Suggest the following changes to OTSG/MEDCOM Policy Memo 09-021, 7 April 2009, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures

1. Add at paragraph 1.i.: Federal Register, Vol. 74, No. 162, 24 August 2009, Rules and Regulations, page 42767, 45 CFR Parts 160 and 164, Breach Notification for Unsecured Protected Health Information; Interim Final Rule.

2. Add after the first sentence at paragraph 5. c. (2)(c )(3)(b): If the organization knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

3. Change the sentence at 5.c.(2)(c )(3)(d)(7) to read: Who the affected individuals should contact at the agency for more information, including a toll free phone number, email address, and postal address.

4. Add at paragraph 5.c.(2)(c )(4): In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.

(a) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(b) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(1) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the organization involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(2) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

5. Add at paragraph 5.c.(2)(c )(5): Notification to the media. For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, an organization shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction.

6. Add at paragraph 5.c.(2)(d): Notification to the Secretary, Health and Human Services (HHS). An organization shall, following the discovery of a breach of unsecured protected health information, notify the Secretary, HHS in a manner specified on the HHS web site (http://www.hhs.gov/ocr/privacy/). HHS has posted links for online forms http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html for covered entities to report breaches.

(a) Breaches involving 500 or more individuals. For breaches of unsecured protected health information involving 500 or more individuals, an organization shall provide notification in the manner specified on the HHS web site

(b) Breaches involving less than 500 individuals. For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification for breaches occurring during the preceding calendar year, in the manner specified on the HHS web site.

7. Add at paragraph 5.c.(2)(e): Notification by a business associate.

(1) A business associate shall, immediately following the discovery of a breach of unsecured protected health information, notify the organization of such breach.

(2) A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).

(3) A business associate shall provide the notification without unreasonable delay after discovery of a breach. The notification shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. A business associate shall provide the organization with any other available information that the covered entity is required to include in notification to the individual under paragraph 5.c.(2)(c )(3)(d) at the time of the notification or promptly thereafter as information becomes available.

8. Renumber 5.c.(2)(c )(3)(f) to 5.d.

9. Modify the PII Incident Notification Flow Chart at enclosure 1 Within 10 days to add: For breaches of PHI > 500 individuals, publish a notice in the local media. Notify HHS @ http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.