

COMMITTEES

ENERGY AND COMMERCE  
SUBCOMMITTEE ON  
TELECOMMUNICATIONS AND  
THE INTERNET  
CHAIRMAN

SELECT COMMITTEE ON  
ENERGY INDEPENDENCE AND  
GLOBAL WARMING  
CHAIRMAN

HOMELAND SECURITY

NATURAL RESOURCES

EDWARD J. MARKEY  
7TH DISTRICT, MASSACHUSETTS

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

<http://markey.house.gov>

March 24, 2008

The Honorable Michael Leavitt  
Secretary  
Department of Health and Human Services  
200 Independence Avenue SW  
Washington, DC 20201

Dear Secretary Leavitt:

According to a report in today's Washington Post ("Patients' Data on Stolen Laptop", March 24, 2008, A1), a government laptop containing sensitive medical information on 2,500 patients participating in a study conducted by the National Institutes of Health (NIH) was stolen last month. The report indicates that the information, which included patients' names, medical diagnoses, and other personally-identifiable data, was not encrypted, despite government information security requirements that mandate encryption in such circumstances. I am concerned about the lack of appropriate security safeguards in this instance and the apparent delay in notification of individuals whose information was breached. Accordingly, I would appreciate the Department's responses to the questions that follow.

- (1) Why was the information contained on the laptop not encrypted? What steps will the Department take to ensure that, in cases where government policy requires encryption, all personally-identifiable information maintained by the Department and its contractors is secured using encryption or other technologies that render the information indecipherable to unauthorized users in compliance with federal requirements?
- (2) Why were individuals whose personal information was breached as a result of the laptop theft not immediately notified? Why did Department officials not report the breach to National Heart, Lung and Blood Institute (NHLBI) Institutional Review Board until six days after the theft?
- (3) According to the Post report, the NHLBI Institutional Review Board chairman stated that the board's decision to delay notification to affected individuals "may or may not have been appropriate." Do you agree the delay was appropriate? If yes, why? If not, why not?
- (4) The Office of Management and Budget (OMB) has mandated that federal agencies encrypt sensitive personally-identifiable information on portable electronic devices unless a senior agency official certifies that the device does not contain such sensitive information. Was such a certification made in this case? If yes, when was the certification made and by whom?

- (5) What assistance will the Department provide individuals whose personal information was breached as a result of the laptop theft – e.g., toll-free hotline to answer patient questions, free credit monitoring, etc.?
- (6) For each of the past three years, please provide details on each instance in which sensitive personal data such as individuals' names, addresses and medical information maintained by the Department or its contractors was lost or stolen. In each instance: list the date the breach was discovered; how many individuals were affected as a result of the breach; whether these individuals were notified (if they were notified, when the notification was made, and if they were not notified, why not?); and what measures the Department implemented in response to each breach to reduce the likelihood that such a breach would recur in the future.

Medical information is among the most sensitive data that individuals have about themselves. Failure to appropriately secure patient records can have serious consequences for these patients, and when the Department does not appropriately safeguard sensitive medical information as part of research studies, it not only violates the trust of study participants but also can undermine efforts to enroll participants in future studies important to public health and research.

Please provide answers to the questions above within 15 business days, or no later than April 14, 2008. If you have questions about this request, please have a member of your staff contact Mark Bayer of my staff at 202-225-2836.

Sincerely,



Edward J. Markey