

EDWARD J. MARKEY

7TH DISTRICT, MASSACHUSETTS

ENERGY AND COMMERCE COMMITTEE

RANKING MEMBER  
SUBCOMMITTEE ON  
TELECOMMUNICATIONS AND  
THE INTERNET

SELECT COMMITTEE ON  
HOMELAND SECURITY

RESOURCES COMMITTEE

Congress of the United States  
House of Representatives  
Washington, DC 20515-2107

2108 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-2107  
(202) 225-2836

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101  
MEDFORD, MA 02155  
(781) 396-2900

188 CONCORD STREET, SUITE 102  
FRAMINGHAM, MA 01702  
(508) 875-2900  
www.house.gov/markey

February 23, 2004

Honorable Tommy G. Thompson, Secretary  
U.S. Department of Health and Human Services  
Hubert H Humphrey Building  
200 Independence Avenue, S.W.  
Washington, D.C. 20201

Dear Mr. Secretary;

I am writing to express my concern about the lack of privacy protection that appears to be afforded to American citizens when their Protected Health Information (PHI) and related financial information is out-sourced and sent off-shore by U.S. companies or other entities.

Recent press reports suggest that many U.S. companies are allowing some of the most intimate personal data they have collected about American citizens -- the most sensitive being individually-identifiable financial and medical information -- and transferring this data to off-shore out-sourcing firms for analysis or processing. This off-shoring of data appears to be carried out by both hospitals and a wide range of companies.<sup>1</sup>

I am concerned that highly sensitive data is increasingly being made available to overseas workers for processing or analysis without the knowledge or informed consent of the American public, who does not know that their personal financial, medical and other sensitive information has been outsourced to companies in India, China, Russia, Vietnam, the Philippines, Malaysia and the Czech Republic or elsewhere that may lack adequate privacy protection environments and are effectively beyond the reach of U.S. privacy laws and regulations.

---

<sup>1</sup> Louis Uchitelle, **A Missing Statistic: U.S. Jobs That Went Overseas**, *New York Times*, October 5, 2003; Sec 1. Page 24; David Lazarus', **Bank Of America to send Tech Work & Data to India**, *San Francisco Chronicle*, October 29, 2003; Page B-1; **California Likely to ban medical data outsourcing**, *Decon Herald* November 21, 2003; Robert Westervelt, **DBAs defend against offshore outsourcing**. *SearchOracle.com*, November 24, 2003; Jay Fitzgerald, **Known around the world: Private records may be at risk**, *Boston Herald.COM Business*, November 30, 2003; Robert J. Samuelson **The Specter of Outsourcing**. *Washington Post*, January 14, 2004, A19;

<sup>2</sup> David Lazarus, **A tough lesson on medical privacy Pakistani transcriber threatens UCSF over back pay**, *San Francisco Chronicle*, October 22, 2003, Page A1.

The threat to personal privacy represented by such actions is not merely theoretical. According to press reports, last year a Pakistani woman who had been hired as a subcontractor to perform medical transcription work for a Texas company engaged as an outsourcing firm for a California hospital threatened to post sensitive patient medical records on the Internet unless she received certain payments she claimed were due to her. Press reports indicate that the Pakistani woman actually posted one file onto the Internet, demonstrating her willingness to carry out her threat if her demands were not met<sup>2</sup>.

This incident highlights the fact that information technology jobs, back office data processing and data analysis jobs, certain financial services sector jobs and some highly technical medical interpretation jobs that used to be performed by Americans, are being out-sourced to off-shore locations by companies seeking to take advantage of the dramatically lower wages available in Third World countries. I am concerned that in their rush to cut costs and increase their bottom line, these companies may be sacrificing the privacy protections American law affords to citizens by transferring sensitive information to off-shore companies that are outside of the reach of U.S. privacy law and beyond the jurisdiction of U.S. regulators.

I therefore request that you explain what steps are being undertaken by The Department of Health and Human Services to protect the privacy of personal information collected about American citizens by companies or other persons subject to your oversight and supervision. Specifically, I request your assistance and cooperation in providing responses to the following questions:

1. The Protected Health Information of an individual may be processed or analyzed internally by a HIPAA-regulated "Covered Entity" or, the processing or analysis of this information may be outsourced to an affiliated or unaffiliated party located in the U.S. or abroad during the process or providing care to the individual, processing a health insurance claim, or billing. Please provide a chart indicating which of the (i) individual and group health plans, (ii) health care clearinghouses (i.e. covered entities that process medical information between health care providers and payers) and (iii) health care providers subject to your jurisdiction (pursuant to the privacy provisions of the HIPAA Medical Privacy Rule), are currently transferring Protected Health Information to offshore or non-U.S. domiciled affiliates or subsidiaries for processing, analysis, billing, maintaining or servicing a patient, customer account, providing a product or service for a patient to a customer, or for any other purpose.
2. Please provide a chart indicating which of the (i) individual and group health plans, (ii) health care clearinghouses (i.e. covered entities that process medical information between health care providers and payers) and (iii) health care providers subject to your jurisdiction (pursuant to the privacy provisions of the HIPAA Medical Privacy Rule), transfer for use, disclosure or otherwise deliver Protected Health Information to unaffiliated third parties or unaffiliated business associates who are located offshore, for processing, analysis, billing, or any medical, non-medical or back-office purposes.
3. Under the HIPAA regulations, Covered Entities are sometimes permitted to transfer Protected Health Information to certain non-covered entities, such as the sponsors of medical research (including pharmaceutical companies) workers compensation and disability programs and for the purpose of life, disability, property, casualty, and automobile insurance coverage and benefits. It is my understanding that such non-covered entities are not required to comply with the HIPAA privacy regulations, even

though they may receive access to private health information. Please provide a chart listing the offshore non-Covered Entities that have received Protected Health Information from each of the covered entities listed in your responses to questions 1 and 2.

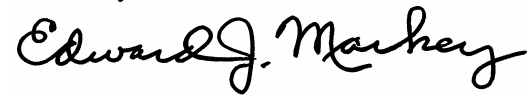
4. For each of the Covered Entities listed in your responses to questions 1, 2, and 3 please provide a chart listing the types of Protected Health Information transferred to covered and non-covered offshore affiliates, subsidiaries, unaffiliated business associates or unaffiliated third parties, including: 1) name of consumer; 2) address of consumer; 3) account numbers; 4) Social Security numbers; 5) account balances; 6) transactional or experiential information about consumer; 7) birthdate of consumer; 8) credit scoring information relating to consumer; 9) names, addresses or other information regarding spouse or dependent children of consumer; 10) medical information and 11) any other categories of commonly collected and transferred information that can be used to identify the patient or consumer.
5. For each of covered entity listed in your responses to questions 1, 2, and 3, please provide a chart indicating: 1) to what countries and to whom in these countries are the Protected Health Information of American citizens being transferred. 2) Please indicate whether the patient, parent of a minor, guardian or person acting in loco parentis was provided with a prior disclosure by the covered entity of the fact that the consumer's nonpublic Protected Health Information would be transferred to an affiliate or non-affiliated party located in a foreign country; 3) whether the implications of such a permitted use for the patient's privacy rights and enforcement of those rights are explained to the patient, client, consumer; and, 4) whether the patient, client, consumer was provided with an opportunity to receive a notice of privacy practices from the affiliate or non-affiliated party, Covered or non-covered entity located in a foreign country 5) whether the patient was provided with an opportunity to direct that such information not be disclosed – either by way of an “opt-out” or an “opt-in”. In a separate column, indicate whether the failure to provide a “notice or consent rights” is based on an exemption or any other provision of law (if so please provide citation).
6. Covered entities, as defined by the HIPAA Privacy Rules, must adhere to certain health privacy regulations. For each of the covered entities listed in your response to questions 1 and 2, please indicate how many have a defined business associate contract with all outsourcing entities, both onshore and offshore, foreign affiliates or unaffiliated business associates that guarantees or purports to guarantee to protect Protected Health Information pursuant to the HIPAA Medical Privacy Rule. What are the penalties for a failure to meet an obligation or requirement under the contract?
7. Since the issuance of the final HIPAA privacy regulations have you conducted a compliance review for all or some of the covered entities listed in your response to questions 1 and 2? If so what did you find in compliance reviews? If you have not preformed such compliance reviews please indicate what your agency has done to ensure that all covered entities are complying with the requirements of the HIPAA Medical Privacy Rule. Please supply information for compliance with in-house Protected Health Information, outsourced information and off-shored information from affiliated or non-affiliated party and business associates.
8. For each of the covered entities listed in your response to questions 1 and 2, please indicate how many inspections or examinations your agency has made since the HIPAA Medical Privacy Rule was adopted to ensure that outsourcing of nonpublic Protected Health Information to off-shore or foreign affiliates or unaffiliated third

parties or by foreign business associates of covered entity will not result in unauthorized disclosure or unauthorized access to or misuse of such information.

9. For each of the covered entities listed in your response to questions 1 and 2, please indicate whether any enforcement actions have been undertaken by your agency to address possible violations of the HIPAA privacy provisions.
10. The privacy of Protected Health Information has been recognized by many countries, such as in the European Union. Please provide a chart listing those countries that have medical privacy laws or regulations (and effective enforcement mechanisms) that you have determined meet or exceed the requirements of the HIPAA Medical Privacy Rules. If you have made such determinations, please indicate the basis for doing so. Do such laws provide any protections for the health information of American citizens that is outsourced to that country for processing or analysis? If so, what protections are provided and how do they compare to those available in the U.S.
11. It would appear financial institutions are not considered to be a Covered Entity under HIPAA, but are instead subject to privacy, confidentiality, and security requirements established pursuant to a business associate agreement that these firms may reach with a HIPAA-Covered Entity. How does HHS ensure that such agreements are fully consistent with the purposes and intent of the HIPAA privacy requirements? Does HHS conduct any examinations, inquiries or investigations to verify that a financial institution serving as a business associate of a HIPAA regulated Covered Entity is complying with its privacy obligations? What if this business associate analyzes or processes health care information offshore, either directly or through a subcontractor? Would HHS view that action as being consistent with HIPAA?
12. In the event that an offshore affiliate or subsidiary of a Covered Entity or a non-affiliated business associate of such a covered entity violated any of the HIPAA privacy provisions, what authority would your agency have to bring legal action against such covered entities or the offshore entity? What authority would you have to bring an enforcement action against a rogue employee of such a company for violations committed in foreign countries? What authority would you have to bring an enforcement action against a rogue employee of such a company for violations committed in foreign countries?
13. What rights and remedies under U.S. law would be available to a U.S. citizen whose privacy had been compromised or violated by the offshore entity or person who obtained access to their Protected Health Information as a business associate of a Covered Entity? What rights and remedies would a U.S. citizen have to seek redress against a rogue employee of an offshore company for privacy violations committed in foreign countries? How do these rights and remedies compare to those available to the citizen if their Protected Health Information is maintained entirely within the U.S.?
14. Given the constraints on your agencies' ability to supervise, regulate, examine and inspect, or undertake enforcement actions against non-U.S. persons, companies, or business associate domiciled offshore, do you believe that a prohibition or other severe limitations should be placed on the ability of U.S. firms to transfer Protected Health Information about American consumers to such foreign entities or persons? If not, why not? If so, will your agency ensure protection of the American patient, client, consumer and the protected health and financial information contained in the medical record?

Thank you for your assistance in providing responses to these questions. If you have any questions about this inquiry, please feel free to have your staff contact Dr. Michael Bailey or Mr. Jeffrey S. Duncan of my staff at 202-225-2836.

Sincerely,

A handwritten signature in black ink that reads "Edward J. Markey". The signature is written in a cursive style with a large, prominent "E" and "M".

Edward J. Markey  
Member of Congress