

OFFICE OF INSPECTOR GENERAL

Date: March 9, 2009

To: Glen Egelman, Director, Office of Medical Services
Garry Stanberry, Acting Associate Director, Office of Management

From: Kathy Buller, Inspector General

CC: Jody Olsen, Acting Director

Subject: Management Implication Report: Unnecessary Use of Social Security Numbers on Agency Forms

Recent breaches in personal identifiable information necessitate that the agency make changes in how such information is handled by the Peace Corps. The manner in which the Office of Medical Services' (OMS) currently collects and disseminates Volunteer applicant medical information has resulted in Volunteer applicant information being sent to the wrong individuals. Specifically, in 2008, pre-service unit assessment officials in OMS mailed personal identifiable information, including social security numbers, on medical inquiry forms and/or medical data to the wrong applicants on more than one occasion. These breaches in confidential data have been attributed to human error.

On June 18 2007, the Office of Personnel Management issued federal guidance on protecting social security numbers and combating identity theft by eliminating the unnecessary use of social security numbers. Peace Corps and other agencies were tasked with reviewing their processes to identify instances in which the collection or use of the social security number is superfluous. In addition, the Office of Management and Budget (OMB) mandated that agencies reduce the volume of information they possess, the risks to the information, and the burden of safeguarding it by collecting only necessary information and managing it properly. Under current federal requirements issued by OMB, the Office of Inspector General (OIG) is tasked with independently evaluating the effectiveness of its agency's programs.

The OIG issued an audit report (Audit of the Safeguarding of Social Security Numbers, IG 05-04-A) regarding the Peace Corps's use of social security numbers on March 5, 2005. Despite report findings that Peace Corps needed to better safeguard social security numbers it collected, a follow-up audit performed two years later (Follow-up Report Audit: Safeguarding of Social Security Numbers, IG-07-10-FUA) disclosed that none of the OIG recommendations had been adequately addressed. Furthermore, the OIG follow-up audit found that: (1) there has not been a coordinated effort to review agency forms since March 2006; (2) the Office of Management did not develop a current records inventory list to assess the agency's use of social security numbers and other personal

identifiable information; and (3) individual offices were never given guidance to gauge appropriate uses of social security numbers on individual forms and documentation. Of chief importance, Peace Corps' Office of Management's review of forms that included social security numbers as identifiers failed to eliminate agency-wide use of these numbers; and the review of forms used by the Office of Medical Services was never completed.

In 2008, OMS officials in the pre-service assessment unit forwarded medical forms with personal identifiable information including social security numbers to the wrong applicant on three separate occasions. In addition, a medical lab report was attached to the wrong authorization form and was then forwarded to the wrong individual. Based upon the lab report, the individual scheduled an unnecessary evaluation with her physician. Human error was attributed to each of these four breaches of personable identifiable information. In each of these instances, the individuals were informed that their social security numbers and/or other personable identifiable information had been sent to other parties. Due to the potential exposure and/or loss of personal identifiable information, the aforementioned breaches were reported to the United States Computer Emergency Readiness Team (US CERT), Office of Homeland Security.

The OIG investigation of breaches of personal identifiable information that occurred in 2008 found that a Volunteer applicant's telephone number and social security number appear at the bottom of several routinely used medical application forms, e.g., follow-up letters requesting additional medical information from applicants as well as instructions and reimbursement information for the examining physician. To date, the OIG has not seen evidence that OMS has taken steps to mitigate exposure, and protect against any future breaches. OMS has not implemented internal control procedures to address the cause of these problems. The OIG also identified the following findings associated with OMS's current breaches in social security information and other identifiable personal identifiable data:

- OMS unnecessarily displays social security numbers on medical forms; all Trainee/Volunteer candidates routinely receive medical forms which have their social security number and telephone number as identifiers.
- OMS has not developed written procedures for the proper labeling, storage, and disposal of printed material containing social security numbers and other personal identifiable data.
- OMS has not implemented internal control procedures to ensure the proper handling, disseminating, and monitoring of social security numbers and other personal identifiable information.
- The physical space where the pre-service unit processes information does not have adequate restrictions to external exposure/interference.

While some corrective actions may have already been implemented, we request management to review OMS operations to reduce or eliminate the use of social security numbers as identifying information and provide better accountability and efficiency in the control of personal identifiable data and medically confidential data. We also request that OMS take action to ensure that the inappropriate disclosure of personally identifiable information due to human error is appropriately addressed.

Within 30 days, please report to the OIG any and all changes that will be implemented based on our investigative findings.