

Congress of the United States
House of Representatives
Washington, D.C. 20515

October 1, 2009

The Honorable Kathleen Sebelius
Secretary
United States Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Madam Secretary:

We are deeply concerned about the high bar that the Department of Health and Human Services (HHS) has set for notification of individuals in the case of an unauthorized use or disclosure of personal health information in its August 24, 2009 interim final regulations on Breach Notification for Unsecured Protected Health Information promulgated pursuant to the American Recovery and Reinvestment Act of 2009 (ARRA). This is not consistent with Congressional intent.

ARRA included provisions promoting health information technology (HIT) as a foundation for quality and efficiency improvements in the U.S. healthcare system. However, these benefits can be fully realized only with the inclusion of strong safeguards that protect the privacy and security of individuals' personal health information. To gain the public trust, it is imperative that there is effective implementation of those provisions by HHS.

Section 13402 of ARRA requires health care entities to notify individuals if there is an "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information." In its interim final rule, HHS interpreted the term "compromises" to include a substantial harm standard. If the breaching entity decides there is no significant risk of financial, reputational or other harm to the individual, that provider or health insurer never has to notify their patients that their sensitive health information was used or disclosed in violation of the federal privacy rule.

ARRA's statutory language does not imply a harm standard. In drafting Section 13402, Committee members specifically considered and rejected such a standard due to concerns over the breadth of discretion that would be given to breaching entities, particularly with regard to determining something as subjective as harm from the release of sensitive and personal health information.

In fact, during development towards final policy, the Committee on Energy and Commerce released a discussion draft of health information technology and privacy legislation in

The Honorable Kathleen Sebelius
October 1, 2009
Page 2

May of 2008. In that draft, in addition to a definition of breach similar to that used here, the language specifically included a harm standard that was later rejected. The discussion draft only required patients to be notified if the unauthorized use of personal health information could “reasonably result in substantial harm, embarrassment, inconvenience or unfairness to the individual.”

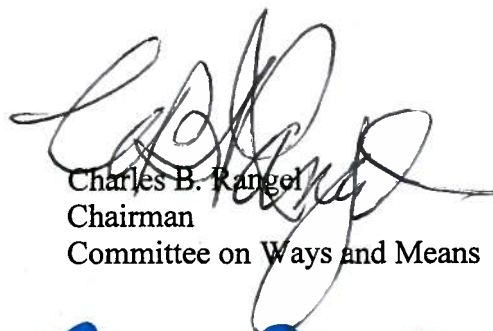
Members considered the comments they received, the practices of States, and ultimately decided against inclusion of a harm standard. Instead, Members reported and passed legislation that has a black and white standard for notification with a safe harbor for information that is rendered unusable, unreadable, or indecipherable to unauthorized individuals, and other specific exceptions. The primary purpose for mandatory breach notification is to provide incentives for health care entities to protect data, such as through strong encryption or destruction methodologies and to allow individuals to assess the level of unauthorized use or disclosure of their information. Such transparency allows the consumer to judge the quality of a health care entity’s privacy protection based on how many breaches occur, enabling them to choose entities with better privacy practices. Furthermore, a black and white standard makes implementation and enforcement simpler.

We urge HHS to revise or repeal the harm standard provision included in its interim final rule at the soonest appropriate opportunity. We hope to work more closely with the agency on future privacy regulations and request this letter be submitted as part of the official comments (reference number RIN 0991-AB56). Thank you for your ongoing commitment and attention to protecting Americans’ health information privacy.

Sincerely,



Henry A. Waxman
Chairman
Committee on Energy and Commerce



Charles B. Rangel
Chairman
Committee on Ways and Means



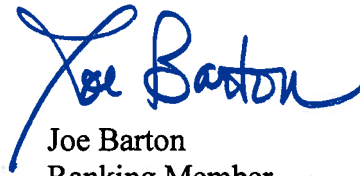
John D. Dingell
Chairman Emeritus
Committee on Energy and Commerce



Frank Pallone, Jr.
Chairman
Subcommittee on Health
Committee on Energy and Commerce



Pete Fortney Stark
Chairman
Subcommittee on Health
Committee on Ways and Means



Joe Barton
Ranking Member
Committee on Energy and Commerce