



REPLY TO  
ATTENTION OF

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

OTSG/MEDCOM Policy Memo 11-070

MCFP

**19 AUG 2011**

Expires 19 August 2013

MEMORANDUM FOR

COMMANDERS, MEDCOM MAJOR SUBORDINATE COMMAND  
DIRECTORS, OTSG/MEDCOM ONESTAFF

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

1. References:

a. 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.

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

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

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

e. Army Regulation 25-2, Information Assurance, 23 March 2009.

f. Message, HQDA, 262121Z Feb 09, ALARACT 050/2009, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures.

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

h. Memorandum, Office of the Assistant Secretary of Defense (Health Affairs), subject: Reporting a Breach as Defined by the Health Information Technology for 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, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII), 5 June 2009.

-This policy supersedes OTSG/MEDCOM Policy Memo 09-021, 7 Apr 09, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures.

MCFP

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

j. OTSG/MEDCOM Policy Memorandum 09-30, 5 June 2009, subject: MEDCOM Command Information (including CCIR, EEFI, SIR, PIR, FFIR).

2. Purpose: This prescribes the responsibilities and procedures for reporting incidents when there is suspected or actual loss, theft, or compromise of PII. This version includes the expanded breach management requirements prescribed in the Interim Final Rule for Breach Notification for Unsecured Protected Health Information, issued pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act.

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

4. Policy:

a. The US Army Medical Command (MEDCOM) continues to implement policies and practices to safeguard the PII of its personnel and their families. Part of this process is to properly report the suspected or actual loss of this information and to notify those impacted so they can properly safeguard against identity theft.

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 hardcopy (paper copy files) or electronic format, stored on personal computers, laptops, and personal electronic devices and found within databases. This information includes, but is not limited to, education records, financial transactions, employment history, criminal records, and medical files. The protected health information (PHI) covered by the Health Insurance Portability and Accountability Act (HIPAA) is a subset of PII.

c. A breach or compromise incident occurs when it is suspected or confirmed that PII is lost, stolen, or otherwise available to individuals without an official need to know. This includes, but is not limited to, posting PII on publicly accessible web sites; sending PII via electronic mail (e-mail) to unauthorized recipients; providing hard copies of PII to individuals without a need to know; loss of electronic devices storing PII; failing to dispose of hard copies of PII by burning or shredding; using PII for unofficial business; misdirecting FAX documents; transmitting unencrypted files and e-mails; unsecured mailing or transporting documents and all other unauthorized access to PII.

d. All suspected or actual loss, theft, or compromise of PII will be reported to the agencies listed below and, in most cases, the individuals affected by the breach. The individual discovering the breach/compromise, in coordination with the Command/ Agency that created the data if known, will report the incidents. Incidents regardless of the format of the PII (paper or electronic) or the number of persons affected will be

MCFP

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

reported. 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.

e. Additional notification and reporting activities are required when there is a breach of unsecured PHI IAW reference 1a (HITECH Act). Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of encryption and destruction methodologies. The requirements for managing breaches of unsecure PHI involving 500 and more individuals are outlined in Enclosure 2.

f. Incidents involving the possible compromise of Army networks will be reported to the appropriate Regional Computer Emergency Response Team (RCERT). If the analysis conducted by the Army CERT (ACERT) confirms data exfiltration and possible PII loss, the RCERT will notify the appropriate agency information assurance officer to initiate PII loss reporting.

g. Local officials will be involved in the management of the PII incident early and often. 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); Congressional liaisons; and law enforcement authorities.

h. Media notifications should be prepared in 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. Early preparation of the media notifications will ensure the organization can readily respond to a media inquiry or, when determined necessary, release information to media organizations.

i. The Privacy Act requires government contractors to immediately notify the organization upon discovery of a breach of PII. The HIPAA has a similar requirement but uses the term “Business Associate” when referring to a person or entity that performs or assists in the performance of a function or activity (legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services) involving the use or disclosure of PHI on behalf of, or to provide services to, an organization. The following applies when a breach occurs and these requirements must be included in all contracts involving the use or disclosure of PII:

(1) 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 contractor/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,

MCFP

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

or other agent of the contractor/business associate (determined in accordance with the federal common law of agency).

(2) The contractor/business associate will provide the notification without unreasonable delay after discovery of a breach. The notification will include, to the extent possible, the identification of each individual whose PII has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed during the breach. In addition, the contractor/business associate will provide the organization with any other available information that is must be included in the notification to the individual. This information will be provided at the time of the notification or promptly thereafter as information becomes available.

j. The bank will be notified when the breach involves the loss, theft, or compromise of government credit cards issued by that bank.

#### 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 as prescribed in paragraph 4i(1) and 4i(2) above.

(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.

MCFP

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

c. Organization Possessing or Responsible for Safeguarding the PII at the Time of the Incident. This organization will:

- (1) Immediately notify local command and higher headquarters officials.
- (2) Prepare draft EXSUM and coordinate with higher headquarters officials. See paragraph 5d(1) below for additional guidance.
- (3) Notify the following agencies within the prescribed timelines as outlined in reference 1b and 1f (DoD 5400.11/ALARACT 050/2009). Internal command notifications should not delay reporting to these agencies.

(a) Within one hour. (US-CERT and CIO/G6 Notification)

(1) Notify the United States Computer Emergency Readiness Team (US-CERT) at <http://www.us-cert.gov>. Use the "Report an Incident" tab on the left side of the US-CERT home page to access the US-CERT Incident Reporting System. If computer access is not available, PII incidents can be reported to (866) 606-9580 from the Office of the Administrative Assistant (OAA) to the Secretary of the Army or US-CERT at (703) 235-5110. Both telephone lines are monitored 24/7.

(2) Notify the Headquarters, Department of Army (HQDA) leadership Chief Information Officer (CIO). Send a brief synopsis of the incident, the name of the local POCs, and their contact information to [pri.reporting@us.army.mil](mailto:pri.reporting@us.army.mil). This e-mail alerts the HQDA CIO that a PII incident was reported to the US-CERT. Provide updates to the HQDA CIO as required.

(b) Within 24 hours. (HQDA FOIA/PA and TRICARE Management Activity (TMA) Privacy Office).

(1) Notify the HQDA FOIA/PA. The online report and submission guidelines are available at <https://www.rmda.army.mil/organization/pa-guidance.shtml>. Click on the "Report a PII Incident to HQDA Privacy Office" link to access the US Army Privacy Incident Report. Provide updates to the HQDA FOIA/PA official as they become available.

(2) Notify the TMA Privacy Office when the breach involves TRICARE beneficiaries IAW reference 1g (OASD(HA) Memo 24 Sep 2007). Send a synopsis of the incident to [PrivacyOfficerMail@tma.osd.mil](mailto:PrivacyOfficerMail@tma.osd.mil) to include the following:

- Component/Organization involved.
- Date of incident and the number of individuals impacted, to include whether they are DoD civilian, military, or contractor personnel; DoD

MCFP

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

civilian or military retirees; family members; other Federal personnel or members of the public, etc.

- Brief description of incident, to include facts and circumstances surrounding the loss, theft, or compromise.
- Actions taken in response to the incident, to include whether the incident was investigated and by whom; the preliminary results of the inquiry if known; and actions taken to mitigate any harm that could result from the loss. Provide the US-CERT Reporting Number when available.
- Whether the affected individuals are being notified and the projected date when they will be notified.
- 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.).

(3) For breaches of unsecured PHI involving 500 or more individuals, the TMA Privacy Office will determine if the incident qualifies as a breach under the provisions of the HITECH Act. IAW reference 1h, if the incident qualifies as a breach under the provisions of the HITECH Act, the TMA Privacy Office will report the incident directly to the Secretary, Health and Human Services (HHS). In such instances where reporting to HHS is required, the TMA Privacy Office will provide courtesy notification to the organization managing the breach and coordinate all subsequent breach notification actions with that organization. See Enclosure 2 for additional guidance on managing this type of breach.

(4) For breaches of unsecured PHI involving less than 500 individuals, the TMA Privacy Office shall maintain a log or other documentation of such breaches and, report this information to HHS as well.

(c) Within ten days. (Affected Individuals)

(1) For all PII breaches and breaches of unsecured PHI involving less than 500 individuals, a risk assessment must be conducted to determine whether notification to the affected individuals is necessary. If required, this notification must occur within ten days from discovery of the breach and the identities of the individuals ascertained.

(2) An organization will assess the risk of harm caused by the breached information and then assess the relative likelihood of the risk occurring (risk level). The following documents are enclosed to assist with this determination: (1) Identity Theft Risk Analysis which provides the factors to consider when assessing the likelihood for risk of harm caused by the breach; and (2) Risk Assessment Model which provides

MCFP

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

algorithms for determining the risk level (i.e., low, moderate, or high). These documents are available at Enclosure 3 and 4, respectively. In general, the risk of harm to the individual is higher the greater the sensitivity of the data involved.

(3) In accordance with reference 1i, 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. 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. The decision whether to contact the affected individuals and the factors considered in reaching this decision must be documented and maintained in the organization's files.

(4) If affected individuals must be notified, the organization responsible for safeguarding the PII at the time of the incident is responsible for making the notifications. When the actual Army activity where the incident occurred is unknown, by default, the responsibility for reporting the incident and notification of affected individuals lies with the originator of the document or information. Notifications 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.

(5) 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.

(6) Specific guidance regarding the notification process is as follows:

The organization responsible for safeguarding the PII at the time of the incident must notify the affected individuals. When the actual Army activity where the incident occurred is unknown, by default, the responsibility for reporting the incident and notification of affected individuals lies with the originator of the document or information. Notifications 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 to impacted individuals. 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

MCFP

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

representative of the individual. The notification may be provided in one or more mailings as information is available. Provide follow-up written notification when telephone notification is effected. Sample notification letters are available at the Records Management and Declassification Agency (RMDA) web site - <https://www.rmda.army.mil/privacy/docs/SampleNotificationLetter.pdf> and in reference 1b.

(b) 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.

(c) The notification letters should address the following elements:

- Brief description of what happened, including the date(s) of the breach and of 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. See Enclosures 2 and 3 for assistance in determining the risk of harm.
- 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

d. MSC Commanders, OTSG/MEDCOM OneStaff Directors, and Executive Agency (EA) Directors. The commanders and directors will:

(1) Immediately notify the OTSG/MEDCOM Operations Center (OPSCENTER21) and provide periodic updates and a final close-out report using the

MCFP

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

CCIR Executive Summary (EXSUM) format and procedures prescribed in reference 1j. Report CCIRs by electronic means to [EOC.OPNS@otsg.amedd.army.mil](mailto:EOC.OPNS@otsg.amedd.army.mil) (listed as "OTSG OPNSCENTER21 OPNS" on the AMEDD Global Directory) or FAX (703) 681-3043. Follow up all electronic submissions with a telephone call to OPNSCENTER21 (703) 681-8052/5095 (DSN 761). Submission of reports will not be delayed due to incomplete information. Additional required information will be provided in subsequent EXSUMs until the situation is resolved. The CCIR EXSUM format is available at Enclosure 5. The initial CCIR EXSUM should 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.

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

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

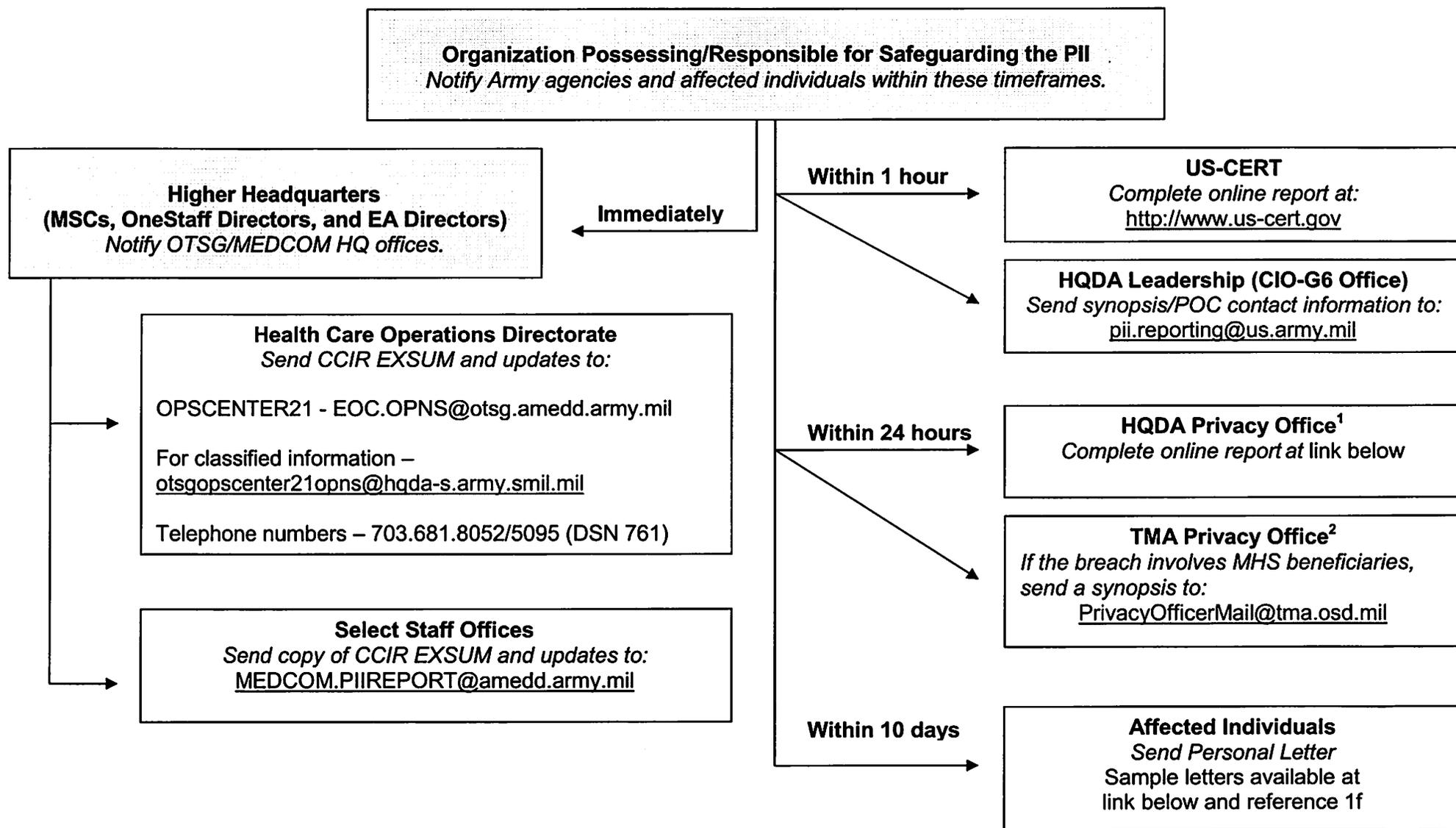
(2) Send a copy of the initial CCIR EXSUM and any updates to [MEDCOM.PIIREPORT@amedd.army.mil](mailto:MEDCOM.PIIREPORT@amedd.army.mil). Reports sent to this e-mail address will be disseminated to the OTSG/MEDCOM FOIA/PA Official, Public Affairs Official, SJA Official, and HIPAA Privacy and Security Officials.

FOR THE COMMANDER:

5 Encls  
as

  
HERBERT A. COLEY  
Chief of Staff

## PII Incident Notification Flow Chart



<sup>1</sup>Link to HQDA FOIA/PA Office report – <https://www.rmda.army.mil/organization/pa-guidance.shtml>

<sup>2</sup>If breach of unsecured PHI involves 500 or more individuals, see Enclosure 2 for additional reporting requirements.

## Breaches of Unsecured PHI Involving 500 or More Individuals

1. The HITECH Act requires that amendments be made to Health Insurance Portability Accountability Act Privacy and Security rules and establishes new individual notification and government reporting requirements when a "breach" of "unsecured Protected Health Information (PHI)" occurs. A "breach" as defined by the Department of Health and Human Services (HHS) differs from the broader definition established by the DoD policy.
2. HHS issued guidance in August 2009 for these new requirements in an Interim Final Rule on Breach Notification for Unsecured Protected Health Information ("HHS Breach Rule"). This new interim rule includes requirements to provide notification to individuals affected by breaches and to report breaches of unsecured PHI to HHS. It should be noted that amendments to various requirements may be implemented when the final rule is published. These provisions apply equally to Military Health System (MHS) Components including business associates of MHS covered entities.
3. The TMA Privacy Office will determine if the incident qualifies as a breach under the provisions of the HHS Breach Rule and will subsequently report the incident directly to the Secretary, HHS, as appropriate. In such instances where reporting to HHS is required, the TMA Privacy Office will provide courtesy notification to the MHS Component. Additionally, to the extent required by the terms of the contract, business associates that discover a breach shall continue to notify the organization immediately in accordance with DoD 5400.11-R, C1.5.1.3. The MHS organization will then report the breach to the TMA Privacy Office, which will make the determination of whether further reporting to HHS is necessary, as outlined above.
4. When the TMA Privacy Office determines that the incident qualifies as a breach under the HITECH Act, the following will occur:
  - a. TMA Privacy Office will report the incident to the Secretary, HHS and initiate correspondence with the organization responsible for managing the breach.
  - b. The organization responsible for managing the breach will prepare a media release and coordinate it with the TMA Privacy Office.
  - c. The organization responsible for managing the breach will notify the Individuals affected by the breach. The following guidelines will be followed:
    - (1) 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.

(2) 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.

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

(a) 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

(b) 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.

d. HHS will list the breach on its web site at:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>

e. HHS will conduct an investigation of the incident and may request the following:

- (1) Organization's internal investigation report.
- (2) Organization's corrective action plan (sanctioning, re-training, etc.)
- (3) Policies and procedures related to disclosure of PHI and safeguarding PHI.
- (4) Verification of employee's HIPAA training for last three years.
- (5) Log of patients to whom the breach notification was sent.
- (6) Copy of notification(s) made to local media.

## Identity Theft Risk Analysis

Five factors to consider when assessing the likelihood of risk and/or harm:

1. 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. For example, theft of a database containing individuals' names in conjunction with Social Security Numbers, and/or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context.

It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context. In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

2. Number of Individuals Affected. The magnitude of the number of affected individuals may dictate the methods you choose for providing notification, but should not be the only determining factor for whether an agency should provide notification.

3. Likelihood the Information is Accessible and Usable. Upon learning of a breach, agencies should assess the likelihood personally identifiable information will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the agency's decision to provide notification.

Depending upon a number of physical, technological, and procedural safeguards employed by the agency, the fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. If the information is properly protected by encryption, for example, the risk of compromise may be low to non-existent. In this context, proper protection means encryption has been validated by National Institute of Standards & Technology (NIST).

Agencies will first need to assess whether the breach involving personally identifiable information is at a low, moderate, or high risk of being used by unauthorized persons to cause harm to an individual or group of individuals. The assessment should be guided by NIST security standards and guidance. Other considerations may include the likelihood any unauthorized individual will know the value of the information and either use or sell the information to others.

4. Likelihood the Breach May Lead to Harm.

*Broad Reach of Potential Harm.* The Privacy Act requires agencies 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, agencies should consider a number of possible harms associated with the loss or compromise of information. 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, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

*Likelihood Harm Will Occur.* The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security Numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of recipients patients at a clinic for treatment of a contagious disease.

In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance from the Identity Theft Task Force found at [www.ftc.gov/os/2008/10/081021taskforcereport.pdf](http://www.ftc.gov/os/2008/10/081021taskforcereport.pdf).

5. *Ability of the Agency to Mitigate the Risk of Harm.* Within an information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken. Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

---

Source: Office of the Secretary of Defense, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (Table 1), 21 September 2007.

## Risk Assessment Model (Notifying Affected Individuals)

No.	Factor	Risk Determination	Low Moderate High	Comments:
				<ul style="list-style-type: none"> <li>• All breaches of PII, whether actual or suspected, require notification to US-CERT.</li> <li>• Low and moderate-risk/harm determinations and the decision whether notification of individuals is made, rest with the Head of the DOD Component where the breach occurred.</li> <li>• All determinations of high risk or harm require notifications.</li> </ul>
1.	What is the nature of the data elements breached? What PII was involved?			
	a. Name only	Low		Consideration needs to be given to unique names: those where one or only a few in the population may have or those that could readily identify an individual, i.e., public figure.
	b. Name plus 1 or more personal identifier (not SSN, Medical or Financial)	Moderate		Additional identifiers include date and place of birth, mother's maiden name, biometric record and any other information that can be linked or is linkable to an individual.
	c. SSN	High		
	d. Name plus SSN	High		
	e. Name plus Medical or Financial data	High		
2.	Number of Individuals Affected			The number of individuals involved is a determining factor in how notifications are made, not whether they are made.
3.	What is the likelihood the information is accessible and usable? What level of protection applied to this information?			
	a. Encryption (FIPS 140-2)	Low		
	b. Password	Moderate/High		Moderate/High determined in relationship to category of data in Number 1.
	c. None	High		
4.	Likelihood the Breach May Lead to harm	High/Moderate /Low		Determining likelihood depends on the manner of the breach and the type(s) or data involved.
5.	Ability of the Agency to Mitigate the Risk of Harm			
	a. Loss	High		Evidence exists that PH has been lost; no longer under DoD control.
	b. Theft	High		Evidence shows that PH has been stolen and could possibly be used to commit ID theft?
	c. Compromise			
	(1) Compromise beyond DOD control	Low High		No evidence of malicious intent. Evidence or possibility of malicious intent.
	(2) Compromise beyond DOD control	High		Possibility that PII could be used with malicious intent or to commit ID theft.

Source: Office of the Secretary of Defense, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (Table 1), 21 September 2007.

## CCIR EXSUM Format

---

UNCLASSIFIED

EXECUTIVE SUMMARY

20 April 20XX

(U) PREPARATION OF AN EXECUTIVE SUMMARY (EXSUM). (U) (Office symbol)

An EXSUM is a brief summary in response to a question or to provide information. The EXSUM should not exceed 15 lines. Prepare in a concise and informative style in the active voice. Use approved acronyms and abbreviations; normally, spell out the abbreviations the first time. EXSUMS containing protected health information should be de-identified and should not contain name, rank, or other individually identifiable information. Use Arial 12 pitch font and 1-inch margins. The EXSUM should begin with the overall classification, followed by the subject (capitalized and underlined) and the originator's office symbol, followed by the body of the summary. Identify the originator and indicate EXSUM approval as shown below. Provide follow up summaries to complete information not available immediately and to indicate the resolution of reported problems.

LTC Staffer/DASG-XX (703) 681-XXXX

APPROVED BY: COL Boss

UNCLASSIFIED

---

Source: OTSG/MEDCOM Policy Memorandum 11-013, 3 Mar 11, subject: Reportable Information (including CCIR, EEFI, SIR, PIR, FFIR).