DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MEDICAL COMMAND
2050 WORTH ROAD
FORT SAM HOUSTON, TEXAS 78234-6013

REPLY TO
ATTENTION OF

MCFP

OTSG/MEDCOM Policy Memo 09-021

Expires 7 April 2011

07 APR 2009

MEMORANDUM FOR SEE DISTRIBUTION

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

1. References:

a. Office of the Secretary of Defense Memorandum, 21 September 2007, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII), https://www.rmda.army.mil/privacy/docs/foia-safeguardingandRespondingtoPIIOMBMemo.pdf.

b. Army Regulation 25-2, Information Assurance, 24 October 2007, http://www.usapa.army.mil/pdffiles/r25_2.pdf.

c. DoD 6025.18-R, DoD Health Information Privacy Regulation, 24 January 2003, http://www.dtic.mil/whs/directives/corres/html/602518r.htm.

d. DoD 8580.02-R, DoD Health Information Security Regulation, 12 July 2007, http://www.tricare.mil/tmaprivacy/downloads/858002rp.pdf.

e. Message, HQDA, 261826Z Jul 07, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures, https://www.rmda.army.mil/privacy/docs/foia-piialaract_072907.pdf.

f. Office of the Assistant Secretary of Defense Memorandum (Health Affairs), 24 September 2007, subject: Breach Notification Reporting for the Military Health System, http://www.tricare.mil/tmaprivacy/downloads/ReportingforMHS.pdf.

g. DoD 5400.11-R, DoD Privacy Program, 8 May 2007, http://www.dtic.mil/whs/directives/corres/html/540011.htm.

h. OTSG/MEDCOM Policy Memorandum 07-033, 13 August 200, subject: Commander's Critical Information Requirements (CCIR), https://www.us.army.mil/suite/doc/8437382.

i. Message, HQDA, ALARACT 050/2009, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures, https://www.rmda.army.mil/privacy/docs/ALARACT_050_2009_1.pdf.

2. Purpose: This prescribes the responsibilities and procedures for reporting incidents when there is suspected or actual loss, theft, or compromise of PII.

3. Proponent: The proponent for this policy is the Freedom of Information Act/Privacy Act (FOIA/PA) Office, Office of The Surgeon General (OTSG)/Headquarters, US Army Medical Command (MEDCOM).

4. Policy:

a. Personally identifiable information 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 in the Health Insurance Portability and Accountability Act (HIPAA) is a subset of PII.

b. 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; and all other unauthorized access to PII.

c. All suspected or actual loss, theft, or compromise of PII will be reported to the agencies listed below and, in most cases, the individuals impacted 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 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.

d. 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 confirms data exfiltration and possible PII loss, the RCERT will notify the appropriate agency information assurance officer to initiate PII loss reporting.

e. Local officials should 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.

f. 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.

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) Commanders and supervisors will ensure that 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 in accordance with references 1b and 1d.

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) Notify the following agencies within the prescribed timelines as outlined in references 1e and 1f. Internal command notifications should not delay reporting to these agencies.

(a) Within 1 hour.

(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 Report. 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)–G6. Send a brief synopsis of the incident, the name of the local POCs, and their contact information to pii.reporting@us.army.mil. This e-mail alerts the HQDA CIO-G6 that a PII incident was reported to the US-CERT. Provide updates to the HQDA CIO-G6 as required.

(b) Within 24 hours.

(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" link to access the HQDA FOIA/PA PII Incident report. Provide updates to the HQDA FOIA/PA official as they become available.

(2) Notify the TRICARE Management Activity (TMA) Privacy Office when the breach involves TRICARE beneficiaries. Send a synopsis of the incident to PrivacyOfficerMail@tma.osd.mil to include the following information:

(a) Component/Organization involved.

(b) Date of incident and the number of individuals impacted, to include whether they are DoD civilian, military, or contractor personnel; DoD civilian or military retirees; family members; other Federal personnel or members of the public, etc.

(c) Brief description of incident, to include facts and circumstances surrounding the loss, theft, or compromise.

(d) 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.

(e) Whether the affected individuals are being notified and the projected date when they will be notified.

(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.)

(c) Within 10 days.

(1) Notify the affected individuals as soon as possible but not later than 10 days after the suspected or actual loss, theft, or compromise of PII is discovered. The 10-day period begins when the identities of the affected individuals are ascertained.

(2) In accordance with reference a., low/moderate/high risk or 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. 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). Two documents are enclosed to assist with this determination:

1. Identity Theft Risk Analysis
2. Risk Assessment Model

The Identity Theft Risk Analysis provides the factors to consider when assessing the likelihood for risk and/or harm and the Risk Assessment Model provides algorithms for determining the level of risk and/or harm (i.e., low, moderate, or high). These documents are available at enclosure 2 and enclosure 3, respectively. The decision whether to contact or not to contact the affected individuals and the factors considered in reaching this decision must be documented and maintained in the organization's files.

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

(a) 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 seriousness of the incident.

(b) 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. Provide follow-up written notification when telephone notification is effected. Sample notification letters are available at the Records Management and Declassification Agency web site - https://www.rmda.army.mil/privacy/docs/SampleNotificationLetter.pdf and in reference 1g.

(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.

(d) The notification should address the following elements:

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

(2) 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.).

(3) Risk of harm associated with the breach. See enclosures 2 and 3 for assistance in determining the risk of harm.

(4) 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.

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

(6) What the organization is doing to investigate the breach, to mitigate losses (i.e., free credit monitoring), and to protect against further breaches.

(7) Who the affected individuals should contact at the agency for more information, including phone number, either direct or toll-free; email address; and postal address.

(e) Notify the bank when the breach involves the loss, theft, or compromise of government credit cards issued by that bank.

(f) 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 CCIR Executive Summary (EXSUM) format and procedures prescribed in reference 1h (CCIR Memo). Send reports with unclassified information to OPSCENTER21 – EOC.OPNS@amedd.army.mil. Reports with classified information will be sent to otsgopscenter21opns@hqda-s.army.smil.mil. The telephone numbers for OPSCENTER21 are (703) 681-8052/5095 (DSN 761). The CCIR EXSUM format is available at enclosure 4. 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. Reports sent to this email address will be disseminated to the OTSG/MEDCOM FOIA/PA Official, Public Affairs Official, SJA Official, and HIPAA Privacy and Security Officials.

6. Our POC is Mr. John Peterson, FOIA/PA Office, DSN 471-7826 or commercial (210) 221-7826, or email: John.P.Peterson@us.army.mil.

FOR THE COMMANDER:

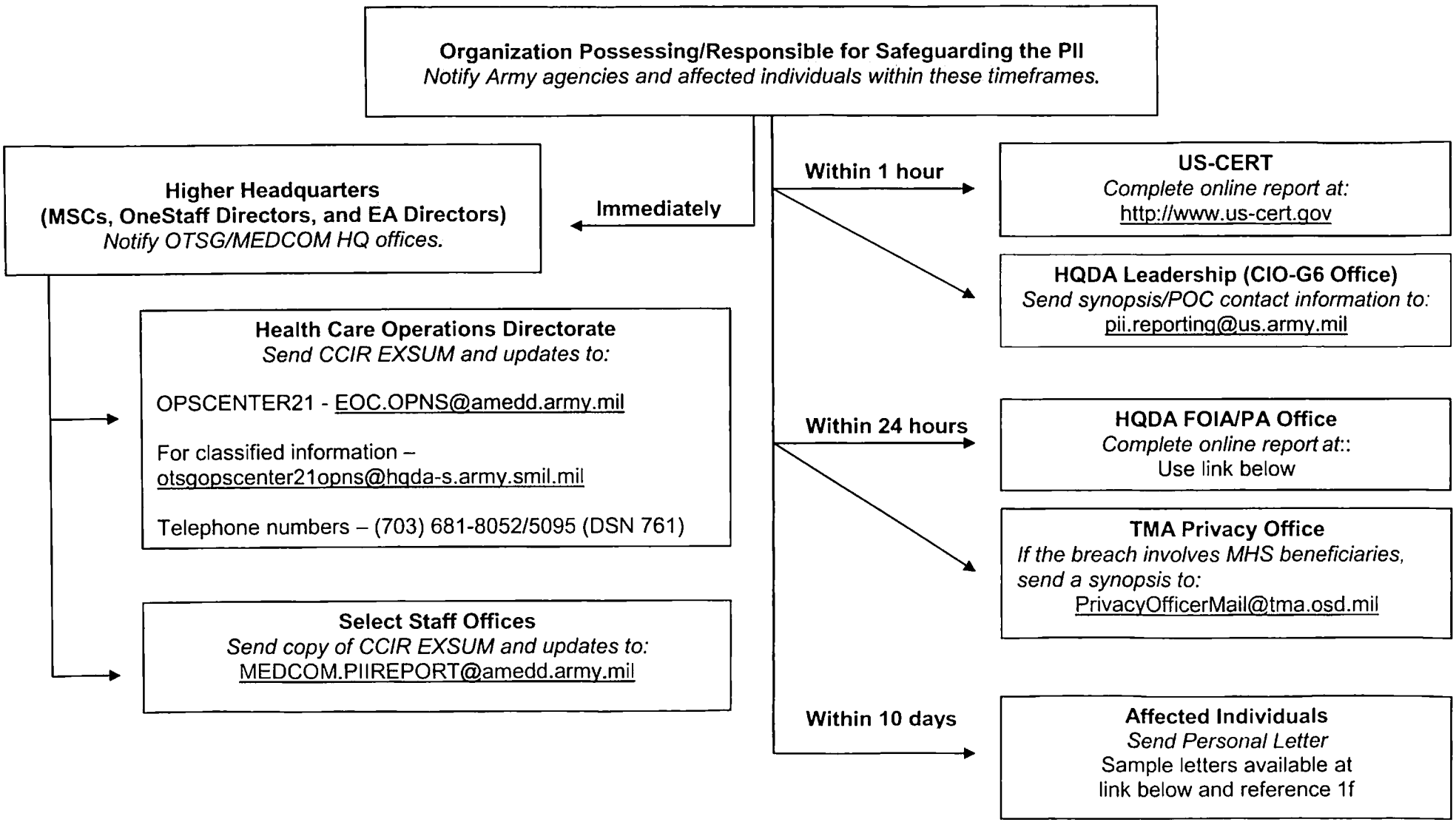
Herbert A. Coley

HERBERT A. COLEY
Chief of Staff

4 Encls
as

DISTRIBUTION:
Commanders, MEDCOM Major Subordinate Commands
Directors, OTSG/MEDCOM OneStaff
Special Staff
Personal Staff
Directors, AMEDD Executive Agencies

PII Incident Notification Flow Chart



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

Encl 1

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 or 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 (Updated link).

5. Ability of the Agency to Mitigate the Risk of Harm. With in 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: All breaches of PII, whether actual or suspected, require notification to US-CERT. 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. All determinations of high risk or harm require notifications.
1.	What is the nature of the data elements breached? What PIT 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 I 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. The words "PREPARE MEMO" should end the summary.
PREPARE MEMO _____.

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

APPROVED BY: COL Boss

UNCLASSIFIED

Source: OTSG/MEDCOM Policy Memorandum 07-033, subject: Commander's Critical Information Requirements (CCIR), 13 August 2007.

Encl 4