontinuing in-house claims processing.

If your staff requires any further information from Safeway, I can be contacted at the address and telephone number shown above.

Very truly yours,

A handwritten signature in cursive script, appearing to read "Linda Watt", with a long horizontal flourish extending to the right.

Linda Watt  
Vice President, Human Resources

**EXHIBIT F**





James E. Lewin, Jr.  
Vice President

Government Affairs  
1850 M Street, NW, 11th Floor  
Washington, DC 20036  
Voice 202 828 7412  
james.e.lewin@mail.sprint.com

June 28, 1999

The Honorable Henry A. Waxman  
Member of Congress  
2157 Rayburn House Office Building  
Washington, DC 20515-6143

Dear Congressman Waxman:

Bill Esrey, the Chairman of the Board and Chief Executive Officer of Sprint Corporation, has asked me to respond to your letter to him dated June 16, 1999 regarding the privacy protections the company provides the health information of employees.

In the delivery of health care coverage to employees and their eligible dependents, Sprint offers several different options or choices from which an employee may select. These options include a self-insured traditional fee for service indemnity plan, a self-insured point of service plan (POS), and several insured health maintenance organizations (HMO). Although the indemnity plan and the POS plan are self-insured, Sprint does not manage the claims payment process. The company has contracted with a third party administrator to pay claims for Sprint based on the provisions of the plans.

Rather than respond to each individual inquiry in your letter, I will provide a general response based on the nature of Sprint's plans. As described above, Sprint outsources the processing of health claims. Thus, no claims information is submitted to Sprint by employees. Claims information is provided directly to the third party administrator by the employee or the employee's physician. Consequently, Sprint does not maintain any written or computerized records of employee health information.

While Sprint does not maintain any written or computerized records of employee health information, the company can request such information from the third party administrator if requested by the employee to assist in a dispute. This happens relatively rarely but is critical to the administration of the plan and the provision of service to our employees. Access to this information is then limited to a small number of employee benefits professionals and attorneys within Sprint and only on an "as needed basis" to resolve the claim dispute.

In developing the cost of the company's self-insured programs, and in forecasting future trends, Sprint's employee benefits professionals do analyze claims data. However, such data is scrambled before it is utilized in this fashion to ensure the confidentiality of the information and protect the privacy of the beneficiaries of the plans.

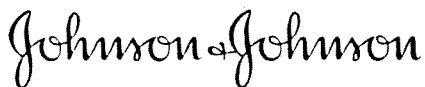
Since access to and use of claims data and health information is extremely limited, Sprint does not have a specific policy to address the proprietary nature of this information. However, the requirement to respect the proprietary nature of such information is incorporated under several different written policies that include standards of conduct and principles of business conduct. Failure to comply with these policies can lead to disciplinary action, including termination of employment.

If you have any questions, please contact myself or Bill Barloon of my staff (202-828-7446).

Sincerely,

J. E. Lewin, Jr.

**EXHIBIT G**



EFREM B. DLUGACZ  
VICE PRESIDENT  
WORLDWIDE BENEFITS  
AND HEALTH RESOURCES

NEW BRUNSWICK, NJ 08933

September 13, 1999

The Honorable Henry Waxman  
US House of Representatives  
2157 Rayburn House Office Building  
Washington, DC 20515

Dear Congressman Waxman:

This is in response to your letter to Ralph Larsen, Chairman and CEO of Johnson & Johnson, regarding the privacy of employee health information under Johnson & Johnson's self-funded medical plan(s).

Johnson & Johnson (J&J) offers its employees many different types of medical plans from which to choose, including self-funded indemnity, point of service and health maintenance organization (HMO) plans, as well as fully-insured HMOs, for which J&J pays an annual premium. All of the medical plans are administered by the Health Plan itself or through a third party arrangement. Johnson & Johnson does not administer any of these plans.

With regard to record keeping, Johnson & Johnson does not maintain any individualized written or computerized records of employee health information. The Health Plans or third party administrators maintain health information/claims data for Johnson & Johnson participants. Johnson & Johnson does not review or have access to such data on an individual basis, and no Johnson & Johnson employee has access to our third party administrators' databases. Should a Johnson & Johnson employee file an ERISA claim appeal, Johnson & Johnson requires the individual to sign an "Authorization to Release" form. This form provides the employee's permission to allow the Health Plan to release relevant medical information to an independent third party for an evaluation. The medical information released is only used to make a final determination on the claim(s) in question.

Johnson & Johnson does not have, use or disclose employee health information for the purpose of making employment decisions or for the purpose of conducting insurance underwriting. Total medical claim costs (e.g., aggregated claims data and plan administration expenses), **not employee-identifiable data**, are used for Plan underwriting/pricing by an independent third party. The independent third party that receives the aggregated claims cost data has signed a confidentiality agreement with the Health Plan and Johnson & Johnson even though there is no employee-identifiable data.

By contractual obligation, the Health Plans that administer Johnson & Johnson's self-funded medical plans limit the disclosure of employee health information to those individuals within their organization who have a need to know in order to provide plan benefits. The Health Plans do not disclose J&J employee-identifiable health information to third parties, including Johnson & Johnson.

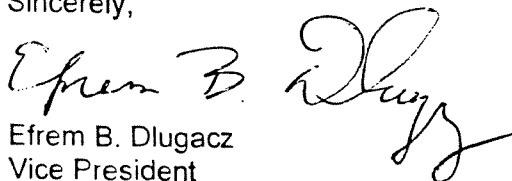
Johnson & Johnson benefits staff are trained not to disclose any employee personal data including employee health information. Also, as a condition of employment, all Johnson & Johnson employees agree to keep confidential data strictly confidential; violation of this policy can lead to disciplinary action up to and including termination of employment. Johnson & Johnson does not use employee health information in marketing activities. We regard employee health information to be confidential information.

Johnson & Johnson's policy concerning personnel records permits employees to review their files containing medical or personal information in the presence of an authorized Human Resources representative once per year. An employee may correct their records or supplement them by sending a written request to their Human Resources Department stating why they believe the information is incorrect along with the corrected information. This request becomes part of the employee's permanent record. Johnson & Johnson complies with all ERISA requirements. If an error was discovered pertaining to an employee's record, Johnson & Johnson or the Health Plans, as fiduciaries of the plan, would be obligated to correct such errors.

Johnson & Johnson is currently in the process of updating all of its Summary Plan Description (SPD) booklets and manuals to more clearly state the Company's policies and practices regarding disclosure of employee health information.

If you have any questions on the information provided here or if you have additional questions, please feel free to contact Darrel Jodrey in our Washington DC office at (202) 408-9482.

Sincerely,



Efrem B. Dlugacz  
Vice President  
WorldWide Benefits and Health Resources

# Johnson & Johnson

EFREM B. DLUGACZ  
VICE PRESIDENT  
WORLDWIDE BENEFITS  
AND HEALTH RESOURCES

NEW BRUNSWICK, NJ 08933

November 11, 1999

The Honorable Henry Waxman  
US House of Representatives  
2157 Rayburn House Senate Office Building  
Washington, DC 20515

Dear Congressman Waxman:

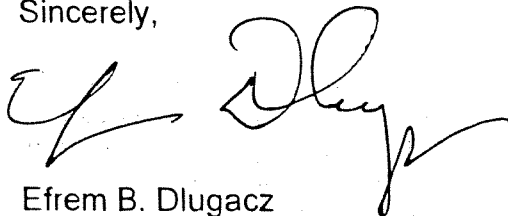
This letter is in response to your correspondence to Ralph Larsen, Chairman and CEO of Johnson & Johnson, dated October 18, 1999 regarding the privacy protections in place for our employees' health information.

Johnson & Johnson does not have a broad written policy regarding the protection of employee health information. However, there are procedures and practices which are in place today within our company as well as with the Health Plans and other third party administrators that address the privacy of employee health information. My previous letter to you dated September 13, 1999, copy attached, detailed these procedures and practices regarding the protection of Johnson & Johnson employee-identifiable health information. Johnson & Johnson is confident that our current practices are ensuring the confidentiality of employee health information.

Johnson & Johnson is in the process of developing a corporate policy that is intended to unify and consolidate policies and practices regarding the protection of all personal health-related information that Johnson & Johnson affiliates may acquire from all sources. We will be happy to make the policy available to you when it is finalized.

If you have any additional questions, please contact Darrel Jodrey in our Washington office at (202) 408-9482.

Sincerely,



Efrem B. Dlugacz  
Vice President  
Worldwide Benefits and Health Resources

**EXHIBIT H**

# JCPenney

JUL 10 1999

July 6, 1999

Mr. Henry Waxman  
Congress of the United States  
House of Representatives  
2157 Rayburn House Office Building  
Washington, DC 20515-6143

Dear Mr. Waxman,

I am responding to your request for information regarding the J.C. Penney Company, Inc. (the Company) self-insured medical plans. The Company does offer to our employees several self-insured medical plan options. All of these plans are administered by Aetna US Healthcare (Aetna), our third party medical claims administrator.

Aetna maintains computerized records of all medical claims and payments on behalf of the Company. Employee health information is not accessible to any Company officer or employee.

On a quarterly basis, individual employee health information is passed to MEDSTAT, our medical claims consultant, who provides statistical medical claims data to the Company. MEDSTAT assigns an employee number to each record. Any data specific to an employee is only revealed with this employee number. The identity of the employee is in no way revealed to the Company.

Should you need any additional information, please contact me at (972) 431-2584.

Sincerely,



Kathy Rattenbury  
Benefits Development Project Manager

cc: G. L. Davis  
R. Gill  
B. Hill  
S. Leight  
J.E. Oesterreicher  
J. Telfair  
D. Wolsieffer

# JCPenney

November 1, 1999

The Honorable Henry Waxman  
U.S. House of Representatives  
2157 Rayburn House Office Building  
Washington, DC 20515-6143

Dear Representative Waxman,

I am responding to your request for information regarding the J.C. Penney Company, Inc. (the Company) privacy protection policies for health information.

As mentioned previously, the Company does not maintain any employee health information internally. Pursuant to Company policy, our employees do not request specific medical records from third party administrators for our medical plan participants unless the information is required to respond to an inquiry initiated by the employee.

All claims data is maintained by either third party administrators or MEDSTAT, our medical claims consultant, who provides statistical medical claims data to the Company. Terms of our third party administrator contracts require confidentiality agreements prohibiting disclosure of employee health information which survive the term of the contract.

Should you need any additional information, please contact me at (972) 431-2584.

Sincerely,



Kathy Rattenbury  
Benefits Development Project Manager

cc: G. L. Davis  
D. M. Drake  
R. Gill  
B. Hill  
S. Leight  
D. McClintock  
J.E. Oesterreicher  
D. Wolsieffer



# **EXHIBIT I**



July 21, 1999

The Honorable Henry A. Waxman  
United States House of Representatives  
Committee on Government Reform  
B-350 A Rayburn House Office Building  
Washington, DC 20515-6143

Dear Representative Waxman:

This letter is in reply to your letter of June 3, 1999 to our Chairman, Richard Brown. Mr. Brown has asked me to provide you with a response to your questionnaire about our health plan and privacy protections EDS provides the health information of our employees.

EDS has in place a Global Data Protection Policy which establishes comprehensive personal data handling requirements applicable throughout EDS. These are set forth in the EDS Global Data Protection Code of Practice which would include requirements providing privacy protections relating to health information and employee rights to their personal health information. A separate EDS Code of Conduct guides personal conduct of employees with regard to all EDS policies, including the handling of sensitive data.

EDS maintains health information for those employees who choose to participate in the Traditional/Indemnity EDS Health Benefit Plan that is both self-insured and administered by EDS. Computerized records of previously submitted health care claims are maintained so that future claims submitted can be processed accurately and in accordance with plan provisions. Written claims and accompanying documents are electronically scanned and imaged, then the paper claims are destroyed within 60-90 days of receipt.

As with all personal data, health information of EDS employees is subject to the EDS Global Data Protection Code of Practice. The requirements set forth in the Code restrict access to and use of any of EDS' personal data to that required for the purposes for which it is held. I would stress, access to health care information of EDS employees is available only to the employees who work directly in support of the Health Benefit Plan. Other employees, including officers of the corporation, have no right to review or obtain information about any other employee's health information.

Further, and consistent with these requirements, health care records are segregated both physically and electronically. Physical separation is accomplished by locating the health benefits section in an isolated area of our corporate headquarters. Entry to this area requires secure access codes limited to employees who work in support of the Health Benefit Plan. All paper information containing health information is held in this secure area, and in advance of disposal, are placed in locked bins. EDS contracts with a local confidential waste disposal firm to remove and shred confidential waste from the area.

Office of Government Affairs  
1331 Pennsylvania Avenue, N.W.  
Suite 1300, North Office  
Washington, DC 20004-1703  
(202) 637-6700  
Fax: (202) 637-6759

The computer systems supporting the Health Benefit Plan are maintained in separate regions of the computer system from all other data. Electronic security is accomplished by using sophisticated computer access controls, logon IDs, and user defined passwords to protect each individual workstation and the mainframe computer systems. EDS employees supporting the Health Benefit Plan who must have access to perform a certain job within the health benefit plan are given access to only those parts of the system that will be necessary for them to accomplish their jobs.

EDS does not disclose employee health information for marketing activities and we do not disclose or use employee health information for the purpose of making hiring decisions. Any such use would clearly violate the EDS Global Data Protection Code of Practice.

EDS does supply certain claims data to health plans or HMOs that may be bidding to offer coverage to EDS employees in a given area of the country. In such cases, all unique employee and dependent identifiers (name, SSN, etc.) are removed from the file and only certain data elements are released. A disclaimer notice is submitted with each claim file stating the data is confidential and is not to be released or used for any purpose other than providing a quote to EDS for their services.

Under the EDS Global Data Protection Code of Practice, employees are informed of their data subject rights, which include certain rights of access, correction, erasure, and objection. More specific to health data, the EDS Employee handbook provides the Summary Plan Documents and a booklet describing employee rights and protections under ERISA. At any time, EDS employees may request a review or copy of their claims and health information maintained by EDS in order to exercise these rights.

Should an employee feel that his or her privacy rights have been violated, that employee has the right to contact his/her supervisor or any manager in that supervisor's management chain to address the grievances. An employee grievance would be subject to review and investigation through the EDS Global Data Protection Office. If it is determined that there was an improper disclosure, such action would be a violation of the EDS Code of Conduct and the EDS Global Data Protection Code of Practice.

Willful violation of these codes of conduct could be grounds for disciplinary action, including immediate termination from EDS. The leadership of Health Benefits Administration would work with the manager of the violator in question, EDS Security, EDS Corporate Ethics Office, EDS Legal, and the EDS Office of Data Protection, as appropriate to the situation, and would impose the appropriate penalty.

Should you have any other questions regarding our policies, please feel free to contact me.

Sincerely,



John D. Lacopo  
Corporate Vice President  
Office of Government Affairs

JDL:med

John D. Lacopo  
Corporate Vice President



November 18, 1999

The Honorable Henry A. Waxman  
United States House of Representatives  
Committee on Government Reform  
B-350 A Rayburn House Office Building  
Washington, DC 20515-6143

Dear Representative Waxman:

This letter is in reply to your correspondence to EDS CEO Dick Brown, dated October 18, 1999. Your letter, which was a follow-up to our earlier response to your inquiry regarding EDS policies on health care data privacy, requested EDS to provide a copy of our company's privacy policy. Attached please find a copy of the "Personal Data Handling Requirements, Duties of Data Controller" section of our corporate Global Data Protection Policy (GDPP).

This section of our privacy policy applies to those circumstances when EDS controls personal data of its own employees, including health care data. It is the guiding corporate policy for data privacy. Within this attached GDPP, there are thresholds of protection that apply to certain kinds of data. Since EDS considers health care data to be of the most sensitive nature, we apply additional restrictions and requirements to its handling - see section "1. B. Sensitive Data" in the attached GDPP.

More specific practice requirements, including the manner in which we segregate and protect the privacy of health care records, are already outlined in our letter to you of July 21, 1999 (see additional attachment).

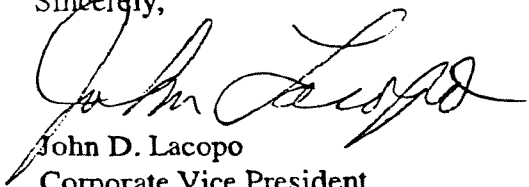
The GDPP enclosed is our corporate-wide policy for data handling and protection which applies to EDS staff, no matter where they are based around the world. It meets current national law, is in compliance with the European Commission's Data Privacy Directive, and is intended to maintain EDS as a trusted source for handling sensitive data of our own employees and that of our customers.

Office of Government Affairs  
1331 Pennsylvania Avenue, N.W.  
Suite 1300, North Office  
Washington, DC 20004-1703  
(202) 637-6700  
Fax: (202) 637-6759

Regarding the third paragraph of your letter that focuses on companies with third party administration of their health care plans, please be informed that EDS does not employ a third party administrator. Accordingly, please do not list us within this section of your report.

Should you have any further questions regarding our policies, please feel free to contact Stephen Ward in my office, who has handled the contact with your staff on this issue.

Sincerely,

A handwritten signature in cursive script, appearing to read "John D. Lacopo".

John D. Lacopo  
Corporate Vice President  
Office of Government Affairs

Enclosures

*Outline of EDS Global Data Protection Policy  
Personal Data Handling Requirements*

The duties of each EDS company under the *EDS Global Data Protection Policy* are determined in relation to each individual item of *personal data* held or otherwise used by the EDS company, and turn on whether the EDS company is a *data controller* (owner) of such data, or a *data processor* (contract service provider for the owner) with respect to such data. These duties are discussed in turn below.

**Duties of Data Controller**

With respect to an EDS company's own *personal data* (for example, *personal data* held by the EDS company related to its employees, business contacts and the like), the EDS company is obligated to meet the requirements of a *data controller*. These duties require the following:

- I. **Use Restrictions.** The EDS company must comply with the following with respect to any use<sup>1</sup> of any item of *personal data*:
  - A. **Fair and Lawful Use.** The use must be fair to the *data subject* and the use not be unlawful. This requires that the *data subject* be generally and fairly informed about what data is being collected and how and by whom it is being used. An example of unlawful use would be use of *personal data* contrary to an obligation of confidentiality.
  - B. **Justified Use.** The use must be justified on the basis of one or more specific set of circumstances.
 

**Non-Sensitive Data.** The specific justifications which might allow the EDS company's use of a particular item of non-sensitive<sup>2</sup> *personal data*, include:

    1. **Consent.** Where the *data subject* has consented<sup>3</sup> to the particular use;
    2. **Required for Contract.** Where the particular use is required to perform a contract with the *data subject*;
    3. **Required by Law.** Where the particular use is required by law; or
    4. **Overriding Legitimate Interest.** Where the use is necessary for the EDS Company's legitimate interests and those interests override the interest of the *data subject* against such use.

**Sensitive Data.** Although the use of sensitive *personal data* is more restricted, certain specific justifications might allow the EDS company's use of a particular item of sensitive *personal data*, including:

    1. **Explicit Consent.** Where the *data subject* has provided express, affirmative and written consent to the particular use;
    2. **Required by Employment Law.** Where the particular use is required by employment law; or
    3. **Required for Legal Claim.** Where the particular use is required in connection with a legal claim.
  - C. **Use for a Specified Legitimate Purpose.** Whether the *personal data* is sensitive or not, the particular use must be for and restricted to one or more specified purposes ( and not for vague, undefined purposes), which purpose(s) are known to the *data subject*.
- II. **Additional Requirements.** In addition to the foregoing use restrictions, the following requirements must be met:
  - A. **Accuracy.** The *personal data* must be accurate.

<sup>1</sup> For purposes of the data protection laws, "use" (also frequently referred to as "processing") is defined extremely broadly to include virtually anything undertaken with *personal data*, from collection to compilation, access, storage, transfer and destruction.

<sup>2</sup> Data protection laws recognize that certain categories of information are particularly sensitive and require a heightened justification for use. These categories include information about such items as racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, health and sex life.

<sup>3</sup> To be valid, the consent must be uncoerced, informed, specific and unambiguous.

- B. **Adequate, Relevant, Non-Excessive Use.** The *personal data* must be adequate, relevant and not excessive in relation to the specified legitimate purpose(s) for its use.
- C. **Maintained No Longer Than Necessary.** The *personal data* must not be kept longer than necessary.
- D. **Data Security and Confidentiality.** The *personal data* must be kept secure and confidential, and its use (including access) limited to that required.
- E. **Automated Decisions.** In the event *personal data* is used for making automated decisions, procedures must be established for review or appeal consisting of non-automated (human) involvement.
- F. **Notification of Supervisory Authority.** As required by applicable law, each EDS company must file registrations/notifications with appropriate supervisory authorities.
- G. **Provision of Data Subject Rights.** The *data subject* must be provided the following rights with respect to his or her *personal data*:
1. **Right of Access.** Such access to the *personal data* as shall enable confirmation of accuracy and use in accordance with the data protection requirements.
  2. **Right of Correction, Blocking and Erasure.** The right to demand correction, up-dating and deletion of the *personal data* as appropriate.
  3. **Compelling Grounds Objection.** The right to object to otherwise appropriate use of the *personal data* and have such use stopped, if based upon a written, specified, compelling and overriding justification.
  4. **Direct Marketing Objection.** The right to prohibit the use of the *personal data* for direct marketing purposes.

**EXHIBIT J**



# DAIMLERCHRYSLER

October 29, 1999

DaimlerChrysler Corporation

Hon. Henry A. Waxman  
U.S. House of Representatives  
Committee on Government Reform  
2157 Rayburn House Office Building  
Washington, D.C. 20515-6143

Dear Representative Waxman:

I am responding to your June 3, 1999 letter addressed to Robert J. Eaton, Chairman - DaimlerChrysler Corporation. Your letter expressed an interest in learning about DaimlerChrysler's policies and practices regarding the privacy of information that employees provide in connection with their receipt of health care benefits under our Company's health care benefit plans. Thank you for the additional time to reply.

DaimlerChrysler is the sponsor of several health care benefit plans that provide benefits to approximately 400,000 union-represented and non-represented employees, retirees, and their spouses and eligible dependents. Our plans provide a comprehensive array of health care benefits, including hospital, surgical, medical, dental, vision, hearing aid, and prescription drug benefits. Seventy-five carriers, health maintenance organizations and third parties administer plan benefits nationwide. Over 10,500,000 claims are generated annually against the plans, producing an immense volume of written and computerized claims data containing patient specific personal information and individually identifiable clinical information. It is in this context that the issue of confidentiality of employee health information takes on significant importance to DaimlerChrysler.

Our response to your letter is particularly timely because the issue of confidentiality of medical information was a topic of considerable discussion during the 1999 United Automobile Workers (UAW)/DaimlerChrysler collective bargaining negotiations. Those negotiations, which set the pattern for similar contracts at our domestic competitors, resulted in a letter agreement memorializing mutual understandings concerning the confidentiality of medical information used in connection with benefit programs. I am attaching a copy of this document and will elaborate on it below as I respond to the inquiries contained in your letter.

1. Record Keeping. The Company may from time to time have a need to maintain employee health information for the purpose of performing administrative and other fiduciary functions under its health care benefits plans. That need arises in large part during benefit claims adjudication. Our plans provide employees the opportunity to appeal benefit claim denials through defined review phases. Selected management employees are delegated responsibility at certain steps of the plan appeal procedures to review employee health information in order to determine whether services are covered under the plan. Appeal records are maintained by appropriate departments within the Company and are kept separate and apart from personnel records and other irrelevant business records. To the extent that the Company uses and maintains employee health information to perform other plan fiduciary functions, our practice is to use aggregate, patient non-specific, employee health information.

2. Employee Access to Information/Penalties for Improperly Accessing Information. Personal information obtained by the Company about employees, including employee health information maintained by the Company, is treated as confidential information. DaimlerChrysler's Standards of Conduct, which are posted throughout the Company, specifically prohibit the unauthorized use, possession, removal of and access to, corporation records of any type or form. Violations of this work place rule may subject an employee to disciplinary action up to and including termination of employment. Employment decisions are made by operating management with advice and input from the Human Resource Department and the Office of the General Counsel.

3. Disclosure and Use of Information/Penalties for Improper Information Disclosure. The same general standards stated above with respect to accessing employee health information also apply to disclosure of information. Employee health information is not disclosed to operating management for purposes of making any employment decisions such as hire, termination, promotion or demotion. Medical information distinct from employee health information is used, however, for purposes of complying with corporate obligations under the Americans with Disabilities Act, Family and Medical Leave Act and related state statutes. Those records are created or solicited by the Company's medical personnel, maintained in separate files as required by applicable law and made available to operating management only on a need-to-know basis. Finally, the company does not use or disclose employee health information for marketing activities or for purposes of conducting insurance underwriting.

4. Written Policies. The UAW/DaimlerChrysler letter agreement referenced above represents an undertaking to address specific privacy issues through the vehicle of collective bargaining. The letter was not negotiated to eliminate or manage any actual or perceived abuses. Uses of employee health information are clarified and a process is established to further discuss the need for supplemental understandings. Explicit provisions safeguarding the confidentiality of employee health information are also contained in written contracts governing the overall duties and obligations of DaimlerChrysler, carriers, HMOs and other third party administrators performing services for our benefit plans. Of relevance, third parties may not make any disclosures of employee health information to any person or entity beyond those disclosure necessary for administration purposes, or to employees, attending physician, or medical facilities, unless an authorization to release information is provided and signed by the employee, legal guardian, or is issued pursuant to statute or court order. DaimlerChrysler also enters into other administrative service agreements that prohibit the disclosure of patient specific employee health information. For example, claim payment auditing agreements require that health care plans provide aggregated data to DaimlerChrysler's auditors and excise individually identifiable employee health information from any other records provided during the scope of audit review.

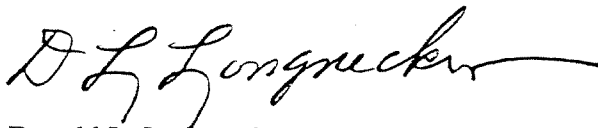
5. Record Review. Because the Company does not generally maintain health information outside the claim review process, employees do not request such information from DaimlerChrysler. Outside of benefit administration, however, company policy and union contract language provide that employees may review personnel file information, including medical information maintained in separate medical department files. These rights are grounded in Michigan law. Employees are entitled to review the content of personal files not more than twice a year and may request copies of these records.

6. Disclosure History. The Company does not maintain records of "disclosures of health information."

7. Notice of Protections and Rights/Notice of Information Practices. DaimlerChrysler provides employees with general notice of its information practices through the attached ethical code and information protection guidelines.

As Congress ponders the breadth and substance of legislation protecting employee health information, we encourage it to consider the protections already implemented by corporations over and above existing legal requirements. As our Company's experience indicates, we have been able to articulate and define uses of employee health information through collective bargaining with our union partner, the communication of internal policy directives to our workforce, and the negotiation of mutual agreements with third party health care benefit plan administrators. Our goal is to work with these parties to strike a reasonable balance between the employee interest in the confidentiality of health information and the business interest in using pertinent employee health information in a responsible fashion to effectively operate benefit plans. We hope that any new legislation will give substantial recognition to the progress already made, and that can continue, through voluntary initiatives.

Very truly yours,

A handwritten signature in cursive script, reading "D L Longnecker", with a long horizontal flourish extending to the right.

Donald L. Longnecker  
Director  
Strategic Planning & Healthcare Initiatives

Attachments

# DAIMLERCHRYSLER

## 1999 Exhibits Book

Document Title : New (03) - Confidentiality of Health Care Information

1999

New - Confidentiality of Medical Information

International Union, UAW

Attn: Mr. Stephen P. Yokich

Dear Sirs:

During these negotiations, the Corporation and the Union agreed on the desirability of maintaining a set of principles concerning the confidentiality of medical information. The Corporation reviewed with the Union its processes and practices in this regard. The parties acknowledged that medical information means any record, written or electronic, identifying a participant in the UAW/Daimler-Chrysler Corporation Pension Agreement or the Life, Disability and Health Care Benefits Program (collectively, "Benefits Programs"), containing diagnostic or treatment information and used in connection with the administration of the Benefits Programs. Accordingly, the following are understood:

- Participants in the Benefits Programs have a legitimate interest in the confidentiality of medical information pertaining to them.
- The Corporation, third party administrators, and other parties acting on behalf of the Corporation or third party administrators in connection with the Benefits Programs ("Other Parties"), have a legitimate need to collect, maintain, and use medical information in the course of performing administrative and other fiduciary functions required by the Benefits Programs and the law (e.g., verifying eligibility and benefit status, claims adjudication, audits for payment purposes, case management, coordination of benefits).
- The Corporation, third party administrators and Other Parties have a legitimate need to collect, maintain and use aggregate medical information for purposes of analysis, evaluation, oversight and quality control.
- In addition to applicable legal requirements, access to medical information maintained by the Corporation, third party administrators and Other Parties will be limited to persons having a need to use the information in the course of performing their job duties, and where appropriate and feasible, narrowly tailored in terms of scope and detail to achieve intended business purposes. Aggregate data and/or summaries will be used by the Corporation to the extent feasible.
- Medical information exchanged with Other Parties for analysis and evaluation will be used and maintained only for the purpose for which it is provided and not redisclosed by Other Parties without the prior consent of the Corporation and the Union.
- The Corporation will establish internal safeguards concerning the exchange of medical information by the Corporation. Employees who inappropriately exchange medical information will be subject to disciplinary action. The Corporation will also require third party administrators and Other Parties to establish and enforce policies and procedures consistent with this letter.
- Medical information may be exchanged with Other Parties for clinical, public health and academic research only if a meaningful purpose is to benefit participants in the Benefits Programs. Absent such purpose, the prior agreement of the Corporation and Union on all aspects of the research (e.g., topics, selection of researchers, distribution of results) is required.

KLE  
9-15-99  
AH

P.S.P. 7.12.9-15-99

9-15-99  
NR  
RJB  
Page: 1

- Benefits Programs treatment interventions should not be made by employees of the Corporation other than its medical personnel in the course of their normal activities.

The Corporation, in consultation with the Union, is committed to continuing its development of processes and practices regulating the use of medical information within the Corporation and by third party administrators and Other Parties. The Corporation and the Union also discussed proposed federal legislation and the possibility of new regulations addressing specific uses of medical information. In the event that federal standards are adopted, the parties will meet to discuss plans for compliance. Should issues arise during the course of the agreement concerning the confidentiality of medical information, the Corporation will meet with the Union to discuss mutually agreeable solutions.

Very truly yours,

DAIMLERCHRYSLER CORPORATION

By Nancy A Rae

Accepted and Approved:

INTERNATIONAL UNION, UAW

By Stephen P. Yockich

*KLY 9-15-99 [Signature] P.S.P. NR 9-15-99*

*9-15-99 NR RAG*



## CODE OF ETHICAL BEHAVIOR

*"As a Company,  
our good fortune  
and our good  
reputation go  
hand in hand. We  
cannot enjoy the  
one without  
earning the  
other—every day,  
at every level of  
the organization."*

*—R.J. Eaton*



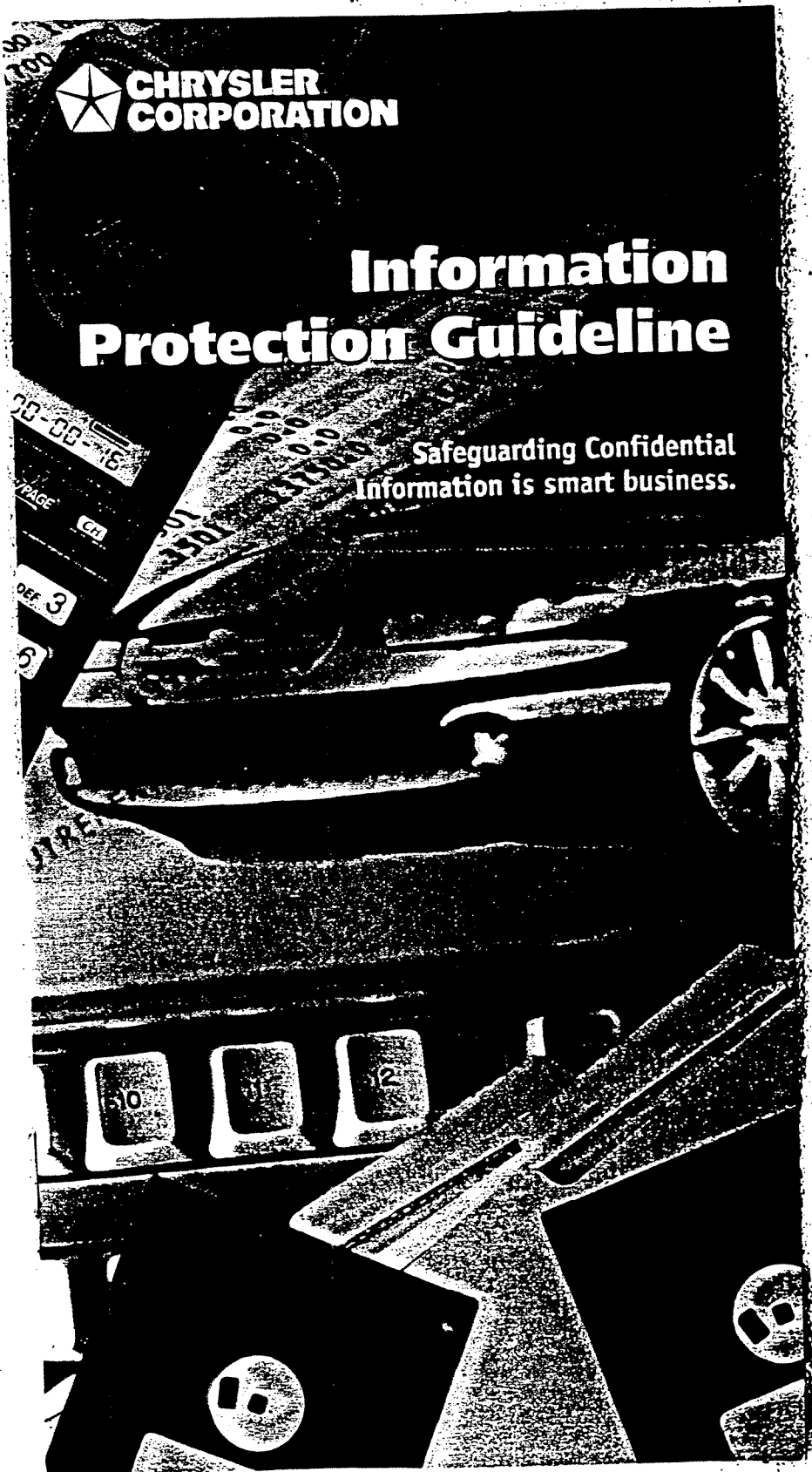
### **Confidential/Inside Information**

Confidential/Inside Information is any non-public information relating to Chrysler, its products, plants, plans, or personnel, and includes any such information which, if disclosed in an untimely or unauthorized fashion, would be detrimental to the best interests of Chrysler Corporation. Such information is to be held in the strictest confidence and should not be shared with the media, financial analysts or competitors, nor should it be used in any way that would give anyone an unfair business or personal advantage. Should there be any doubt as to whether information has been publicly released, contact the Corporate Public Relations Office.



# Information Protection Guideline

Safeguarding Confidential  
Information is smart business.





**I**t was the worst place in the world that he could imagine being, especially at 11:45 p.m. He sat bleary-eyed in the airport boarding area with his laptop glowing in front of him. He had intended to catch up on some work, but the images blurred as he stared blankly past the screen.

Suddenly he realized he wasn't alone. A fellow weary traveler appeared. She paced and glanced at her watch several times before taking a seat across from him.

"The flight's delayed," he said. "They announced that it'll arrive about two hours late."

"Just my luck," she replied. "I missed my flight earlier because I had car trouble. The electronic widget control failed on my 1991 Apex sedan and I couldn't get it started. By the time I called a cab, I missed the plane."

"That's too bad," he offered, "but not unusual with that model. The supplier never really met specs on that component and there have been a lot of failures. The good news is that

there's a fix in for next model year."

"Wow, it sounds like you know a lot about cars," she said.

"Well, I'm an engineer with Apex," he replied, "and, while I had nothing to do with that bad component design, I am proud to say that I had a part in correcting the problem."

"And what do you do?" he asked with a smile.

"Oh, me?" she replied. "I'm a reporter with Automotive Gazette."

Confidential Information can be disclosed, or "leaked," in a number of ways. Often it's inadvertent, in casual situations and frequently the source is unaware that they've disclosed anything of a sensitive nature.

Understanding the definition of Confidential Information and learning how to safeguard it is an important part of every Chrysler employee's day-to-day job.

# PROTECTING CONFIDENTIAL INFORMATION—IT'S SMART BUSINESS

## WHAT'S THE PURPOSE OF THIS BOOKLET?

This booklet explains the Company's guidelines for the definition, protection and proper use and sharing of Confidential Information, as established by Corporate Process Guideline (GEN001).

Confidential Information is an asset of Chrysler Corporation and therefore must be safeguarded by everyone—that's just plain smart business.

## WHAT IS "CONFIDENTIAL INFORMATION?"

Confidential Information (sometimes referred to as "Inside Information") is any non-public information relating to Chrysler, its products, plans or personnel, and includes any such information which, if disclosed in an untimely or unauthorized way, would be detrimental to the best interests of the Company.

## WHO IS RESPONSIBLE FOR SAFEGUARDING CONFIDENTIAL INFORMATION?

Everyone. All Chrysler employees, and all employees of Chrysler subsidiaries are responsible for protecting any Confidential Information in their possession.

## DOES MY OBLIGATION TO SAFEGUARD CONFIDENTIAL INFORMATION CONTINUE AFTER MY CHRYSLER EMPLOYMENT ENDS?

Each employee is obligated by terms of law and the Employee Assignment and Confidential

Information Agreement, to protect Chrysler's Confidential Information even after they leave Chrysler's employment. Before leaving, a separating employee must turn over to their supervisor, all documents, equipment, materials, etc., in the separating employee's possession that are the property of Chrysler.

## BUT I DON'T HAVE ANY REAL CONFIDENTIAL INFORMATION, DO I?

You probably do. No matter where you work, or at what level, from time to time you may work with information that, in the hands of others, could be used in a way that is damaging to Chrysler. Consider these examples:

- Engineering technology including patent applications, design models and trade secrets that may be part of, or necessary to the design, engineering or manufacture of Chrysler products. Other confidential engineering technology includes inventions, applications, licenses, software programs, prototypes, designs, techniques, methods, ideas, concepts, data, specifications, diagrams, drawings, schematics, test and evaluation results and blueprints
- Photographs, slides, transparencies, sketches, drawings, and computer data of advance products, components and concept models
- Manufacturing or process technology—old fashioned "know-how"
- Current and future business, product and facilities plans including capacity planning volumes, industry planning volumes, production programs, plant operating rates,

work schedules, sourcing plans or the transfer, relocation, construction, closing or disposal of facilities

- Pricing, marketing and/or financial strategies or results, including financial planning volumes, profit budget volumes, cash/capital allocation plans, earnings/losses and capital assets or financing transactions
- Information regarding contemplated structural or organizational changes including mergers and acquisitions and dispositions of subsidiaries, joint ventures and partnerships
- Information regarding Chrysler's business arrangements with outside firms, both current and future, including cooperative programs, acquisitions, trade agreements and technological development efforts
- Information about Chrysler's customers, suppliers and dealers including customer and dealer lists, incentive programs, contractual or financial relations, supplier bids and quality ratings
- Pending or threatened litigation, recalls, investigations, administrative or regulatory proceedings
- Personnel Information—Information about employees

### **WHO DECIDES WHAT'S CONFIDENTIAL INFORMATION?**

Identifying Confidential Information is primarily the responsibility of each department or function head. He or she may also designate other indi-

viduals within their area of operations who are authorized to classify information as Confidential.

However, any employee who is responsible for generating or processing information that they think should be classified as Confidential Information, should bring the information to the attention of their immediate supervisor. The supervisor will ensure that the information is reviewed by someone authorized to make the "Confidential" classification.

In cases where an employee cannot reach their immediate supervisor for help in classifying the information, the employee should treat the information as Confidential until a classification resolution can be made.

### **IS CONFIDENTIAL INFORMATION EVER DECLASSIFIED?**

Some Confidential Information is automatically declassified if it relates to a specific event or date, after which the information no longer meets the criteria for Confidential classification. In cases like this, the information should be clearly marked "Confidential until (specific date or future event)."

Other Confidential Information can only be declassified by the individual who originally made the Confidential classification, or by someone else with the same authority.

Still other Confidential Information may be declassified by the Company when it makes the information public with an authorized disclosure, such as a press release or the publication of a service manual.

## HOW CAN CONFIDENTIAL INFORMATION BE SHARED PROPERLY?

Within Chrysler Corporation, Confidential Information is shared with employees on a need-to-know basis. Once an employee is entrusted with Confidential Information, it becomes his/her responsibility to safeguard it.

- Externally, Confidential Information can be shared with individuals not employed by Chrysler on a need-to-know basis, and with the understanding that the information is to remain confidential.

For individuals not employed by Chrysler, need-to-know is determined by the requirement to perform a service or provide a product that the Company has requested and authorized.

The responsibility to determine need-to-know rests with the individual sharing the Confidential Information, based on normal and customary working relationships. In case of doubt, the decision is made by the immediate supervisor of the individual sharing the Confidential Information.

## OK, HOW DO I PROTECT INFORMATION THAT HAS BEEN ENTRUSTED TO ME?

- By being careful and aware when working with that information, and by exercising caution every time you share information.

When discussing Confidential Information, make it clear to the individual you are speaking with that it is indeed confidential. Take any necessary precautions to ensure that your conversation is not overheard or monitored.

When handling or passing along printed information, be sure that, when appropriate, it is clearly marked "Confidential." This is not to say, however, that something not marked "Confidential" should not be treated in a confidential manner. When in doubt, treat all information as Confidential Information. Here are a few other ways to protect Confidential Information:

- Only make the number of original copies of Confidential documents that are absolutely required
- Do not photocopy Confidential documents without proper authorization
- Certain Confidential documents, like the Long Range Plans for product development, are copied and numbered on special paper that cannot be legibly reproduced.
- To safeguard the confidentiality of highly sensitive data that will be distributed at meetings or among groups of individuals, number copies of booklets, reports and information packages. (This way, you can track which copy of each document was given to each individual.)
- When you mail Confidential Information, place it in a sealed envelope and clearly mark the envelope "Confidential" for both internal and external mailing. Some Confidential documents, like personnel material, are highly sensitive and should be marked "Confidential: To be opened by addressee only."

- The Confidential Information of others entrusted to our care relative to authorized agreements should be protected in the same manner that we handle our own Confidential Information.

### **HOW DO I STORE PRINTED CONFIDENTIAL INFORMATION?**

Confidential documents should be stored in locked containers, file cabinets or desk drawers. Never leave Confidential documents unattended on desktops for any period of time, and certainly never overnight.

### **HOW SHOULD I DISPOSE OF PRINTED CONFIDENTIAL DOCUMENTS THAT I NO LONGER NEED?**

When any Confidential documents, including working drafts and notes, are no longer needed, they should be destroyed by shredding. If shredding is not available, tear the document into small pieces and deposit in a waste basket. NEVER place Confidential documents in recycling boxes, bins or barrels!

### **I FAX A LOT OF INFORMATION.**

#### **HOW CAN I PROTECT WHAT I SEND?**

Before you fax Confidential Information internally or externally, call the person receiving the information and tell them to stand by their fax machine to receive a confidential document. Do not fax Confidential Information without contacting the intended recipient. Your fax cover sheet should be clearly labeled "Confidential" and should carry this,

or a similar, message:

*"The information in this fax is confidential and intended only for the use of the individual to whom it is addressed. If you are not the intended recipient, you are hereby notified that any use, distribution or copying of this information is strictly prohibited. If you have received this fax in error, please notify us immediately by telephone. Thank you."*

### **MOST OF THE INFORMATION I GENERATE AND HANDLE IS DONE BY COMPUTER.**

#### **HOW CAN I PROTECT ELECTRONIC INFORMATION?**

All your electronic information must be secured from general access with security measures like passwords, encryption or other corporate-approved secure access controls. Be aware of all the ways you transmit information electronically. There's more than just your computer. You transmit through networks, printers, video communications, and don't forget modems, telephones and faxes. Exercise caution whenever you work with electronic equipment. You must ensure that your access and your remote connection are secure.

The principles of protecting electronic information are similar to protecting printed information. Caution and care are the watchwords. Here are some examples:

- All Confidential Information should be clearly marked "Confidential" and/or should be protected using a corporate-approved secure access control system

- Make only the required number of original copies of electronic Confidential documents and remember: Everyone who is entrusted with a copy of a confidential document is responsible for the security of the document
- Don't make electronic copies of Confidential Information; if absolutely necessary, do so only with the proper authorization
- Certain Confidential documents should only be stored in an encrypted format. Encryption is the process of converting some information from an easily understandable format into what appears to be random, useless unintelligible characters
- Some Confidential documents, like Long Range Plans for product development, may be reproduced for contingency planning purposes, but only in an encrypted format
- When you send Confidential or highly sensitive material over a network, make sure your transmission is encrypted
- Highly sensitive Confidential Information, like personnel documents, should be safe-guarded with multiple layers of access controls
- Contact your computer service organization for further information and/or assistance.

### **HOW ABOUT SAFELY STORING ELECTRONIC INFORMATION?**

Again, the principles are the same as with printed information. Store electronic information in locked cabinets, desks or rooms using an encrypted format and/or use a corporate-

approved secure access control. Never leave electronic information unsecured. Don't leave modem or network connections open and never leave a computer with Confidential Information unattended.

### **OK, HOW DO I DISPOSE OF ELECTRONIC CONFIDENTIAL INFORMATION? CAN I JUST THROW AWAY A DISK OR TAPE?**

NO! When Confidential electronic information, including working files, is no longer needed it should be destroyed by degaussing, or erasing, of tape, or reformatting of floppy disks or hard disk space. Information that is merely deleted can be recovered with special software.

### **WHAT ABOUT THINGS LIKE CLAY MOCK-UPS AND PROTOTYPE VEHICLES? AREN'T THEY "INFORMATION" THAT NEEDS TO BE PROTECTED?**

Certainly. Models, mock-ups and prototype components and vehicles (as well as corresponding photographs, sketches and related electronic versions) are what is called "information in a physical medium" and they need the same kinds of safeguarding as other forms of information.

Physical information should be contained in areas or spaces protected from unauthorized access. During off hours, those areas should be locked and secured with an alarm system.

When you transport physical information, it should be suitably protected or disguised with

wrapping, shielding, or other means to prevent it from being viewed by unauthorized individuals.

When physical information is no longer needed, it should be destroyed by disassembly and, if necessary, disguised or modified to protect the features that had been classified as Confidential.

### **IS THAT EVERYTHING I NEED TO KNOW ABOUT INFORMATION PROTECTION?**

It's a real good start. But, because the methods and technology of communication are constantly changing, there may be, from time to time, additions or modifications made to this guideline by corporate officers. Each department is free to establish additional safeguards appropriate for its operations.

If you have any questions involving the protection of Confidential Information, speak to your immediate supervisor.

### **OK, SO NOW I KNOW HOW TO PROTECT CONFIDENTIAL INFORMATION, BUT WHAT IF I SEE SOMEONE ELSE HANDLING OR SHARING CONFIDENTIAL INFORMATION CARELESSLY OR IMPROPERLY? SHOULD I REPORT IT? TO WHOM?**

If you're aware that Confidential Information is being handled carelessly or even "leaked" outside the corporation, report it immediately to your immediate supervisor. You may also contact the Manager, Special Security Operations or call the Business Practices

Hotline: (810) 512-9800; Tie Line: 722-9800; Toll-free: 1-800-543-1391. Information that damages Chrysler also injures everyone who works for Chrysler.

Reports of lapses in information protection or leaks can be made anonymously. And remember, reporting such incidents isn't "snitching," it's just smart business!



### **ATTENTION:**

This Guideline applies to Chrysler Corporation and each of its subsidiaries.

Chrysler reserves the right to monitor information use to ensure compliance with its policies.

Violations of this guideline, or any other Chrysler policy or procedure, may result in disciplinary action up to and including discharge and, if warranted, legal proceedings. Chrysler reserves the right to amend, interpret and construe this guideline. Nothing herein, however, shall constitute a contract of employment with any employee or conflict with Chrysler's right to terminate employment relationships at will.



## STANDARDS OF CONDUCT

To all Chrysler employees:

We set the highest business and ethical standards for ourselves and our operations at Chrysler. Our conduct must reflect our commitment and responsibility to our customers, our employees, our dealers, our suppliers, our shareholders, our governments, and the communities in which we operate.

We rely on every employee to maintain a cooperative relationship with his or her fellow workers. This relationship requires respect for each other and recognition that every employee is a valuable contributor to the overall success of our organization.

In order to maintain a safe, well run organization, certain conduct cannot be tolerated. Engaging in any of the following actions - which are intended as examples - violates the standards that Chrysler expects of its employees and is grounds for disciplinary action up to and including discharge.

1. Providing false and/or misleading information to the corporation.
2. Failure to ring in your own time card, ringing another employee's time card, or permitting another to ring your time card.
3. Unexcused absence or tardiness from plant or work station.
4. Leaving your work station, office or plant during working hours without permission or failing to return to work after lunch or relief without permission.
5. Failure to exert normal effort on the job, wasting time, loafing, loafing or sleeping on the job.
6. Failure or refusal to follow the instructions of supervision.
7. Leading, instigating, supporting or taking part in any strike, work stoppage, or picketing in violation of the collective bargaining agreement, or in any slowdown or other improper interference with or restriction of operations.
8. Harassing any person, whether or not a Chrysler employee, based on that person's sex, race, religion, age, handicap, national origin, sexual orientation, or membership in another protected class.
9. Production of excessive scrap or inferior work.
10. Negligent or deliberate damage or destruction of property owned or held by the corporation or any employee, or the abuse or misuse or unauthorized use of any such property.
11. Immoral or indecent conduct.
12. Use, possession, distribution, sale or offering for sale, or being under the influence of alcohol or drugs (other than use or possession of narcotics in medicines prescribed by the employee's physician), on corporation property, or while operating a corporation owned motor vehicle, or while engaged in corporate business.
13. Unacceptable conduct due to alcohol or drug abuse (other than use or possession of narcotics in medicines prescribed by the employee's physician), or conduct that indicates a potential for impaired or unsafe job performance due to drug or alcohol abuse.
14. Threatening, intimidating, coercing, harassing, retaliating, or using abusive language to others.
15. Fighting, "horseplay" or other disorderly, disruptive or unruly conduct.
16. Creating or contributing to unsafe or unsanitary conditions.
17. Smoking or parking in unauthorized areas.
18. Unauthorized solicitation, except such solicitation during non-working time as is protected by the National Labor Relations Act.
19. Unauthorized distribution of literature except such distribution during non-working time in non-working areas as protected by the National Labor Relations Act.
20. Posting, removing or in any manner defacing notices or other signs on bulletin boards without specific authorization of management.
21. Unauthorized use, possession, or removal of, or access to, corporation records of any type or form.
22. Engaging in, participating in, aiding or approving conduct constituting or appearing to constitute a conflict with the interests of the corporation.
23. Actual or attempted theft, fraud, or misappropriation of property, including the aiding or abetting of the same.
24. Gambling, conducting games of chance, or possessing gambling equipment on corporation premises.
25. Bringing firearms, knives or other weapons on to company property or possessing the same on company property.
26. Failure or refusal to show proper identification upon entering a facility or when requested to do so.
27. Permitting improper use of your badge, identification card, or other corporation passes, papers, or properties which may be entrusted to you.
28. Failure or refusal to permit inspection of items such as lockers, vehicles, packages, lunch boxes or hand bags when requested to do so.
29. Failure to follow safety procedures, or to wear or use as instructed required safety or health protective equipment.
30. Failure or refusal to work overtime as instructed by supervision.
31. Removing, altering or making inoperative any equipment or device designed to protect employees from injury and/or illness.
32. Conducting a check cashing service or other business enterprise or engaging in any illegal acts such as "loan sharking" while on corporate premises.
33. Unauthorized use of, or access to, Chrysler's computer systems and software.
34. Failing to observe the terms of dress codes established by your work location.

**IMPORTANT NOTICE:** The Corporation, through its Human Resources Department, reserves the right to modify, revoke, suspend or terminate the Standards of Conduct, or any portion thereof, at any time, at its sole discretion. These Standards of Conduct shall not, under any circumstances, be deemed to be part of any employment contract or agreement with any employee.



ADMINISTRATIVE SERVICES AGREEMENT  
between  
BLUE CROSS AND BLUE SHIELD OF MICHIGAN  
and  
THE CHRYSLER CORPORATION

This Agreement, effective as of January 1, 1993, is by and between the Chrysler Corporation (Employer) whose address is 12000 Chrysler Drive, Highland Park, Michigan 48288, and Blue Cross and Blue Shield of Michigan (BCBSM), a Michigan nonprofit Corporation, whose address is 600 Lafayette East, Detroit, Michigan 48226.

WHEREAS, the Employer has established a Program, as defined below, making available health care benefits to eligible, on-roll Chrysler employees and retirees, and their respective surviving spouses and dependents, and

WHEREAS, the Employer has requested BCBSM to furnish administration services in connection with operation of the Program and to serve as the Control Plan, as defined below, for the purpose of ensuring conformance to the Program and this Agreement by the Blue Cross and/or Blue Shield plans serving as Participating Plans, as defined below, and

WHEREAS, it is the purpose of the Agreement to establish a relationship whereby BCBSM shall undertake receiving and processing claims for benefits under the Program, disbursing claim payments under the Program, and performing such administrative duties as set forth herein.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, it is hereby agreed as follows:

Article I. Definitions.

1. "Administrative Manual" means the manual(s) describing benefits, eligibility criteria and various other administrative undertakings selected or negotiated by the Employer.

- b. A listing of all BCBSM subsidiaries, subcontractors, vendors or agents providing services specific to the Employer under this Agreement where compensation is in excess of two percent (2%) of the annual administrative fee paid by the Employer.
- c. A determination of financial accuracy in accordance with Article VI of this Agreement. This report shall be in a format mutually acceptable to the Employer and BCBSM and shall provide sufficient detail to allow independent confirmation of the calculations.

**3. Other Reporting.**

BCBSM will continue to provide all other reports and data that it presently provides to Employer.

**4. Disclosures to Enrollees.**

The Employer will disclose to Enrollees all information as required by law, including any disclosures required by MCLA 550.1211(a)(4).

**Article IX - Data Analysis**

**1. Data Access.**

BCBSM will cooperate fully in providing Employer, or Employer's agent and auditor, access to data which may be required for purposes of analyzing Employer's health benefit costs and utilization subject to the provisions of an executed Data Protection and Confidentiality Agreement, the terms of this Agreement and any requirements imposed by law. Data requests to BCBSM will be made in writing and only after consultation with BCBSM regarding data requirements. BCBSM will provide the requested data for a time period(s) as mutually agreed.

Data requested may include, but not be limited to the following:

- a. **Claims Data** - In response to a request submitted by Employer, BCBSM will deliver, following each calendar quarter, a data processing file containing all claims paid during the just-ended quarter which meet such criteria as may be contained in the data request.
- b. **Supporting File and Documentation** - In response to requests for claims and eligibility data, BCBSM will also provide Employer with documentation and supporting files which may be needed to understand the values of any variables contained in the claims or eligibility files. Documentation and supporting files will be specified and costed. Such supporting information will include but not be limited to data dictionaries, record layouts, and cost-to-charge files, excluding provider contracts or contractually protected information.

## **2. Accuracy of Data.**

Required data files will be delivered at dates mutually agreed upon and will be complete in terms of all data elements and all claims which meet data request specifications. BCBSM will verify completeness prior to delivering data. Data accuracy standards for each ad hoc report will be mutually determined prior to the data being provided.

## **3. Reimbursement.**

Employer will directly and separately from other amounts due under this Agreement reimburse BCBSM for its costs incurred in connection with services provided Employer under this Article.

## **4. Protection Agreements.**

Prior to the release of any data to a party other than Employer, a Data Protection and Confidentiality Agreement, approved by BCBSM, will be executed between Employer and any person or entity to which the data is to be released.

## Article XII - Records, Audit, and Confidentiality

### 1. Records Access and Audits.

BCBSM will make available for inspection by the Employer or the Employer's agent or auditor, at any reasonable time during the term of the Agreement any records directly bearing upon claim payments made under this Agreement, excluding provider contracts and contractually protected information. This provision shall be subject to all provisions of this Agreement regarding use of data and confidentiality and any provisions of law. Audits will be conducted by an auditor acceptable to BCBSM and will be subject to the auditor and the Employer executing BCBSM's Audit and Indemnification Agreement with BCBSM and any other Participating Plan deemed necessary by BCBSM. Such Agreement will include provisions on audit process and procedures, proprietary and confidential information, costs, indemnification, and other audit matters. All costs related to the audit will be paid by the Employer directly and separately from other amounts due under this Agreement.

### 2. Provider Audits.

Any agreement between the BCBSM or a Participating Plan and an Affiliated Provider shall allow the Employer to audit the records of the Affiliated Provider that pertain to the Program.

### 3. Confidentiality of Records.

Except as the Employer may deem appropriate for audit purposes, the Employer and Participating Plans will treat with confidentiality all information provided to one another under the terms of this Agreement, including but not limited to information relating to specific Enrollees, will use such information only to administer this Agreement and/or analysis to manage costs and utilization hereunder, and will not release any information for any other purpose, except as permitted by law. The Employer may, however,

utilize information regarding overall claims experience for comparative rate quotations. Further, the Employer, BCBSM and Participating Plans shall comply with all federal laws and regulations determined applicable regarding access to, review of, and/or use of such information, including but not limited to information relating to Enrollees.

### Article XIII - Litigation

In the event of any litigation, administrative proceedings or arbitration between Employer, BCBSM and/or a Participating Plan and a person or entity who is not a party to this Agreement involving a dispute directly or indirectly arising under the Program or this Agreement, the Employer and BCBSM shall, and BCBSM shall cause Participating Plans to:

- (a) reserve the right to select and retain counsel to protect its interests and, unless otherwise expressly provided in this Agreement, be liable for the payment of its own legal fees, disbursements and court costs;
- (b) promptly notify the other after learning of such litigation, administrative proceeding or arbitration;
- (c) cooperate fully by providing the other with all relevant information and documents within their control; and
- (d) reasonably assist the other in the defense of such litigation, administrative proceeding or arbitration.

If BCBSM, or a Participating Plan, is the sole named defendant, it shall have discretion to defend, settle, compromise or otherwise resolve ("Resolve") such matter in a manner which BCBSM or the Participating Plan determines to be consistent with the terms of the Program and this Agreement, but only after consultation with the Employer. If the Employer, BCBSM and/or a Participating Plan are co-defendants, they will cooperate fully with each other to Resolve such matter consistent with the terms of the Program and this Agreement. If the preceding sentence applies, the Employer shall have the right to select and retain lead counsel with respect to the defense, settlement, compromise or other

8. Consent or Approval.

Whenever the Employer's or BCBSM's consent, approval or agreement is required pursuant to this Agreement, it is agreed that such consent, approval or agreement shall not be unreasonably withheld.

9. Scope and Effect.

This Agreement, and any attachments hereto, constitute the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior agreements and representations, whether oral or written, with respect to the subject matter and shall be binding upon the parties, their successors and assigns.

10. Amendment.

This Agreement may be amended from time to time as mutually agreed by the parties. To be effective, any amendments to this Agreement must be written and signed by the authorized designated representatives of each party.

BLUE CROSS AND BLUE SHIELD OF MICHIGAN

CHRYSLER CORPORATION

By: Thomas W. Ruloff  
(Signature)

By: D. L. Longnecker  
(Signature)

Name: Thomas W. Ruloff  
(Print)

Name: D. L. LONGNECKER  
(Print)

Title: Director, Chrysler Financial Program Administration

MANAGER, FINANCE & PLANNING  
Title: Health Care & GROUP INSURANCE

**CHRYSLER CORPORATION  
HEALTH CARE SERVICES AGREEMENT**

An Agreement between Chrysler Corporation  
and Health Alliance Plan

1996

Agreement. If Company desires to change the monthly premium payments, Company will inform Chrysler in writing of the desired new monthly premium at least one hundred eighty (180) days (or such later date as mutually agreed in writing between the Company and Chrysler) in advance of said anniversary date. Chrysler will notify Company in writing, prior to said anniversary date, of the acceptability or unacceptability of the premium increase. If Chrysler fails to notify Company prior to said anniversary, the requested premium increase will become effective in the first month following said anniversary. If Chrysler notifies Company of the unacceptability of the premium increase, the Parties will work together to establish a mutually acceptable monthly premium. If the Parties are subsequently unable to agree upon an acceptable monthly premium, then notwithstanding Section 2.3 of this Agreement, either party will have the right to terminate this Agreement effective as of the first day of the month following the anniversary date upon 15 days advance written notice of termination. In such case, for the one month period after the anniversary date and prior to termination, the monthly premium will remain at the level in effect prior to said anniversary date. If, on the other hand, neither party terminates this Agreement within such one month period, the requested premium increase will become effective retroactive to the first month following said anniversary date.

Section 5.2 No Other Payments. The payments described in Section 5.1 above will be the only responsibility that Chrysler will have with respect to paying for the Program. Chrysler will have no responsibility to pay any other person or entity including, but not limited to, Enrollees, Affiliated Providers and Nonaffiliated Providers, for services rendered pursuant to the Program.

Section 5.3 Determination of Eligibility. Chrysler will furnish Company with the name, birth date, Social Security number, gender and address of each Enrollee as well as certain other identifying information as may be requested by the Company. Chrysler will furnish Company with Enrollee updates on a monthly basis as necessary. Company agrees to accept each Enrollee, and Chrysler will have the sole power and authority to remove Enrollees from the Program. Company shall treat such information as confidential.

## ARTICLE VI PERFORMANCE EXPECTATIONS

Section 6.1 Performance Expectations. Company agrees that it will meet the performance expectations set forth in Appendix E to this Agreement.

Section 6.2 Audit of Records. Subject to Section 7.2 herein, the Parties expressly agree that Chrysler will have the absolute right to engage the services of any person or entity to audit any aspect of Company's performance with respect to this Agreement. Company will make available for audit by Chrysler or any auditor designated by Chrysler its files, books and records pertaining to the Plan or the Program and the services provided to Chrysler hereunder, including without limitation documents relating to credentialing, utilization review and quality assurance. Said inspection will occur during normal business hours after Company has received reasonable notice from Chrysler or the auditing entity.

## ARTICLE VII PLAN RECORDS AND CONFIDENTIALITY

Section 7.1 Plan Records. Any data provided to Company by Chrysler will remain the property of Chrysler. Company will maintain or cause to be maintained adequate records relating to the Coverage(s) it provides under the terms of this Agreement. Company will maintain



its records relating to these Coverage(s) for the greater of six (6) years or the period of time required by law. Subject to Section 7.2 herein, such records will remain confidential. However, Chrysler or its designated agents will have, upon request and after reasonable notice, the right to inspect any relevant books, records, reports, documents, writings or other data prepared and maintained in connection with the Program. Company will take all necessary measures to ensure that Chrysler also will be permitted, upon request and after reasonable notice, to inspect the medical records of Enrollees to the extent reasonably necessary in connection with workers' compensation and occupational safety laws, or any other laws affecting the safety of Chrysler's workplace or any potential liability with respect to its workforce.

**Section 7.2 Confidentiality.** Except as preempted by ERISA, Company and Chrysler will comply with all applicable laws and regulations regarding the privacy and confidentiality of the health and medical records of Enrollees. Company will not be required to unlawfully disclose the medical records of any Enrollee to the extent it has such records; provided, however, Company shall make such medical records available to Affiliated Providers. Nonaffiliated Providers or Chrysler as needed to fulfill their legal or contractual duties. Company agrees that neither it, nor any of its employees, Affiliated Providers or agents, will make any other disclosure to any person or entity outside the Company of information identifiable to any Enrollee beyond those disclosures necessary for administration purposes or to the Enrollee, attending physician, clinic, group of physicians, hospital, or other provider or payor unless an authorization to release such information is signed by the Enrollee or legal guardian, or pursuant to statute or court order for the protection and discovery of evidence.

**Section 7.3 Proprietary Information.** Company agrees that information regarding any financial arrangements of Chrysler is proprietary information that will not be disclosed to anyone who is not employed by Chrysler and directly involved in the performance of this Agreement, without Chrysler's prior written authorization.

## **ARTICLE VIII INDEMNIFICATION**

Company will hold harmless and indemnify Chrysler, the Plan(s), and any of their respective officers, directors or employees from and against any claims, losses, damages, liabilities, costs, expenses (including attorney fees and related costs), or obligations arising out of or resulting from (a) the breach of any of its duties and responsibilities set forth in this Agreement, (b) the breach of its fiduciary duties and responsibilities under ERISA, or (c) the negligence, willful misconduct or fraud or criminal misconduct of Company or any of its officers or employees in the performance of services rendered in connection with the Program or this Agreement.

## **ARTICLE IX INSURANCE**

**Section 9.1 Insurance for Company.** Company will procure and maintain a policy of general liability insurance, including broad form contractual coverage, in an amount not less than \$1,000,000 per occurrence, with Chrysler and the Plan(s) as named additional insureds. Company will provide Chrysler with evidence of such coverage upon request and agrees to provide prompt notice to Chrysler of the loss of such coverage.

**Section 9.2 Insurance for Affiliated Providers.** Company also will require by contract that each Affiliated Provider procure and maintain a policy of professional liability insurance against any claim for damages arising by reason of personal injury to an Enrollee caused

IN WITNESS WHEREOF, the Parties have executed this Agreement this  
25 day of November, 1996.

CHRYSLER CORPORATION

By: D. Longmeyer

Title: Mgr Finance & Planning

HEALTH ALLIANCE PLAN

By: Mansoor Khan (Mohammed KANAWALA)

Title: UNDERWRITING & RATING MANAGER

**EXHIBIT K**



Office of the Director of Public Affairs

1301 K Street, Northwest, Suite 1200  
Washington, DC 20005 3307

October 29, 1999

Honorable Henry A. Waxman  
United States House of Representatives  
Committee on Government Reform  
2157 Rayburn House Office Building  
Washington, D.C. 20515

Dear Representative Waxman:

I am responding on behalf of Mr. Gerstner to your October 18 letter requesting additional information about IBM's voluntary policies with respect to employee medical records.

As we stated in our June 25 letter, IBM's interest in this important issue comes from our role as an employer as well as a provider of information technology solutions and services. As an employer, we address medical records confidentiality both during the process of arranging for health insurance coverage, and during workplace encounters (e.g. workers' compensation and wellness programs).

To supplement the information we originally provided, enclosed are (1) excerpts from IBM's policy on employee medical records, as that policy is posted on our internal Web site for employees and (2) a sample of the language we would typically include in contractual arrangements with third party companies who might manage certain health-related functions and who would be expected to handle personally-identifiable employee information.

I can be reached directly at 202-515-5036 should you have additional questions.

Sincerely,

Harriet P. Pearson

HPP:tkl  
Enclosures

cc: Mr. Gregory Waddell, IBM

## Enclosure 1

### A. IBM Guidelines For The Protection Of Employee Information

[These are corporate wide policies, applicable to all types of employee information; there is a supplement to this policy below, that deals specifically with medical records]

#### Introduction

As a global company, IBM's business processes increasingly go beyond the borders of one country. This globalization demands not only the availability of communication and information systems across the IBM group of companies (IBM), but also the worldwide processing and use of Employee Information within IBM.

IBM remains committed to protecting the privacy and confidentiality of information about its Employees. Establishing uniform practices for collecting, using, disclosing, storing, accessing, transferring or otherwise processing Employee Information helps IBM use Employee Information fairly and appropriately and disclose it only under appropriate circumstances.

The Guidelines set forth the fundamental practices for collecting, using, disclosing, storing, accessing, transferring or otherwise processing Employee Information. The purpose of these Guidelines is to provide an adequate level of protection for Employee Information on a worldwide basis.

In these Guidelines 'Employee Information' means information relating to an identified or identifiable Employee which is processed electronically or as part of a manual file, and 'Employee' means any current or former employee of an IBM company.

In the event of conflict, local law will prevail over these Guidelines. These Guidelines are not to be construed as a contract, either express or implied.

#### 1. General Processing Principles

The proper processing of Employee Information is an important part of the effective management of IBM's business processes which use such information. IBM will:

- process Employee Information fairly and lawfully;
- process Employee Information in a manner which is not incompatible with the purposes for which it is collected;
- only process Employee Information which is relevant to and necessary for the particular purposes; and
- instruct third parties processing Employee Information on behalf of IBM, if any, to implement appropriate measures to safeguard the Employee Information.

#### 2. Processing of Sensitive Information

IBM recognizes that under the laws of some countries certain information about Employees, such as information regarding racial or ethnic origin, political opinions or philosophical beliefs, trade-union membership, and health or sex life, should be considered 'sensitive.' Whenever possible, such sensitive information should be processed in aggregate or anonymous form so that a particular individual is not identifiable. If this is not possible IBM will only process the information:

- in accordance with applicable local law (and any designated safeguards provided therein);
- with Employee consent; or
- where necessary for the establishment, exercise or defense of legal claims.

### 3. Collection of Employee Information

The effective management of IBM's business processes requires IBM to collect information about its Employees. When doing so, IBM will:

- where appropriate, collect information directly from employees;
- when collecting information from Employees, describe the categories of information and the purposes for collection, unless obvious or collected in connection with an internal investigation or audit; and
- collect information from outside of IBM only when necessary.

### 4. Use of Employee Information Within IBM

Use of Employee Information is subject to the following requirements:

- Employee Information will only be made available within IBM to other individuals with a 'need to know' such information;
- when making Employee Information available within IBM involves a transborder data flow, the Employee Information will receive the level of protection described in these Guidelines in every country. The receiving IBM company will assume responsibility for complying with these Guidelines with respect to such Employee Information;
- 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.

### 5. Disclosure of Employee Information Outside IBM

IBM will only disclose Employee Information outside IBM where it is:

- necessary to protect the vital interests of the Employee;
- with the consent of the Employee;
- required or authorized by local law;
- necessary for IBM's business purposes provided that they are not overridden by the privacy interests of the Employee concerned;
- necessary to satisfy the legitimate requirements of a company or other entity which is considering acquiring some of IBM's business operations.

## 6. Storage of Employee Information

When storing Employee Information, IBM will:

- take every reasonable step to keep the Employee Information as accurate, complete and up-to-date as is necessary for the purposes for which it is processed;
- retain Employee Information no longer than necessary for the purposes for which the information is processed, or as required or permitted by local law.

## 7. Security of Employee Information

Employee Information will be classified according to its sensitivity using the IBM security classification system and will be handled according to the applicable IBM Corporate Instructions. These include physical access control, logical access control, inter-enterprise control, data transfer security, filing media security, tractability of access and auditability of processing.

## 8. Access to Employee Information

An Employee, upon written request to IBM, will be entitled to have access to his or her Employee Information, and to have such Employee Information corrected if inaccurate. This does not apply to Employee Information which is investigative or evaluative in nature, or which would disclose information about another Employee.

In the event of a dispute between IBM and an Employee regarding the accuracy of his/her Employee Information, consideration will be given to the temporary blocking of that information.

## 9. Compliance

IBM is committed to comply with these Guidelines and to provide Employees with effective mechanisms to raise concerns regarding, and obtain appropriate redress for noncompliance with, these Guidelines:

- if any instance of noncompliance is discovered, the IBM company concerned must modify its practices to comply with these Guidelines;
- failure by an Employee to comply with these Guidelines may result in disciplinary action;
- Employees may use the IBM Open Door Program to obtain an impartial investigation of disputes regarding compliance with these Guidelines;
- compliance with these Guidelines is subject to IBM audits under applicable IBM procedures.

## **B. Guidelines specifically for the handling of medical information:**

### Health Information Management

#### OBJECTIVE

To assure that health information obtained on individuals in the course of implementing GOHS (acronym for IBM's medical staff) Occupational Health Programs is handled confidentially and is collected, used, disclosed, stored, accessed, and transferred in accordance with legal and IBM requirements.

In this document, "GOHS staff" or "GOHS personnel" stands for medical staff (physician, nurse, and support staff); "GOHS professional" stands for physician, nurse, or technician; and "health information" stands for personal health or medical information on a specific individual.

In some locales outside the United States, health information pertaining to GOHS programs is maintained by IBM personnel who are not part of GOHS (such as Human Resources personnel). GOHS geographic managers must establish processes which assure that health information maintained by non-GOHS personnel is handled according to the requirements below. When a requirement must be fulfilled by a GOHS professional, the GOHS geographic managers must establish processes to assure that appropriate professionals can fulfill the requirement.

This document does not pertain to health information that may be created as a result of any other IBM program, such as health insurance benefits administration.

#### REQUIRED PROGRAM ELEMENTS

1. Country-specific laws may dictate how health information shall be managed. Each GOHS unit, or non-GOHS personnel who maintain health information, must be familiar with and follow the legal requirements for health information management.

2. In addition, GOHS staff and non-GOHS personnel who maintain health information must follow IBM's requirements unless the country-specific laws prohibit following any or all of the Company requirements. The IBM requirements for managing employee information are found in IBM Corporate Instruction, Human Resources 113, "Protection of Employee Information" and in the IBM Guidelines for the Protection of Employee Information. The requirements below supplement the IBM Guidelines for the Protection of Employee Information for health information only.

##### a. Creation of Health Information

1. Written or electronic health information must be created when a GOHS professional counsels, examines, or conducts a test (such as audiometry) on an employee:



in the course of carrying out GOHS occupational health programs;  
when an employee raises a concern about a potential work-related exposure, injury,  
illness, or symptom; and  
when an employee presents with a personal injury or illness that may affect job  
performance.

2. This health information shall be maintained by GOHS.

b. Confidential Storage of Health Information

1. Hard copy (paper) health records on individuals shall be maintained in secure cabinets that are separate from cabinets containing other kinds of information (for example, industrial hygiene and other human resources information). The cabinets shall be located in a room that is locked when GOHS personnel are not present. The GOHS unit in which that room is located shall also be locked when GOHS personnel are not present or when the room is not being observed by GOHS personnel.

2. Health information maintained by non-GOHS personnel must also be kept in locked cabinets and separate from any other information.

3. Both hard copy and electronic health information shall be accessible only by personnel authorized by the GOHS health care professional in charge of a GOHS unit, or by personnel authorized by the GOHS geography manager for information maintained by non-GOHS personnel.

4. Neither paper nor electronic health information that is in use shall be placed so that it can be viewed by unauthorized individuals.

c. Access to Health Information

1. Unless prohibited by law, each employee has a right to access his or her health information. An employee shall make a written request for access or copies of the health information. When an individual wants only to review his or her health information, this review shall take place in the presence of a GOHS professional. (1)

2. If an employee requests that an addition be made to his or her health information, a GOHS professional will, within a reasonable period of time or within a period of time required by law, either:

make the addition, noting that it was requested by the employee; or  
inform the individual of a refusal to do so and the reason for the refusal.

3. If the GOHS professional refuses to make an addition to the employee's record, the employee is allowed to write a statement, to be placed in the health record, disputing the denial. In any subsequent disclosure of the disputed information, this statement shall also be disclosed.

4. Employees must sign a written consent for access to their personal health information or release of their health information in the following circumstances:

- for an employee wanting a copy of his or her health information;
- to honor a request from a properly identified health care professional;
- for investigators looking into work-related claims, where required by law.

5. Unless prohibited by local law, employee health information may be disclosed by the GOHS physician in charge, without written employee consent, under the following circumstances:

- to assist in emergency treatment when the employee is unable to give consent;
- when Company legal counsel requests health information related to legal issues involving legitimate Company interests;
- when there is a demonstrable, overriding need for information to protect public health or safety;
- when conducting human health research in accordance with IBM Corporate Instruction, Human Resources 102, "Human Health Research";
- when assisting law enforcement or public health authorities, as required by law; and
- when IBM has been served with a subpoena or court order to which IBM is not actively in the process of objecting.

## Attachment 2

IBM expects that the reputable companies that we engage to administer health insurance-related programs will keep personally-identifiable employee information secure and in accordance with appropriate privacy practices. Below is a sample of a typical contractual provision we would include in our agreements with such firms.

Sample clause: “[*Third party*] shall establish and maintain adequate safeguards to protect the confidentiality of all medical records and names, addresses, telephone numbers, Social Security numbers, dates of birth and all other personal information pertaining to Participants that [*third party*] may be given or obtain as a result of performing services for [*company*] except as required to perform services pursuant to this Agreement, or requested by applicable law.”

In addition we follow a policy of maintaining a separation between personally-identifiable employee medical information gathered and managed by health care providers and insurers on the one hand, and IBM human resources personnel on the other, such that the services provided by such third parties would not result in employee personal information being shared with IBM personnel without the employee’s consent.



Office of the Director of Public Affairs

1301 K Street, Northwest, Suite 1200  
Washington, DC 20005 3307

June 25, 1999

Honorable Henry A. Waxman  
United States House of Representatives  
Committee on Government Reform  
2157 Rayburn House Office Building  
Washington, D.C. 20515

Dear Representative Waxman:

This letter responds to your June 3 inquiry to Mr. Gerstner requesting information about IBM's policies with respect to employee medical records.

IBM's interest in this important issue comes from our role as an employer as well as a provider of information technology solutions and services. As an employer, we address medical records confidentiality both during the process of arranging for health insurance coverage, and during workplace encounters (e.g., workers' compensation and wellness programs). I trust that the material enclosed, which was recently presented in testimony, addresses your questions about our policies.

We are supportive of a federal legislative framework to address medical records privacy, and look forward to continued work in this Congress to achieve that goal.

Sincerely

A handwritten signature in cursive script that reads "Harriet P. Pearson".

Harriet P. Pearson

Enclosures

cc: Mr. Gregory Waddell

**STATEMENT OF**

**DOUGLAS WEIR, M.D.  
PROGRAM MANAGER, OCCUPATIONAL HEALTH SERVICES  
IBM CORPORATION--ESSEX JUNCTION, VERMONT**

**before the**

**HEALTH, EDUCATION, LABOR & PENSIONS COMMITTEE  
UNITED STATES SENATE**

**FIELD HEARING  
BERLIN, VERMONT**

**MARCH 15, 1999**

Thank you for the opportunity to present IBM's views on medical records confidentiality legislation. My name is Dr. Douglas Weir, and I am a physician who trained in internal medicine at the Medical Center Hospital in Burlington. For the past 15 years I have worked at the IBM facility in Essex Junction where I am currently the Program Manager of IBM Occupational Health Services.

We offer two perspectives on this very important issue: First, as the world's largest information technology company, and second, as an employer with over 150,000 employees in the United States, including over 7,000 in Vermont.

### **Technology and Medical Records Confidentiality**

IBM's Global Healthcare Industry division is a leader in providing new solutions for improving health care systems, patient responsiveness, and communications within far flung health care operations. We work with our customers--hospitals, providers, insurers, and others--to address their evolving needs and assist them in integrating new technologies into their healthcare systems. I have attached material in the Appendix to this Statement that provides more detail on our experience in this industry.

As a technology company, we see every day the role that information technology plays in improving the delivery of healthcare--and we believe that such technology can also be used to protect the privacy and security of personally identifiable information.

As a practicing physician, I can personally imagine a healthcare organization being able to access patient charts and X-rays, attach a physician progress note to an existing electronic chart via voice recognition software, and send that file across town or across country to another doctor or hospital. Patients could sit at home and view the doctor's schedule to arrange an appointment, or ask a nurse practitioner about a sick child through an Internet chat session. Even using a computer link to determine eligibility and to electronically handle a co-pay while the patient is seeing the doctor. Consumers could even use the Internet or other computer network to buy exercise equipment, or create a diet and exercise plan monitored by an online physician. Some of these are happening even now!

At the same time, technology offers many forms of security controls that can appropriately manage access to protected health information--controls that were

not possible or cost-effective in a paper-based environment. Some technology--like biometrics-- can authenticate or verify the identity of an individual in a manner that is more foolproof than a set of questions that (ironically) ask for additional personal information. Technology also enables the "de-identification" of information, so that it no longer identifies a specific individual. What that means, in the context of federal privacy legislation, is that it can create information that does not constitute "protected health information" in a manner that is viable for large volumes of healthcare records--something that was not feasible with paper. Encryption and digital signatures are additional components of the technology security portfolio that can be used to enhance the security of health information.

The tools and capabilities I've mentioned here will only get better and more sophisticated in the future, given the fast pace of technological advances. In other words, technology can help to implement the goals of this legislation.

Yet this legislation is not directed at these technology solutions, because they are largely addressed under the security standards of the 1996 Health Insurance Portability and Accountability Act's Administrative Simplification provisions, which are now being implemented by Health and Human Services. Federal medical records confidentiality legislation is directed, instead, at the policies by which organizations will establish who has access to protected information and what the right of individuals are with respect to the uses of the information.

We know as a healthcare information systems company that the only way our customers will be able to take advantage of the capabilities of the Internet and other technologies is if we can create a trusted environment where personal health information is protected. It is to this end that we support the need for and the intent of the legislation, to address this important and sensitive category of information.

### **An Employer's Perspective**

We all know that most Americans and their families receive health care coverage through their employer--whether that's a private company or a government. IBM believes that employers play a very constructive role in today's U.S. health care system and have helped bring about many of the most innovative developments in health care delivery.

Employers regularly play three distinct roles relevant to the medical privacy debate:

- ☒ Providers of health benefits and payers of health claims. Self-insured firms like IBM actively design, manage, and fund health benefits for their employees.
- ☒ Providers of emergency care when necessary, and
- ☒ Stewards of a healthy and safe workplace to promote the well-being of their employees. Employers are responsible for ensuring that a healthy and safe workplace exists at their facilities, and they underpin the nation's worker compensation system.

Employers' role is an active and central one, resulting in many positive programs that companies like IBM voluntarily undertake, such as health prevention and wellness programs.

It follows, then, that employers' benefit plans generate and use much of the health information that flows through the health care system today. In turn, we have a keen interest in the privacy debate.

To be of benefit, privacy legislation should not tie the hands of employers so severely that they lose the flexibility to perform these necessary functions. Employers need to have access to sufficient information to manage their workforce effectively and perform necessary research and analysis that requires medical information. But clearly, employees need to have assurances that the privacy of their medical records will be protected by their employers.



## IBM Privacy Policies and Practices

As an information technology company, IBM has maintained a very high standard with respect to ensuring the confidentiality of information entrusted to it. The company's interest dates back to the 1960s when our privacy policies were formalized due to our desire to respect our individual employees and a general public apprehension about the effects of computers on privacy.

In the 1970s, we conducted a comprehensive review of specific internal guidelines and began management training programs to support compliance with these guidelines.

In the 1980s, we revisited these privacy principles to test their viability given technological and social changes that had occurred and to think through the new challenges presented by these changes.

These are our privacy principles relative to employee personnel information.

- Collect, use and retain only personal information that is required for business or legal reasons.
- Provide employees with a means of ensuring that their personal information in IBM personnel records is correct.
- Limit the internal availability of personal information about others to those with a business need to know
- Release personal information outside IBM only with employee approval, except to verify employment or to satisfy legitimate purposes, such as investigatory or legal needs.

In the 1990s, and with the explosive growth of the Internet and other networked technologies, we updated our privacy policies by adopting a global online policy for our websites--take a look at our website, at *ibm.com*. And with the taking effect in October 1998 of the European Union Data Protection Directive, we are again ensuring that our policies meet the requirements of this law.

But we have never lost sight of the fundamental principles, which underlie our employee privacy policies.

These principles apply to all personal information but have particular meaning for medical information which, we believe, deserves the greatest degree of protection. Inside IBM, access to confidential medical records is limited to IBM medical staff and department personnel under their immediate supervision. They will disclose information from those records to others within IBM, but only:

- to benefits plan administrators who may review information needed for determining eligibility for benefits
- to others with a need-to-know to evaluate medical recommendations, medical restrictions and accommodations as they relate to the work environment and ability to perform the job
- to legal counsel when medical status or information is at issue or required.

All employees may obtain copies of their records from the IBM medical department. Further, with few exceptions (where required by law or legal process, or where necessary to protect the vital interests of the patient) we require our medical staffs to obtain prior approval of the employee before either disclosing or seeking confidential medical information.

Because we believe that empowered employees with knowledge of their rights is our best assurance that these rules will be followed, we publish our principles and guidelines and periodically remind the 2000+ IBM managers in the U.S. of their responsibilities.

In addition to the information which is contained in our own internally generated medical records, we recognize the need to protect employee medical information associated with our benefits programs. IBM provides a wide array of benefits to our employees, many of which involve treatment for medical conditions--our company provides coverage for over half-million employees, dependents, and retirees. Consistent with our emphasis on employee privacy, we have placed restrictions on our benefits contract administrators on how this information can be used and even what information they will pass on to us. For example, our plan administrators receive only aggregate data derived from the medical records available to the carriers which does not permit linkage of any individual employee with a particular medical condition.

We have imposed these restrictions because we believed it was important to strike the right balance between the needs of the business and the need to protect an

employee's privacy. The fact that we have been able to continue to provide our employees a broad array of medical benefits at reasonable costs while operating with these self-imposed restrictions is evidence, we believe, that maintaining high standards of confidentiality need not compromise efficiency.

## Federal Legislation Issues

IBM has for years supported federal medical record confidentiality legislation. Personally identifiable medical information is sensitive and deserving of a federal framework for the protection of its privacy and security. We commend Senator Jeffords' and Leahy's interest and leadership on this issue, and hope to continue to work with you and your staffs. We also hope that the new Congress will enact such legislation, in time for the August 1999 deadline set by the Health Insurance Portability and Accountability Act.

Such legislation should include the fundamental "fair information" principles recognized in the privacy debate: notice, access/supplementation, security, and enforcement.

Such legislation should also reflect the following:

**Strong preemption.** Legislation should establish a strong federal framework--we cannot encourage development of a sophisticated health care delivery system without national standards for information management.

**Health Information Security.** Privacy and security are closely related, but as noted previously, security standards for health information have already been enacted by Congress in 1996. Final implementing regulations from HHS are expected this year. Federal privacy legislation should not "re-legislate" these information security standards and therefore create uncertainty, delay implementation and undermine the rulemaking process.

**Flexibility.** Federal legislation that sets out uniform standards and responsibilities in this area should strive to create a flexible environment, that recognizes the need for balance of interests. It should also encourage organizations to develop innovative approaches in order to meet their compliance obligations. This flexibility should help spur innovation and minimize costs.

**Employer's Appropriate Use.** We also have a concern over judgments employers must make regarding an employee's ability to perform a job or continue to be eligible for paid or unpaid leave according to company policy. Uses of medical information provided by employees to help us make such judgments is a legitimate use, and should be accommodated in legislation (e.g., there should be no blanket prohibition of the use of information for purposes unrelated to treatment or payment). In fact, proper compliance with laws such as the

Americans with Disabilities Act and the Family and Medical Leave Act require that employers make use of personally identifiable medical information in a manner unrelated to treatment or payment

**Technology Neutrality.** While there is certainly a role for strong technology to protect the security of health information, legislation should be written in technology-neutral terms. This is to allow the flexible use of current technologies while at the same time not discouraging the development of newer alternative technologies in the future. Finally, privacy legislation should address all types of medical records, regardless of the medium.

Once again, thank you for the opportunity to share IBM's views on federal medical records confidentiality legislation. As we have an opportunity to study the legislation recently introduced, we will be very pleased to provide further input or answer questions.

**APPENDIX**

**IBM & HEALTH CARE INFORMATION TECHNOLOGY**

## **IBM Global Healthcare Industry**

404 Wyman Street

Waltham, MA 02254

(781) 895-2486

(781) 895-2235 (fax)

e-mail: [healthid@us.ibm.com](mailto:healthid@us.ibm.com)

Web Site: <http://www.solutions.ibm.com/healthcare>

## *IBM Global Healthcare Industry*

As the industry's leading provider of e-business® solutions, IBM® offers a suite of comprehensive, end-to-end technology solutions to the Healthcare Industry. In the current healthcare marketplace, networking technology now points the way to new methods of improving care systems, patient responsiveness, streamlining cost of operations and improving communications within increasingly far-flung healthcare organizations. IBM's network-enabled commerce, information sharing, management and information technology consulting combined with innovative research offer tangible benefits to healthcare organizations and their constituents.

As healthcare organizations continue to broaden their operations, often including healthcare providers, payers, pharmaceutical and other suppliers in the mix, the need for integrated, secure, scalable networks is leading healthcare organizations towards some form of Internet-based communications.

IBM offers complete solutions suitable for all network configurations: Intranets or internal networks based on local area networks and some form of e-mail and other applications, often built on the Lotus Notes® platform; Internet-based programs (Intranets) offering communications and information through websites secured through firewalls and IBM network servers designed for this use; and Extranets which connect Intranets of many organizations through secure Internet channels.

"End-to-end" network computing solutions -- from the initial consulting project to implementation and managed operations -- address the full spectrum of healthcare organizations' evolving requirements and the need to migrate healthcare systems to new technologies. IBM's 24 development laboratories worldwide work with customers on new technologies such as genomics research to design pharmaceuticals, or continuous speech technology that enables physicians to dictate reports into their computers while reading X-rays or doing a variety of tasks including referrals and other administrative functions.

E-business is the foundation of IBM's network computing offerings providing a flexible, modular approach from a basic foundation level to highly secure, advanced applications. For those customers who want to create content and establish their presence on the Web, IBM offers solutions including Lotus Notes and Domino™, HTML authoring and HTML templates, TCP/IP and related networking services, web content hosting, e-commerce functions, business recovery services, security, consulting services, and systems management. Our web site development and

content hosting services, provide healthcare organizations with a simple-to-operate, engaging set of networked applications offering quality healthcare information and services, personalized to each individual user.

Our Health Data Network provides the framework and solutions whereby payers, providers, government and others share information. The architecture is open and can scale up to support the needs of a growing networked organization. Health Data Network applications enable healthcare organizations to consolidate and access information, automate business processes, minimize redundant data re-entry and extend the useful lives of legacy systems.

Other IBM competitive-advantage healthcare business solutions include data mining to identify marketing trends or ferret out fraudulent claims, etc.; call center technology to handle customer service operations more efficiently at lower costs; mobile computing for enhanced communications with doctors, home healthcare workers, and other healthcare professionals; financial and human resources information systems; year 2000 consulting and software; systems integration and much more.

Professional Service offerings focus on meeting customer requirements which have rapidly increased in scope along with the need to create competitive advantage in a consumer-driven healthcare market environment. Healthcare organizations are looking for sophisticated assessments of Information Systems, HIPAA security readiness, business process evaluation and analysis, reengineering expertise, systems integration, advice on best-of-breed application selection, customization and implementation, ongoing support for such activities, end-user training, and managed operations such as desktop support, data centers, transaction processing, networks and other operational business processes.

Recognized as the industry's leading provider of electronic business solutions, IBM offers a suite of comprehensive, "end-to-end" technology solutions. IBM's network-enabled e-commerce, information sharing, management and information technology consulting combined with innovative research offer tangible benefits to healthcare organizations and their constituents in improved customer service, enhanced patient care and decreased operating costs.