MS 899 Breach Notification Response Plan

Effective Date: August 1, 2016
Responsible Office: M/FOIA & Privacy Office
Supersedes: 01/28/13; 01/7/13; 07/23/08

Issuance Memo (08/01/2016)
Issuance Memo (01/28/2013)
Issuance Memo (01/07/2013)
Issuance Memo (07/23/2008)

Attachment A - 2006 OMB Memo

1.0 Purpose

The purpose of this Manual Section is to set out Peace Corps policy regarding actions that should be taken when Personally Identifiable Information in the possession or control of the Peace Corps has been compromised. This policy covers incident reporting, incident response, the breach notification response team, external notification of breaches, training requirements, and consequences of breaches by staff. This Manual Section constitutes the Peace Corps Breach Notification Response Plan (Breach Plan).

2.0 Authorities

Executive Order 13402, May 2006; Office of Management and Budget (OMB) Memorandum, September 20, 2006, *Recommendations for Identity Theft Related Data Breach Notification;* OMB Memorandum, May 22, 2007, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, and 45 CFR Part 160 and 164 (Breach Notification for Unsecured Protected Health Information)

3.0 Definitions

3.1 ***Personally Identifiable Information*** is information that can be used to distinguish or trace an individual's identity, such as his or her name, Social Security Number, or biometric records, alone or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name.

3.2 ***Covered Information*** means Personally Identifiable Information that poses a risk of identity theft. Covered Information includes, at a minimum, the following information, whether on paper, in electronic form, or oral communication:

(a) An individual's Social Security Number alone; or

(b) An individual's name, address, or phone number in combination with one or more of the following: date of birth, Social Security Number, driver's license number, other state identification number or foreign country equivalent, passport number, or financial account number or credit or debit card number.

3.3 ***Medically Confidential Information*** for the purposes of this Manual Section means oral or written information relating to the past, present or future health, condition, care or treatment of a Peace Corps applicant, Trainee or Volunteer created or received by the Office of Health Services, a Peace Corps Medical Officer (PCMO) or other Peace Corps health care provider. It also includes information relating to the past, present or future payment for such care.

3.4 ***Breach and/or Incident*** means loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to Personally Identifiable Information or Covered Information, whether physical or electronic.

In the context of Medically Confidential Information, a breach is the acquisition, access, use or disclosure of an individual's Medically Confidential Information in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPPA) that poses a significant risk of financial, reputational, or other harm to the individual.

3.5 ***Response Team*** means one or more of the following supervisory groups (collectively the Response Teams) that may be involved in responding to breaches of Personally Identifiable Information:

(a) ***Core Response Team*****.** Used when a breach of Personally Identifiable Information [physical records, such as paper files, documents and reports,] involves a limited number of individuals and a limited amount of breached Personally Identifiable Information. The Core Response Team should, at a minimum, include:

(1) Chief Privacy Act Officer (Associate Director for Management);

(2) Chief Information Officer;

(3) General Counsel;

(4) Associate Director for Safety and Security;

(5) Manager of the program office experiencing the breach; and

(6) Privacy Officer.

(b) ***Full Response Team.*** This Response Team is used when there is a major breach involving a large amount or significant types of Personally Identifiable Information. It includes:

(1) Chief Privacy Officer;

(2) Chief Information Officer;

(3) General Counsel;

(4) Associate Director of the Office of Safety and Security;

(5) Manager of the program or the office experiencing the breach;

(6) Privacy Officer;

(7) Director of the Office of Communications;

(8) Director of the Office of Human Resource Management;

(9) Director of the Office of Congressional Relations;

(10) Associate Director of Global Operations;

(11) Chief Compliance Officer;

(12) Chief Financial Officer; and

(13) Associate Director of the Office of Health Services in breaches involving Medically Confidential Information shall be included.

Note that in cases involving breaches of Personally Identifiable Information in electronic records and assets, the Office of Chief Information Officer may employ the Incident Response Team generally made up of IT security specialists supplemented by representatives from other offices, as more fully described in the Incident Response Plan. The Incident Response Team is not a Response Team as defined under this Manual Section, nor does it have direct responsibilities under this Manual Section, unless specifically noted or unless assigned by the Core Response Team or the Full Response Team.

4.0 Policies

(a) All employees, contractors, and Volunteers shall immediately report any suspected or known breach of Personally Identifiable Information, Covered Information and/or Medically Confidential Information (whether paper and/or electronic) and follow the rules set out in this Manual Section.

(b) The Breach Plan policies are supplemented by the requirements for reporting and handling breaches of electronic records and assets under the Incident Response Plan.

(c) Breach Plan requirements and responsibilities shall, as appropriate, be included in Peace Corps contracts and agreements to ensure that experts, personal services contractors, and other contractors who use, access, or handle Personally Identifiable Information are similarly informed and held accountable.

5.0 Roles and Responsibilities

5.1 Response Teams

(a) In order to ensure an adequate response to a breach, the Peace Corps has identified certain individuals who will be part of the Response Teams that address a breach. The responsibilities of the teams are to determine how to respond to a breach. The nature and potential impact of the breach determines whether the Core Response Team or the Full Response Team should be involved.

(b) The Response Team's mission is to provide planning, guidance, analysis, and a recommended course of action in response to a breach. In the event of a breach, the Response Team will be convened promptly to conduct a risk analysis to determine whether the breach poses risks related to identity theft or other harms and will implement a timely, risk-based, tailored response to each breach.

(c) The Response Team will be convened to evaluate any potential breach and to help guide the Peace Corps' response. The Response Team should include staff with expertise in information technology; legal authorities, including law enforcement; the Privacy Act; or other area of expertise necessary to respond to a breach.

(d) The Response Team will coordinate with other Peace Corps offices, as appropriate, to ensure that appropriate risk-based, tailored responses to data breaches are developed and implemented. Responding to a particular breach will likely require assistance from the managers and staff of the office or program that experienced the breach. The Response Team will coordinate actions with the Incident Response Team when there has been a breach of Personally Identifiable Information contained in electronic records or assets.

(e) The Response Team will work closely with other federal agencies, offices, and teams, as appropriate.

(f) If there has been breach of Personally Identifiable Information of a staff member or Volunteer, which was provided to the Peace Corps and then transmitted to another federal agency, the Response Team will monitor the remedial action taken by such agency and, as appropriate, the notifications made by the agency to affected parties.

5.2 Office of the Chief Information Officer

The Office of the Chief Information Officer will take all necessary steps to contain, control, and mitigate the risks from a breach involving information contained in IT systems and prevent further unauthorized access to or use of individual information, including as appropriate: (1) monitoring, freezing, or closing affected Peace Corps accounts; (2) modifying computer access codes; and (3) taking other necessary and appropriate action. Without undue delay, the Chief Information Officer shall take steps consistent with current requirements under the Federal Information Security Management Act (FISMA).

5.3 Office of Management/Chief Privacy Officer

The Chief Privacy Officer is responsible for:

(a) Serving as the Chair of the Response Team, presiding over meetings and initiating responses to incidents as appropriate.

(b) Participating in all phases of the Peace Corps planning, preparation, investigation, and response to breaches involving Personally Identifiable Information and Covered Information.

(c) Where there is a breach, with the assistance of the Office of Safety and Security, ensuring that necessary steps are taken to contain and control the breach and prevent further unauthorized access to or use of individual information. Such steps may include changing locks; deactivating facility access cards; enhancing physical security measures; alerting the Federal Protective Service; and/or developing or implementing special instructions, reminders, or training.

(d) Determining whether the Response Team should review the reported incident to determine any other appropriate Peace Corps response.

5.4 Privacy Act Officer

The Privacy Act Officer will provide subject matter expertise and operational support in analyzing and responding to a suspected or actual breach.

5.5 Office of Safety and Security

The Office of Safety and Security is responsible for the restriction of physical access to Peace Corps space through the revocation of facility access cards and/or keys as appropriate. The Office of Safety and Security is also responsible for the operation of the Insider Threat Program. See MS 404 *Insider Threat Program*.

5.6 Office of the General Counsel

The Office of the General Counsel is responsible generally for providing legal support and guidance in responding to a suspected or actual breach.

5.7 Office of Inspector General

The role of the Office of Inspector General is to provide oversight over the agency's incident response and investigate breaches when appropriate. The Office of Inspector General reviews the Incident Response Report and any other relevant information to independently evaluate the Peace Corps response to a breach. Additionally, the Inspector General must independently evaluate the Peace Corps response to a breach. When applicable, the Inspector General, in accordance with responsibilities set forth in the Inspector General Act, may initiate an investigation of a breach. To report an incident to the OIG, an employee, contractor or Volunteer

should call the OIG hotline numbers at 202-692- 2915, or 800-233-5874, via email or the IG's web based form.

6.0 Response Actions

6.1 Initial Notification of Breach

(a) **Domestically.** When there is a suspected or known breach domestically, a domestic staff member or contractor shall promptly notify the Domestic Service Desk by calling +1-202-692-1000.

(b) **Overseas.** When there is a suspected or known breach overseas, a staff member, contractor, or Volunteer shall notify the post's IT specialist. The IT specialist shall promptly notify the Domestic Service Desk by calling +1-202-692-1000.

6.2 Incident Response Report

(a) Upon notification of an incident, the Domestic Service Desk shall fill out the top portion of the Incident Response Report (located on the Office of IT Security intranet webpage) and assign the incident to the Office of IT Security queue.

(b) After receiving the Incident Response Report, the Incident Response Coordinator in the Office of the Chief Information Officer will complete the Incident Response Report and forward it to: the Chief Privacy Officer, the Privacy Officer, and the Inspector General. The Incident Response Coordinator should forward the Incident Report to the U.S. Computer Emergency Readiness Team (U.S.-CERT) for external reporting as soon as possible after the first notice of the suspected or confirmed breach.

6.3 Convening the Response Team

Within 24 hours of being notified of an incident involving or potentially involving Covered Information, Personally Identifiable Information or Medically Confidential Information, the Chief Privacy Officer should, as appropriate, convene a meeting of the Core Response Team or the Full Response Team.

The Response Team should evaluate the available information to help determine whether data has been compromised or potentially compromised and how to respond.

As part of the initial evaluation, the following issues should be investigated:

(a) Date of incident;

(b) Nature of incident and the means by which the breach occurred;

(c) Unauthorized access to information;

(d) Unauthorized use of information;

(e) Lost computer, storage device, or portable media;

(f) System or network intrusion;

(g) Loss of control of paper documents containing sensitive information;

(h) Person who reported the incident;

(i) Person who discovered the incident;

(j) Number of individuals potentially affected; and

(k) The accessibility of the information.

6.4 Breach of Electronic Information

If an incident appears to involve the unintentional loss of control or disclosure of Personally Identifiable Information, Covered Information, or Medically Confidential Information, which is in electronic records and assets, the OCIO shall have primary responsibility for conducting an inquiry into the circumstances surrounding the loss.

6.5 Determining Whether Notification is Required for Personally Identifiable Information

To determine whether notification of a breach to potential victims is required, the Response Team will assess the likely risk of harm caused by the breach and the level of risk. To assess the likely risk of harm, the following factors should be considered:

(a) **Nature of the Data Elements Breached.** The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. The data elements should be considered in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals;

(b) **Number of Individuals Affected.** The magnitude of the number of affected individuals may dictate the method(s) chosen for providing notification, but should not be the determining factor for whether an agency should provide notification;

(c) **Likelihood the Information is Accessible and Usable.** Upon learning of a breach, the Agency should assess the likelihood that Personally Identifiable Information will be or has been used by unauthorized individuals. The Response Team should consider whether the information has been encrypted, for example;

(d) **Likelihood the Breach May Lead to Harm.** The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the types of data involved in the incident; and;

(e) **Ability of the Peace Corps to Mitigate the Risk of Harm.** The risk of harm will depend on how the Peace Corps is able to mitigate further compromise of the systems affected by

the breach. In addition to containing the breach, countermeasures, such as monitoring the misuse of Personally Identifiable Information and patterns of suspicious behavior, should be taken.

6.6 Determining Whether Notification is Required for Medically Confidential Information

For Medically Confidential Information, an individual shall be notified where disclosures not authorized under HIPAA regulations pose a significant risk of financial, reputational or other harm to the individual.

6.7 Determining if Breach Causes Identity Theft Risks

To determine if a breach causes identity theft risks, the Response Team should evaluate the factors identified in the 2006 OMB Memo (Attachment A)**.** These factors include:

(a) The type of Covered Information that was compromised;

(b) How easy or difficult it would be for an unauthorized person to access the information given how it was protected;

(c) The means by which the loss occurred, including whether the incident might be the result of criminal activity or is likely the result of criminal activity;

(d) The ability of the Peace Corps to mitigate the identity theft; and

(e) Evidence that the compromised information is actually being used to commit identity theft.

6.8 Other Potential Harms

Even if there is no risk of identity theft, the Response Team shall consider a wide range of potential harms and determine whether external notification of a breach is necessary. The Privacy Act requires the Peace Corps to protect against any anticipated threats or hazards to the security or integrity of records, which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Additionally, the Response Team may consider a number of possible harms associated with the loss or compromise of information. For example, such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, and the potential for secondary uses of the information which could result in fear or uncertainty.

Notification of a breach involving Medically Confidential Information is required where there is a significant risk of financial, reputational or other harm to the individual.

6.9 Impact Levels

The Response Team should also review and assess the level of impact already assigned to the information using the impact levels defined by the National Institute of Standards and Technology (NIST). The three impact levels (low, moderate, and high) describe the potential impact on an organization or individual if a breach of security occurs.

(a) **Low:** the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals;

(b) **Moderate:** the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals; and

(c) **High:** the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

6.10 Ability of the Agency to Mitigate the Risk of Harm

Within an information system, the risk of harm will depend on how Peace Corps is able to mitigate further compromise of the information and/or system(s) affected by a breach. In addition, countermeasures to contain the breach or its impacts should be considered. This could include monitoring other appropriate systems for misuse.

6.11 Notification

6.11.1 Delaying Notification of Individuals

Notification where there is little to no risk of harm might create unnecessary concern and confusion. Under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

6.11.2 When Notification is Appropriate

If the Response Team determines that notification of the breach is appropriate, it shall consider the following factors:

(a) **Timing of Notification.** A notification will be issued without unreasonable delay following the discovery of a breach, consistent with the needs of law enforcement, including the OIG, national security, and any measures necessary for the Agency to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised. Decisions to delay notification will be made by the Director of the Peace Corps or his or her designee, in writing. In some circumstances, law enforcement or national security considerations may require a delay if it would seriously impede the investigation of the breach or the affected individual. However, any delay should not exacerbate risk or harm to any affected individual(s).

Notifications in the context of Medically Confidential Information must be made within 60 days of discovery of the breach;

(b) **Source of Notification.** Notification to individuals should generally be issued by the Director or a senior-level individual designated by the Director, in writing; and

(c) **Contents of the Notice.** The contents of the notice given by the Peace Corps to individuals shall include the following:

(1) A brief description of what happened, including the date(s) of the breach and of its discovery

(2) To the extent possible, a description of the types of personal information that were involved in the data security breach (e.g., full name, SSN, date of birth, home address, account number, disability code, etc.);

(3) A statement whether the information was encrypted or protected by other means, when it is determined by the FOIA/Privacy Office or the IT Security staff, that such information would be beneficial and would not compromise the security of the system;

(4) What steps individuals should take to protect themselves from potential harm, if any;

(5) What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and

(6) Who affected individuals should contact at the agency for more information, including a toll-free telephone number, e-mail address, and postal address.

(d) **Means of Notification.** The best means for notifying affected individuals or others will depend on the number of individuals affected and the available contact information. The means used should be commensurate with the number of people affected and the urgency with which they need to receive notice. Among possible means are:

(1) Telephone - if used, it should be in conjunction with first-class mail notification;

(2) First-Class Mail - to the last known mailing address in Agency records. This should be the primary means of notification;

(3) E-Mail - can be used in conjunction with other methods. If the only available contact information is an e-mail address, then use this;

(4) Existing government-wide services, such as www.USA.gov and 1-800-FedInfo;

(5) Newspapers or other public media outlets, including call centers;

(6) Substitute Notice - where individual contact information is unavailable, posting on websites and using print and broadcast media may be appropriate. This should include a toll-free number where individuals can find out whether their information is included in the breach; and

(7) Accommodations - Special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973 should be given.

6.11.3 Notification to Third Parties

(a) Notice to individuals and to third parties, including the timing, order, and content of such notice, shall be carefully coordinated so that ongoing investigations are not compromised, the risk of harm to individuals is minimized, and the information provided is consistent and accurate. Notice to the following third parties may be considered depending on the nature of the breach and the following:

(1) **Media and the Public.** The Director of the Office of Communications, in coordination with the Response Team, and with approval from the Director's office, is responsible for directing all meetings and discussions with the news media and the public. This includes the issuance of press releases and related materials on the Agency's website.

(2) **Financial Institutions.** If the breach involves government-authorized credit cards, the Peace Corps must notify the issuing bank promptly as set forth in the 2007 OMB Memo. The Response Team shall coordinate with the OCFO regarding such notification and suspension of the account. If the breach involves individuals' bank account numbers that are used in employment or volunteer-related transactions, the Peace Corps will notify the bank or other entity that handles that particular transaction for the Agency.

(3) **Appropriate Members of Congress.** The Office of Congressional Relations, in consultation with the Response Team, is responsible for coordinating all communications and meetings with members of Congress and their staff.

(b) If communicating with third parties regarding a breach is necessary, the Peace Corps will consider the following:

(1) **Careful Planning.** The Peace Corps' decision to notify the public media will require careful planning and execution so that it does not unnecessarily alarm the public or undermine any OIG coordination with law enforcement or prosecutorial entities. When appropriate, public media should be notified as soon as possible after the discovery of a breach and the response plan, including the notification, has been developed. Notification should focus on providing information, including links to resources, to aid the public in its response to the breach. Notification may be delayed upon the request of law enforcement or national security agencies. To the extent possible, when necessary prompt public media

disclosure is generally preferable because delayed notification may erode public trust;

(2) **Web Posting.** The Chief Privacy Officer will generally post information about the breach and notification in a clearly identifiable location on the home page of its web site as soon as possible after the discovery of a breach and the decision to provide notification to the affected individuals. The posting may include a link to Frequently Asked Questions (FAQ) and other talking points to assist the public's understanding of the breach and the notification process. The information could, if appropriate, also appear on the www.USA.gov web site;

(3) **Notification of other Public and Private Sector Agencies.** Other public and private sector agencies may need to be notified on a need-to-know basis, particularly those that may be affected by the breach or may play a role in mitigating the potential harm stemming from the breach.

(4) **Notification to the Department of Health and Human Services**. The Privacy Act Officer shall notify the Department of Health and Human Services:

(i) at the same time that individuals are notified where the breach affects more than 500 people; and

(ii) by March 1 of each year, with a log of all of the breaches occurring during the previous calendar year.

Such notifications must be provided as specified on the DHHS website.

6.11.4 Documentation of Breach Notification Response

The Response Team, in coordination with the Records Management Office, OGC, and any other appropriate officials and staff, shall ensure that appropriate and adequate records are maintained to document the Response Team's response to all breaches reported under this plan. Such records shall be destroyed only in accordance with the General Records Schedule.

6.12 Evaluation of Breach Response

The development and implementation of this Breach Plan is an ongoing process, not a one-time exercise. Accordingly, following the handling and disposition of all suspected or actual breaches reported under this plan, the Response Team will evaluate its response, identify tasks that could have been conducted more effectively and efficiently, and make improvements or modifications to the Breach Plan as appropriate.

The Response Team will meet regularly when an incident takes place and meet once per year to discuss employee training and the status of data breaches at the Peace Corps.

7.0 Training

The Privacy Act Officer will train managers, supervisors, employees, and contractors regarding their responsibilities for safeguarding Personally Identifiable Information. For example:

(a) Staff member and contractors will be trained on how to respond to and report a potential or confirmed data breach;

(b) Formal incident response procedures shall be part of the Peace Corps' mandatory annual IT security awareness and privacy training;

(c) Supervisors will attend privacy awareness training sessions during the Human Resource Management sponsored supervisor training and overseas training programs held at headquarters; and

(d) Privacy awareness training will be included as part of new employee orientation.

8.0 Disciplinary Action

Any Peace Corps employee who has been trained and does not meet his or her responsibilities to safeguard Personally Identifiable Information may be subject to appropriate disciplinary action. Responsibilities that may lead to disciplinary action include failure to implement and maintain security controls for personally identifiable information, for which an employee is responsible, regardless of whether the employee causes the loss of control or unauthorized disclosure of personally identifiable information; exceeding authorized access to, or disclosure to unauthorized persons of, personally identifiable information; failure to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information; and for managers, failure to adequately instruct, train, or supervise employees in their responsibilities.

Any contractor who has been trained and does not meet his or her responsibilities to safeguard Personally Identifiable Information may be subject to action consistent with the terms of the relevant contract. Any temporary employee or expert consultant who has been trained and does not meet his or her responsibilities to safeguard Personally Identifiable Information may be subject to termination of their appointment.

9.0 Effective Date

The effective date is the date of issuance.