



**DEPARTMENT OF THE ARMY**  
**HEADQUARTERS, UNITED STATES ARMY MEDICAL COMMAND**  
**2748 WORTH ROAD**  
**JBSA FORT SAM HOUSTON, TEXAS 78234-6013**

REPLY TO  
ATTENTION OF

**OTSG/MEDCOM Policy Memo 13-057**  
**11 OCT 2013**

**MCFP**

**Expires 11 October 2015**

**MEMORANDUM FOR**

**Commanders, MEDCOM Major Subordinate Commands**  
**Directors, OTSG/MEDCOM OneStaff**

**SUBJECT: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures**

**1. References:**

a. Federal Register, Vol. 78, No. 17, 25 January 2013, Rules and Regulations, page 5566, 45 CFR Parts 160 and 164, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.

b. 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.

c. DoD 5400.11-R, DoD Privacy Program, 8 May 2007.

d. DoD 6025.18-R, DoD Health Information Privacy Regulation, 24 January 2003.

e. DoD 8580.02-R, DoD Health Information Security Regulation, 12 July 2007.

f. Office of the Secretary of Defense (Administration and Management), subject: Use of Best Judgment for Individually Identifiable Information (PII) Breach Notification Determinations, 2 August 2012.

g. Office of the Assistant Secretary of Defense Memorandum (Health Affairs), subject: Breach Notification Reporting for the Military Health System, 24 September 2007.

h. Office of the Assistant Secretary of Defense Memorandum (Health Affairs), subject: Reporting a Breach as Defined by the Health Information Technology for

\* This policy supersedes OTSG/MEDCOM Policy Memo 11-070, 19 Aug 11, subject: PII Incident Reporting and Notification Procedures.

**MCFP**

**SUBJECT: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures**

**Economic and Clinical Health Act Provisions of the American Recovery and Reinvestment Act of 2009, 28 April 2010.**

**i. Memorandum, Office of the Secretary of Defense, 5 June 1009subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII).**

**j. OTSG/MEDCOM Policy Memo 12-016, 7 March 2012, subject: MEDCOM Reportable Information Policy.**

**2. Purpose: This prescribes the responsibilities and procedures for reporting incidents when there is suspected or actual loss, theft, or compromise of PII and/or protected health information (PHI). This version updates the reporting procedures and includes the expanded breach management requirements prescribed in reference 1a.**

**3. Proponent: The proponent for this policy is the Freedom of Information Act/Privacy Act (FOIA/PA) Office.**

**4. Policy:**

**a. Protecting the privacy and security of PII and PHI is the responsibility of all members of the MEDCOM workforce to include contractors. A critical component of this process is to properly report the suspected or actual loss of this information and notify those impacted by the breach so that they can properly safeguard against their personal information being used for unlawful purposes such as identity theft and fraud.**

**b. PII is any information about an individual which can be used to distinguish or trace an individual's identity such as name, social security number, date and place of birth, mother's maiden name, and biometric records. This information can be in paper or electronic files and includes, but is not limited to, education records, financial transactions, employment history, criminal records, and medical files. PHI is a subset of PII.**

**c. The DoD Privacy Program Regulation (DoD 5400.11-R) defines a breach as the actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected. Examples of a breach include, but are not limited to:**

**(1) Transmitting unencrypted files and electronic mail (e-mail).**

**(2) Misdirecting FAX documents that reach individuals other than the intended recipient.**

MCFP

SUBJECT: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures

- (3) Failing to shred or burn documents prior to disposal.
- (4) Failing to properly secure documents being mailed or transported.
- (5) Lost or stolen laptops and other electronic media devices.
- (6) Posting PII on publicly accessible websites.
- (7) Sending PII via e-mail to unauthorized recipients.
- (8) Providing hard copies of PII to individuals without a need to know.
- (9) Using PII for unofficial business.
- (10) Unauthorized access to computer systems.

d. All suspected or actual loss, theft, or compromise of PII and PHI must be reported and, in some cases, the individuals affected by the breach should be notified. These notification requirements are provided in paragraph 6 below. Incidents will be reported regardless of the format of the PII (paper or electronic) or the number of persons affected. The individual discovering the breach/compromise, in coordination with the Command/Agency that created the data if known, will report the incidents. When the actual organization is unknown, by default the responsibility for notifying the affected individuals lies with the originator of the document or information.

#### 5. Responsibilities:

a. OTSG/MEDCOM FOIA/PA Office. The OTSG/MEDCOM FOIA/PA office is the primary point of contact (POC) for overseeing and managing the PII incident notification and reporting process.

b. Heads of Organizations. The heads of organizations will:

- (1) Ensure administrative, physical, and technical safeguards protect PII against disclosure, unauthorized access, or misuse.
- (2) Publish local procedures for managing PII incidents.
- (3) Appoint an official to oversee and manage the PII incident reporting and notification process.
- (4) Ensure there are clauses in contracts requiring the contractor/business associate to report breaches of PII.

MCFP

SUBJECT: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures

(5) Ensure appropriate remedial action(s) are taken when PII is lost or compromised. At a minimum, if PII is lost as a result of negligence or failure to follow established procedures, the individual(s) responsible will receive counseling and additional training reminding them of the importance of safeguarding PII. Additional remedial actions may include prompt removal of authority to access information or systems from individuals who demonstrate a pattern of error in safeguarding PII as well as other administrative or disciplinary actions as determined appropriate by the commander or supervisor IAW references 1b – 1e.

6. Procedures:

a. Reporting PII and PHI Breaches. Complete the following notifications within the prescribed timelines, as appropriate. No PII should be provided in these reports. The PII Incident Notification Flow Chart at Enclosure 1 can be used as a “quick look” reference when reporting a PII incident.

(1) Notify your supervisor and local command officials immediately upon discovery. These may include, but are not limited to, FOIA/PA officials; HIPAA privacy and security officials; information assurance officials; public affairs officials; Staff Judge Advocates (SJA); and Congressional liaisons.

(2) Notify the OTSG/MEDCOM Operations Center immediately using the Critical Command Information Report (CCIR) Executive Summary (EXSUM) format and procedures prescribed in reference 1j. Send CCIR EXSUM and updates to: OPSCENTER21 - OPNS@amedd.army.mil. For classified information, send the report to: [usarmy.ncr.hqda-otsg.mbx.medcom-ops-center@mail.mil](mailto:usarmy.ncr.hqda-otsg.mbx.medcom-ops-center@mail.mil). In addition, send a copy of the EXSUM to: [usarmy.jbsa.medcom.list.medcom-pii-report@mail.mil](mailto:usarmy.jbsa.medcom.list.medcom-pii-report@mail.mil) for distribution to the OTSG/MEDCOM HQ FOIA/PA Official, Public Affairs Official, SJA Official, and HIPAA Privacy and Security Officials. The initial CCIR EXSUM will address the following:

(a) Nature of the incident. Include the dates and description of the incident, how the incident was discovered, cause of incident, and the estimated number of affected individuals.

(b) Type of personal information involved in the incident (e.g., name, address, social security number, date of birth, medical data, etc.).

(c) Whether the personal information was encrypted or protected by some other means.

(d) The estimated number of affected individuals and the perceived impact of this incident.

**MCFP**

**SUBJECT: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures**

(e) Steps taken to respond to the incident and mitigate the impact.

(f) Agencies notified. Provide the US-CERT Reporting Number when available.

(3) Notify the US Computer Emergency Readiness Team (US-CERT) within one hour. The online form is available at <https://forms.us-cert.gov/report/>. If computer access is not available, PII incidents can be reported via telephone to (888) 282-0870.

(4) Notify the HQDA FOIA/PA Office within 24 hours. The online report is available at: [https://www.rmda.army.mil/privacy/docs/DPCLO\\_Breach\\_Report\\_Template.pdf](https://www.rmda.army.mil/privacy/docs/DPCLO_Breach_Report_Template.pdf). Once completed, attach the report and email to: [usarmy.belvoir.hqda-oaa-aha.mbx.rmda-foia-privacy-alert@mail.mil](mailto:usarmy.belvoir.hqda-oaa-aha.mbx.rmda-foia-privacy-alert@mail.mil). The HQDA FIOA/PA Office will report this incident to the Department of Defense and Department of Army leadership.

(5) Notify the TRICARE Management Activity (TMA) Privacy and Civil Liberties Office within 24 hours when the breach involves PHI at: [PrivacyOfficerMail@tma.osd.mil](mailto:PrivacyOfficerMail@tma.osd.mil). The report should include the following:

(a) Name of the Component/Organization involved.

(b) Date of initial discovery and date(s) of the actual breach if known. Provide the US-CERT Reporting Number when available.

(c) The contents and nature of the PHI involved, including the types of identifiers and the likelihood of re-identification, and whether or not unsecured PHI is involved.

(d) Documentation of any assessments and actions taken regarding mitigation of the breach and the extent to which risk to the PHI has been mitigated.

(e) Whether the affected individuals are being notified and the projected date when they will be notified. Any additional details believed to be necessary for justifying any determinations for notification and further reporting.

(f) What remedial actions have been, or will be, taken to prevent a similar incident in the future (e.g., additional training conducted, new or revised guidance issues, etc.).

(6) Notify affected individuals within 10 work days of the discovery of the breach and the identification of individuals affected by the breach, if required. A risk of harm determination should be made prior to making the decision to notify the individuals affected by the breach. The risk of harm analysis evaluates the likelihood that the individual will be harmed as a result of the breach and its impact. The risk of harm determination identifies if the risk of harm is low, moderate, or high. Guidance for

MCFP

**SUBJECT: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures**

determining the risk of harm and notifying the affected individuals is provided in Enclosures 2 and 3, respectively.

(7) Notify the Regional Computer Emergency Response Team (RCERT) when the incident involves the possible compromise of Army networks. If the analysis conducted by the Army Computer Emergency Response Team (ACERT) confirms possible PII loss, the RCERT notifies the appropriate Unit Information Assurance Officer to initiate PII loss reporting. The Army FOIA/PA office will provide a copy of all Army PII reports received involving automation equipment to the ACERT Theater Operations Center for situational awareness and analysis.

(8) Notify issuing banks if government issued credit cards are involved.

(9) Notify law enforcement authorities, if necessary.

(10) Notify the media for cases where the breach is significant (i.e., impacting thousands of individuals, the PII is highly sensitive) and the risks and potential for harm to the affected individuals are greater than the risks and potential for harm to the investigation when the breach is disclosed to the public.

b. Additional Reporting Requirements for Breaches Involving PHI. The TMA Privacy and Civil Liberties Office will determine if the incident qualifies as a breach under the provisions of the HIPAA Breach Rule and will subsequently report the incident directly to the Secretary, Department of Health and Human Services (HHS), as appropriate. The HIPAA Breach Rule requires covered entities to report breaches of unsecured PHI. In such instances where reporting to HHS is required, the TMA Privacy and Civil Liberties Office will provide courtesy notification to the organization managing the breach and coordinate all subsequent breach notification actions with that organization. These actions will include: (1) publishing a media release; (2) notifying the individuals affected by the breach; and (3) preparing for the investigation by HHS. If the breach involves 500 or more individuals, HHS will post the breach on its website at: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html> If the breach involves fewer than 500 individuals, the TMA Privacy and Civil Liberties Office will report the incident to HHS at the end of each calendar year.

c. Breaches Involving Government Contractors and/or Business Associates. The government contractors and/or business associates that perform functions involving PII and PHI should immediately notify the organization upon discovery of a breach. A breach shall be treated as discovered by the contractor/business associate as of the first day on which such breach is known or, by exercising reasonable diligence, would have been known to the contractor/business associate. The notification should include, to the extent possible, the identification of each individual who's PII has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed during the

MCFP

SUBJECT: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures

breach. In addition, the contractor/business associate should provide the organization with any other available information that must be included in the notification to the individual.

FOR THE COMMANDER:

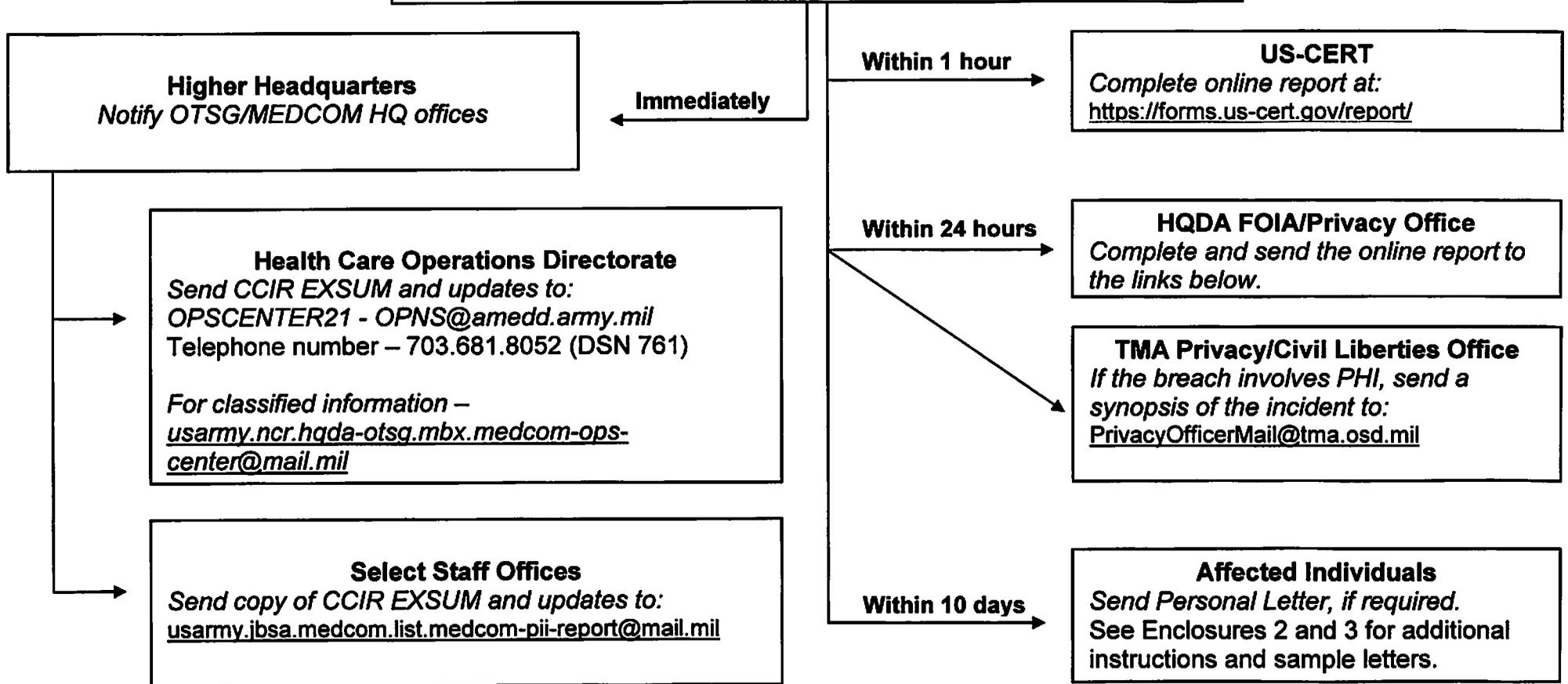
3 Encls  
as



ULDRIC L. FIORE, JR.  
Chief of Staff

## PII Incident Reporting Requirements AT-A-GLANCE

**Organization Possessing/Responsible for Safeguarding the PII**  
*Notify agencies within the prescribed timeframes.  
Notify affected individuals, when required, within the prescribed timeline*



Link to HQDA FOIA/PA Office PII Report: [https://www.rmda.army.mil/privacy/docs/DPCLO\\_Breach\\_Report\\_Template.pdf](https://www.rmda.army.mil/privacy/docs/DPCLO_Breach_Report_Template.pdf).  
Send the report to: [usarmy.belvoir.hqda-oaa-aha.mbx.rmda-foia-privacy-alert@mail.mil](mailto:usarmy.belvoir.hqda-oaa-aha.mbx.rmda-foia-privacy-alert@mail.mil).

## Guidelines for Determining Whether to Notify Individuals Affected by the Breach

1. Determining the Risk of Harm. The determination whether to notify individuals of a breach is based on an assessment of the likelihood that the individual will be harmed as a result of the breach and its impact. Harm includes embarrassment, inconvenience, financial loss, blackmail, identity theft, emotional distress, and loss of self-esteem. Five factors should be weighed to assess the likely risk of harm.

- Nature of the data elements breached
- Number of individuals affected
- Likelihood the information is accessible and usable
- Likelihood the breach may lead to harm, and
- Ability of the organization to mitigate the risk of harm.

A final decision regarding whether to make notification cannot be made until after each risk of harm factor has been assessed. The decision to notify should not be based on one factor alone. For example, a breach may involve social security numbers (SSNs) making that factor a high risk. However, SSNs may be stored on an encrypted, Common Access Card-enabled laptop that mitigates potential compromise which could lead to harm. Therefore, although one factor in this example (data elements) rates as high likelihood of harm, after all factors are evaluated and considered, the overall likelihood of harm resulting from the breach is low given the technical safeguards in place. Generally, absent other factors, organizations should not notify personnel of breaches that have a low overall likelihood of harm.

2. Making the Decision to Notify the Individuals. The risk of harm determinations and the decision whether notification of affected individuals is made, rests with the head of the Army command/agency where the breach occurred. However, all determinations of high risk/harm require notification. The decision whether to contact the affected individuals and the factors considered in reaching this decision will be documented and maintained in the organization's files.

3. Other Factors to Consider. Organizations should bear in mind that notifying individuals of a breach when there is little or no risk of harm could create unnecessary concern and confusion. Components should remain cognizant of the effect that unnecessary notification may have on the public.

---

Source: Office of the Secretary of Defense (Administration and Management), subject: Use of Best Judgment for Individually Identifiable Information (PII) Breach Notification Determinations, 2 August 2012. This memorandum replaced Table 1 in reference 1i.

## Guidelines for Notifying Individuals Affected by the Breach

1. **General.** Notification decisions will be made by the head of the organization or a senior-level individual who is in the chain of command for the organization where the loss, theft, or compromise occurred to reinforce the seriousness of the incident. Notifying the affected individuals may be delayed for good cause (e.g., law enforcement authorities request delayed notification as immediate notification will jeopardize the investigative efforts). If the organization cannot identify the affected individuals, a generalized notice to the potentially affected population will be published. This general notice can be posted on the organization's web site, local newspaper, or other publicly accessible media. When notification is not made within the 10 day period, the organization reporting the incident will inform the OTSG/MEDCOM HQ FOIA/PA Official.

2. **Notification Methods.** The preferred method of notification is by first-class mail but other means (i.e., telephone, email, and substitute notice) are acceptable as long as there is reasonable assurance that the affected individuals will be contacted. 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 is to be made 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. Provide follow-up written notification when individuals are notified by telephone.

### 3. **Notification Letters.**

a. The notification letter should contain the following elements:

- Brief description of what happened, including the date(s) of the breach and its discovery.
- Description of the types of personal information involved in the breach (e.g., full name, social security number, date of birth, home address, account number, etc).
- Risk of harm associated with the breach.
- Statement whether the information was encrypted or protected by other means if it is determined that such information would be beneficial and would not compromise the security of the system.
- What steps individuals should take to protect themselves from potential harm, if any.
- What the organization is doing to investigate the breach, to mitigate losses (i.e. free credit monitoring), and to protect against further breaches.

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

b. Sample notification letters are available in reference 1c and the Records Management and Declassification Agency (RMDA) web site at:  
<https://www.rmda.army.mil/privacy/docs/SampleNotificationLetter.pdf>.

c. When sending the notification by mail, the front of the envelope will have a label to alert the recipient of the importance of its contents (e.g., "Data Breach Information Enclosed"). The envelope will also be marked with the name and postal address of the organization that suffered the breach.

5. Notification When There is Insufficient or Out-of-Date Contact Information. When 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. The number of individuals affected by the breach determines the preferred notification method as follows:

a. Fewer Than 10 individuals. 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. 10 or More Individuals. 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 PHI may be included in the breach.

---

Source: Office of the Secretary of Defense Memorandum, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII), 5 June 2009.