



DEPARTMENT OF THE NAVY

BUREAU OF MEDICINE AND SURGERY
2300 E STREET NW
WASHINGTON DC 20372-5300

IN REPLY REFER TO

5239

Ser M09B6/09UM09B6121

6 Jul 09

MEMORANDUM FOR COMMANDER, NAVY MEDICINE EAST
COMMANDER, NAVY MEDICINE WEST
COMMANDER, NAVY MEDICINE NATIONAL CAPITAL AREA
COMMANDER, NAVY MEDICINE SUPPORT COMMAND

Subj: PERSONALLY IDENTIFIABLE INFORMATION (PII) INCIDENT REPORTING
REQUIREMENTS

- Ref: (a) DoD 5400.11-R, DoD Privacy Program, May 14, 2007
(b) DoD Memorandum, Safeguarding Against and Responding to the Breach of PII,
5 Jun 09
(c) DoD Memorandum, Breach Notification Reporting for Military Health System,
24 Sep 07
(d) DON CIO Washington DC 291652Z FEB 08
(e) OPNAVINST 3100.6H
(f) SECNAV M-5214.1 of December 2005

Encl: (1) Personally Identifiable Information Incident Reporting Flowchart

1. Purpose. Update Navy Medicine reporting requirements and process for incidents involving PII. Identify new and existing requirements for incident reporting issued by the Department of Navy (DON) and Department of Defense (DoD), per references (a) through (d).
2. Scope. Applies to all Navy Medicine personnel (military, civilian, and contractors), and to all known or suspected breaches of PII. Per reference (d), all Navy Medicine activities should have a designated official in the chain of command responsible for PII incident reporting, follow-up actions, and individual notifications.
3. Background. This memorandum supersedes the reporting process described in BUMEDNOTE 5239 of 3 June 2008. Reviewing references (a) through (d) is strongly encouraged in order to understand the nature of PII related incidents. In particular, reference (b) provides clarification on the definition of PII and what constitutes an incident. Per reference (b):
 - a. PII refers to information which can be used to distinguish or trace an individual's identity, e.g., name, social security number, date and place of birth, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, mother's maiden name, biometric, personnel, medical, financial information, and other demographic data, including any other personal information which is linked or linkable to a specified individual (note: protected health information (PHI) is a subset of PII).

Subj: PERSONALLY IDENTIFIABLE INFORMATION INCIDENT (PII) REPORTING REQUIREMENTS

b. An incident involving PII, also known as a “breach,” refers to the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for other than an authorized purpose, have access or potential access to PII, whether physical or electronic.

c. Examples of PII that are subject to release under the Freedom of Information Act include name, civilian grade, and salary. Other elements of PII are considered For Official Use Only (i.e., sensitive), but are commonly shared in the work environment, including name, business phone, and military rank. In both situations, release of these items of information, in general, do not constitute a “breach” or an “incident.” In situations where an incident is suspected, the context of information must be considered and a determination of risk must be conducted to determine if (a) a breach has actually occurred, and (b) whether notification to affected individuals is required. The responsibility for determining the potential risk of harm to impacted personnel and whether notification is required is specified in paragraph 4.f.

4. Action. The updated process outlined below will be used for reporting known or suspected incidents involving PII. Please note that personal names or other forms of PII should **not** be included in any of the following incident reports. Also, please be sure to spell out all acronyms, as appropriate.

a. Within one hour of the discovery of a known or suspected incident of PII, the designated official of the Navy Medicine command/activity associated with detecting the incident shall complete OPNAV 5211/13, DON Loss or Compromise of Personally Identifiable Information (PII) Breach Reporting Form and notify via a single e-mail the following privacy officials and agencies: (1) Address to: the United States Computer Emergency Readiness Team (US-CERT), soc@us-cert.gov; (2) Copy to: the DON CIO Privacy Office, don.privacy.fct@navy.mil; the Chief of Information (CHINFO), chinfo.dutyoffic.fct@navy.mil; TRICARE Management Activity (TMA) Privacy Office, privacyofficermail@tma.osd.mil; and the Navy Medicine CIO Privacy & Security Team (BUMED M62), bumed.pii.rpt@med.navy.mil. The completed OPNAV 5211/13 can be sent with a built-in e-mailing function (auto-populates the addressees in your local e-mail client); alternatively, it can be saved and attached to an e-mail. The OPNAV 5211/13 shall be sent via e-mail with the below information, but shall not be delayed due to lack of detailed information:

(1) Component/organization involved/affected (i.e., accountable). Note: the command/activity that detected the incident may not be involved with nor affected by the incident. It is important, however, that the incident is reported as soon after detection as possible in order to mitigate potential damage. The DON CIO Privacy Office will assist, as needed, in determining the accountable command/activity;

(2) Date of incident, the number of individuals impacted, and whether they are government civilian, military, and/or private citizens (include percentage of each category);

Subj: PERSONALLY IDENTIFIABLE INFORMATION INCIDENT (PII) REPORTING REQUIREMENTS

(3) Brief description of incident, including circumstances surrounding the suspected or confirmed loss, theft, or compromise, the specific type of information, and if the PII was encrypted and/or password protected. Again, do **not** include PII (including personal names of those affected) or other sensitive information in the incident report.

b. If the incident involved the loss or suspected loss of a government authorized credit card or associated financial data associated with the card, immediately notify the issuing bank, and the command's government credit card manager.

c. If commission of a crime is suspected, notify the local Naval Criminal Investigative Service (NCIS) office to conduct an investigation. It is recommended that you also contact the local Staff Judge Advocate (SJA) or Office of General Council (OGC).

d. When applicable, issue an OPREP3, per reporting procedures contained in reference (e).

e. As soon as additional information becomes available, the designated official of the accountable command/activity will send a follow-up report to the addressees specified in paragraph 4.a. Information to be submitted should include:

(1) Actions taken in response to the breach, to include whether the incident was investigated and by whom;

(2) The preliminary results of the inquiry if then known;

(3) Actions taken to mitigate any harm that could result from the breach;

(4) Remedial actions that have been, or will be taken to prevent a similar such incident in the future, e.g., refresher training conducted, new or revised guidance issued;

(5) Any other information considered pertinent as to actions to be taken to ensure that information is properly safeguarded.

The same form used for the initial report can be used for supplemental reports. Note: this follow-up may be used to submit the US-CERT Case Number so as not to delay initial reporting.

f. Within 24 hours of receiving the initial report, the DON CIO Privacy Office will direct the designated official of the accountable command/activity as to whether notification of affected individuals is required, i.e., the individuals whose information was compromised. The DON CIO Privacy Office will base the decision to notify individuals on a review of the initial breach report and determine, using DoD's risk analysis methodology in reference (b), the potential risk of harm to impacted personnel.

Subj: PERSONALLY IDENTIFIABLE INFORMATION INCIDENT (PII) REPORTING REQUIREMENTS

g. Notifications to affected individuals, if required, are to be made as soon as possible, but not later than 10 working days of the discovery of the suspected or confirmed incident. The designated official shall, by written letter or digitally signed email, notify all affected individuals. A sample notification letter is available at:

<http://www.doncio.navy.mil/uploads/SampleBreachNotificationLetter.pdf>. The 10-day period begins after the command/activity is able to determine the identities of the individuals whose information was affected. If the 10 day requirement is not met, the designated official must notify the DON CIO Privacy Office and the TMA Privacy Office by a single e-mail, providing the reason why notification was not made, and what actions are being taken to complete the notification process. For all incidents that require notification, the command/activity is directed to investigate whether DON/DoD policy was followed. In cases where policy was not followed, appropriate disciplinary action should be taken, weighing mitigating circumstances, severity of the PII loss or compromise, and other extenuating factors.

h. The accountable command/activity should use any means that will likely succeed in reaching the impacted individuals, such as establishing a call center (i.e., toll-free number). Guidance for establishing a call center is provided at <http://www.doncio.navy.mil/uploads/CallCenterGuidance.pdf>.

i. The designated official of the accountable command/activity shall complete OPNAV 5214/14, DON Loss or Compromise of Personally Identifiable Information (PII) After Action Reporting Form and notify via a single e-mail the DON CIO Privacy Office, the TMA Privacy Office, and the Navy Medicine CIO IT Privacy & Security Team (BUMED M62) as soon as available, but no later than 30 days after discovery of the incident involving PII. The completed OPNAV 5214/14 can be sent with a built-in e-mailing function (auto-populates the addressees in your local e-mail client); alternatively, it can be saved and attached to an e-mail. The OPNAV 5214/14 should be sent by e-mail and include the information listed below:

- (1) Remedial actions taken to prevent reoccurrence;
- (2) Individual notification status, if notifications were required;
- (3) Lessons learned, if available;
- (4) Disciplinary action taken, where appropriate.

5. My point of contact for this matter is CDR Rich Makarski, at (202) 762-0037 or by email: Richard.Makarski@med.navy.mil.

6. Forms and Reports.

a. The following OPNAV forms are available electronically from the DON Forms Web site at: <https://navalforms.daps.dla.mil/web/public/home>.

Subj: PERSONALLY IDENTIFIABLE INFORMATION INCIDENT (PII) REPORTING
REQUIREMENTS

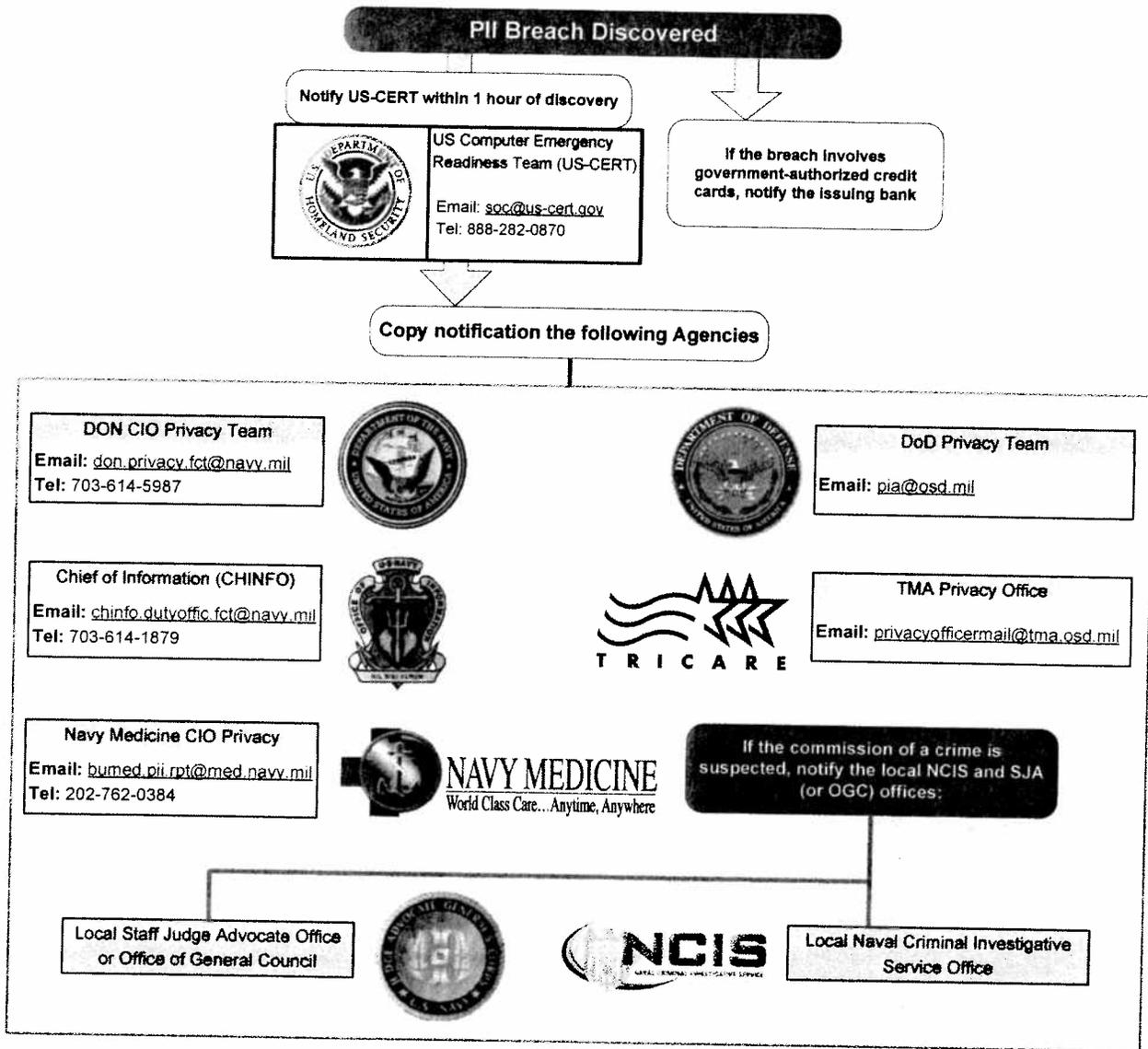
(1) OPNAV 5211/13 (Jun 2009), DON Loss or Compromise of Personally Identifiable Information (PII) Breach Reporting Form.

(2) OPNAV 5211/14 (Jun 2009), DON Loss or Compromise of Personally Identifiable Information (PII) After Action Reporting Form.

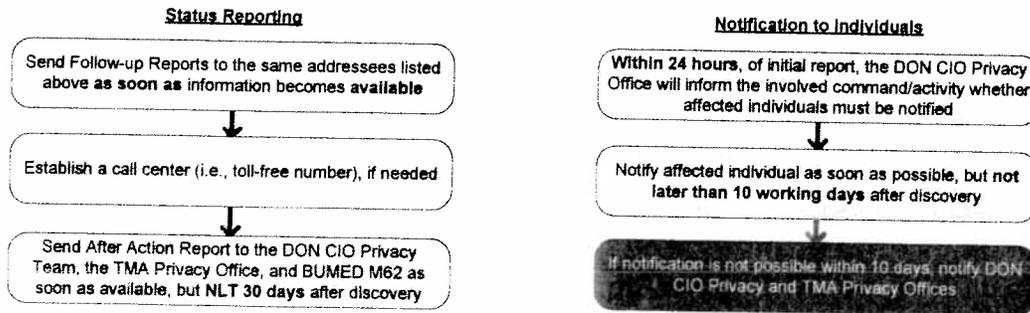
b. The reports required in this BUMED Memorandum are exempt from report control per reference (f), part IV, paragraph 7p.

Adam M. Robinson, Jr.
A. M. ROBINSON, JR.

PII INCIDENT REPORTING FLOWCHART



After One-Hour Reporting



DEPARTMENT OF THE NAVY (DON)
LOSS OR COMPROMISE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)
BREACH REPORTING FORM
OPNAV 5211/13 (Jun 2008)

(this page left intentionally blank)

DEPARTMENT OF THE NAVY (DON) LOSS OR COMPROMISE OF PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACH REPORTING FORM

This form is intended to provide information regarding the INITIAL REPORT of a loss or suspected loss of PII (i.e., a breach). As additional breach information becomes available, this form can be submitted as often as necessary as a SUPPLEMENTAL REPORT. Select the report type from the drop down menu above. **DO NOT DELAY** submission due to lack of information.

US-CERT Number: _____
(In most cases, the US-CERT number will not be available for inclusion in the initial report. Please provide in supplemental report, when available.)

Today's Date: _____

PERSON MAKING INITIAL REPORT

1. Name:	2. Title:
3. Phone Number:	4. E-mail Address:
5. Component (<i>BUMED Activities should Select CNO</i>):	
6. Organization/Branch/Unit Office:	

LOSS OF PII/BREACH INFORMATION

7. Date of Breach: _____ 8. Breach Discovery Date: _____ 9. Breach Discovery Time: _____
(The one hour reporting requirement to notify US-CERT begins at the Date and Time command became aware of the breach. Use military format for time (i.e. 0930, 1455))

10. Individuals Affected by Breach:

Government Civilians: _____	Government Contractors: _____	Military (Active): _____
Military (Reserve): _____	Military (Dependent): _____	Military (Retired): _____
Members of the Public: _____	Other: _____	If Other, Specify: _____

Total Number of Individuals Affected by Breach: _____ 0

11. Type of PII Lost (e.g., SSNs, Financial Data, Medical Data, etc): _____

12. Brief Description of the breach. Do not include specific names or PII of personnel whose information was lost or compromised. _____

DATA STORAGE/COLLECTION MEDIA TYPE INFORMATION

13. Data Storage/Collection/Media Type involved in Breach:	14. If Other or More Than One Type, Specify:
--	--

15. If the Breach Involved Hardware or Equipment, was the equipment (Check All That Apply):

<input type="checkbox"/> Personally Owned	<input type="checkbox"/> Government Owned	<input type="checkbox"/> Contractor Owned
<input type="checkbox"/> Encrypted	<input type="checkbox"/> Password Protected	<input type="checkbox"/> PK Enabled

16. If the Breach Involved a Government Credit Card, was the Issuing Bank Notified: Yes No N/A

17. What was the Cause of the Breach? _____

18. If Other, Specify: _____

ORGANIZATION DESIGNATED OFFICIAL

19. Name:	20. Title:
21. Phone Number:	22. E-mail Address:

Individual Notifications:

Based on information provided in this report, a risk analysis will be conducted by the DON CIO Privacy Office. If the analysis leads to the determination of a high risk potential for identity theft, this report's Organization Designated Official will be contacted within 24 hours and provided with additional guidance regarding the requirement for notifying individuals.

SENIOR OFFICIAL SIGNING NOTIFICATION LETTERS (IF APPLICABLE) (Usually the Commanding Officer)

23. Name:	24. Title:
25. Phone Number:	26. E-mail Address:

Submit Initial Report for SECNAV/NAVY Breaches

Submit Initial Report for MARINE CORPS Breaches

Submit Initial Report for BUMED Breaches

Submit Supplemental Report for SECNAV/NAVY Breaches

Submit Supplemental Report for MARINE CORPS Breaches

Submit Supplemental Report for BUMED Breaches

If this form will not work with your version of Adobe Acrobat, please follow the procedure in DON CIO WASHINGTON DC 291652Z FEB 08 LOSS OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORTING PROCESS or MARINE CORPS ENTERPRISE INFORMATION ASSURANCE DIRECTIVE 011

**DEPARTMENT OF THE NAVY (DON)
LOSS OR COMPROMISE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)
AFTER ACTION REPORTING FORM**

This form is intended to provide additional breach information and the status of follow-up actions as information becomes available. It may be used multiple times, as required.

US-CERT Number: _____
(Please provide when available.)

Today's Date: _____

PERSON MAKING INITIAL REPORT

1. Name:	2. Title:
3. Phone Number:	4. E-mail Address:
5. Component (BUMED Activities should Select CNO):	
6. Organization/Branch/Unit Office:	

ADDITIONAL BREACH INFORMATION AND STATUS OF FOLLOW-UP ACTIONS

7. If it was previously determined that individual notifications were required, provide status of notifications. If not complete, indicate estimated completion date.

8. Provide actions taken to prevent reoccurrence:

9. Provide lessons learned:

10. If breach occurred on a IT system, provide system name:

11. If a paper document or e-mail, was it marked correctly?

Yes No N/A

Submit for SECNAV/NAVY Breaches

Submit for MARINE CORPS Breaches

Submit for BUMED Breaches