

Naval Audit Service



Audit Report



Managing Personally Identifiable Information at Naval Medical Center, Portsmouth and Naval Hospital, Jacksonville

This report contains information exempt from release under the Freedom of Information Act. Exemption (b)(6) applies.

Do not release outside the Department of the Navy, post on non-NAVAUDSVC Web sites, or in Navy Taskers without prior approval of the Auditor General of the Navy.

N2016-0013
29 December 2015

Obtaining Additional Copies

To obtain additional copies of this report, please use the following contact information:

Phone: (202) 433-5757
Fax: (202) 433-5921
E-mail: NAVAUDSVC.FOIA@navy.mil
Mail: Naval Audit Service
Attn: FOIA
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005

Providing Suggestions for Future Audits

To suggest ideas for or to request future audits, please use the following contact information:

Phone: (202) 433-5840 (DSN 288)
Fax: (202) 433-5921
E-mail: NAVAUDSVC.AuditPlan@navy.mil
Mail: Naval Audit Service
Attn: Audit Requests
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005

Naval Audit Service Web Site

To find out more about the Naval Audit Service, including general background, and guidance on what clients can expect when they become involved in research or an audit, visit our Web site at:

<http://www.secnav.navy.mil/navaudsvc>



DEPARTMENT OF THE NAVY
NAVAL AUDIT SERVICE
1006 BEATTY PLACE SE
WASHINGTON NAVY YARD, DC 20374-5005

7510
2014-070
29 Dec 15

MEMORANDUM FOR COMMANDER, NAVAL MEDICAL CENTER,
PORTSMOUTH
COMMANDER, NAVAL HOSPITAL, JACKSONVILLE

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

Ref: (a) NAVAUDSVC memo 7510 2014-070, dated 16 Sep 14
(b) SECNAV Instruction 7510.7F, "Department of the Navy Internal Audit"

Encl: 1. Status of Recommendations
2. Pertinent Guidance
3. Scope and Methodology
4. Activities Visited
5. Glossary of Acronyms
6. Management Response from Naval Medical Center, Portsmouth
7. Management Response from Naval Hospital, Jacksonville

1. **Introduction.** We have completed the subject audit announced in reference (a). Paragraph 8 provides a summary of audit results. The audit found opportunities to improve personally identifiable information (PII) procedures and internal controls, including the disposal of medical equipment that may contain PII/protected health information (PHI). Paragraph 9 provides our recommendations to the Commanders for Naval Medical Center, Portsmouth (NMCP) and Naval Hospital, Jacksonville (NHJAX), and their summarized responses. Management took or plans appropriate corrective actions on all of the recommendations.

2. **Reason for Audit.** The audit objectives were to verify that selected Department of the Navy (DON) East Coast commands' internal controls (1) were operating effectively to protect PII from unauthorized disclosure, and (2) ensure sufficient disposal of medical treatment equipment containing PII. This audit specifically focused on NMCP and NHJAX. We conducted this audit because PII vulnerability was identified as a high risk by the DON Chief Information Officer (CIO) in the Fiscal Year (FY) 2014 annual risk assessment. Our focus on medical treatment equipment PII was due to Chief, Bureau of

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

Medicine and Surgery (BUMED) personnel stating that BUMED medical treatment equipment containing PII and/or PHI may not have been disposed of properly.

3. Background.

a. BUMED's mission is to: (1) ensure personnel and material readiness of shore activities as assigned by the Chief of Naval Operations; (2) develop health care policy for all shore-based treatment facilities and operating forces of the Navy and Marine Corps; (3) provide technical support in the direct health care delivery system of shore-based treatment facilities and operating forces of the Navy and Marine Corps; and (4) manage the use of the Civilian Health and Medical Program of the Uniformed Services, and other indirect health care delivery systems. BUMED is the Echelon 2 Headquarters of Navy Medicine. Navy Medicine consists of three Echelon 3 (Flag level) commands – Navy Medicine West, Navy Medicine East, and Navy Medicine Education and Training Command. Subordinate Echelon 4 commands under Navy Medicine East include Naval Medical Center, Portsmouth, VA and Naval Hospital, Jacksonville, FL. Activities visited during this audit are identified in Enclosure 4.

b. The Privacy Act of 1974 established requirements for Federal agencies maintaining information in a system of records. The Department of Defense's (DoD's) definition of a system of records is a group of records under the control of a DoD component from which personal information is retrieved by the individual's name or by some identifying number, symbol, or other identifier assigned to an individual. This type of information was previously called "Privacy Act Information" and "protected personal information." It is now referred to as PII.

4. Briefings with Management. Opening conferences were held with officials at BUMED on 30 September 2014, NMCP on 3 November 2014, and NHJAX on 10 March 2015. We kept the commands apprised of our progress throughout the audit. The closing conference was held on 14 October 2015.

5. The Federal Information Security Management Act (FISMA) permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000, which expired in November 2002. Under the provisions of FISMA, DoD must provide Congress with an annual report on DoD's information assurance posture. DON CIO submits DON input for the DoD FISMA report. Additionally, FISMA requires an annual independent evaluation of an agency's information security program and practices to determine the effectiveness of such program and practices. The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to the programs or practices of the applicable agency. DON CIO can use this report in partially meeting that requirement.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

6. Federal Managers' Financial Integrity Act (FMFIA) of 1982. This Act, as codified in Title 31, United States Code, requires each Federal agency head to annually certify the effectiveness of the agency's internal and accounting system controls. Recommendations 1 through 19 address issues related to the internal control weaknesses in the use, collection, safeguarding, and disposal of PII. In our opinion, the internal control weaknesses noted in this report are significant issues of noncompliance with the DON Privacy Act Program and could potentially result in the compromise of PII. Therefore, this audit in conjunction with other similar audits, shows that insufficient controls over PII may warrant reporting in the Auditor General's annual FMFIA memorandum identifying management control weaknesses to the Secretary of the Navy.

7. Scope and Methodology. The audit was conducted at two Navy Medicine East commands, NMCP and NHJAX, from 30 September 2014 to 19 November 2015. Our audit scope included steps to determine whether the commands' internal controls were operating effectively to protect PII from unauthorized disclosure and that medical equipment containing PII or PHI were sufficiently disposed of. In addition, we reviewed policies and procedures related to PII. We reviewed matters related to the Privacy Act program, semi-annual spot checks, disposal methods, internal PII/PHI forms, safeguarding PII, and PII breach reporting. We examined the sufficiency of the disposal of medical treatment equipment containing PII by requesting relevant records, and analyzing judgmental samples from equipment disposal records. Enclosure 3 provides details concerning the scope and methodology used for the audit. Enclosure 2 contains the guidance used during this audit. Enclosure 5 is a glossary of acronyms contained in this report.

8. Audit Results. We examined PII internal controls at NMCP and NHJAX. The examinations were conducted through analyses, interviews, and reviews of appropriate documentation and information systems. We found opportunities for improvement in the following areas:

- Staff assistance visits;
- Semi-annual PII spot checks;
- Disposal method policy;
- Internal PII/PHI forms;
- Technical safeguards;
- Breach reporting; and
- Medical equipment disposal.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

These conditions occurred because: (1) improvement was needed in monitoring and oversight of the Privacy Act program; and (2) DON guidance and internal controls were not fully implemented. When internal controls are not properly implemented and executed, there is an increased risk of personal information compromise, and a limited ability to plan for and respond to unintended releases, breaches, or unauthorized disclosures. This could result in identity theft or fraud, which would have a negative impact on DON and the individuals whose PII/PHI is compromised.

a. **Staff Assistance Visits.** NHJAX had not fully implemented the Privacy Act guidance contained within Secretary of the Navy (SECNAV) Instruction 5211.5E. This instruction requires the Privacy Act Coordinator (PAC) to conduct and document staff assistance visits within their command and lower echelons to ensure compliance with the Privacy Act. Based on interviews conducted with the NHJAX PAC, we determined staff assistance visits at NHJAX and lower echelon commands (i.e., branch clinics, dental clinics) were not conducted or documented.

b. **Semiannual PII Spot Checks.** NHJAX did not conduct and document semiannual PII spot checks as required by SECNAV Message 042232Z of October 2007. This policy requires commanding officers to ensure that supervisors conduct and document spot checks of their assigned areas of responsibility, focusing on those areas that deal with PII on a regular basis. The PAC had been in this position more than a year and was aware of the requirement but had not performed semiannual PII spot checks as of the time of our audit.

c. **Disposal Method Policy.** The disposal method policy outlined in NHJAX Instruction 5211.7A does not reflect the current disposal process used. Currently, an authorized contractor comes to the hospital once a week and destroys documents on site by a secure information destruction process that renders PII unrecognizable or beyond reconstruction, as required by SECNAV Instruction 5211.5E. However, NHJAX Instruction 5211.7A states cross-cut shredders are to be used on-site by the command. Since auditors observed the disposal process that is in place, and it does not include the use of cross-cut shredders, we recommend that the NHJAX Instruction be updated to reflect the current policy of using an authorized contractor that destroys documents on site by a secure destruction process. NHJAX personnel stated that the hospital implemented this disposal process almost a year ago. In addition, the audit team also observed straight-cut shredders in multiple departments. If used on PII/PHI documents, these shredders are not sufficient to render PII/PHI unrecognizable per SECNAV guidance. To mitigate the potential for PII/PHI documents being shredded improperly, straight-cut shredders should be removed from administrative areas.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

d. **Internal PII/PHI Forms.** We examined internal forms at NMCP and NHJAX used to collect PII/PHI information.

(1) **Approval Process for Internal Forms.** We examined the form processes at NMCP and NHJAX. At each activity a form¹ was found that was not reviewed and approved by the Activities' Forms Manager Officers, as required by BUMED Instruction 5210.9B. The instruction directs that when Navy Medical Department personnel within an activity require a form they shall use, in order of precedence, General Services Administration Standard or Optional forms, then DoD forms, and finally existing DON (including Navy Medicine) forms. If there are no existing forms that will suit their needs, the last option is to create a new Navy Medicine Activity form. This option requires approval and assignment of a form number from the Activity Forms Manager.

(2) **Privacy Act Statement on Internal Forms.** We found one internal form at NMCP that was not marked with a Privacy Act statement nor any indication that the individuals were to be informed of the Privacy Act notice. SECNAV Instruction 5211.5E has explicit requirements on how to notify individuals of the Privacy Act when collecting their PII.

e. **Technical Safeguards.** Technical safeguards for PII/PHI at NMCP and NHJAX need improvement. SECNAV Instruction 5211.5E states that DON activities are responsible for establishing appropriate administrative, technical, and physical safeguards to ensure that the documents in every system of records are protected from unauthorized alteration or disclosure. They are also responsible for ensuring that confidentiality is protected. Additionally, Navy Medicine (NAVMED) Policy 08-005 requires that when transmitting PII or PHI by e-mail, the subject line of the message should include "FOUO."² This sensitivity marking appries the receiver of the need to properly protect the information. When PHI or PII is to be transmitted by e-mail, Navy Medicine personnel shall only use Government-furnished equipment and software, and encrypt the sensitive information with DoD-approved encryption methods prior to transmission. This requires authorized, non-DoD recipients to use a DoD-approved digital certificate to encrypt and decrypt sensitive e-mail. In addition, DON CIO Message 201839Z of November 2008 states that command leadership must ensure that proper controls and permissions are in place to safeguard data on a shared drive.

(1) At NMCP, 8 "sent" e-mails were arbitrarily selected for review at each of the 5 departments visited for a total of 40 e-mails reviewed. Of these, 12 of the "sent" e-mails contained PII/PHI and were further evaluated. We found 11 of these 12 e-mails did not include "FOUO" in the subject line of message and 6 of the 12 e-mails were not

¹ The forms found were different at each of the activities. Each of the forms collected PII or PHI.

² "For Official Use Only"

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

encrypted. Also, 7 of 9³ e-mails had attachments containing PII/PHI information that did not include the required FOUO statement.

(2) In addition, NMCP management at all five departments assessed did not know whether all personnel with access to shared drives had a need to know for the information contained on those shared drives.

(3) At NHJAX, 8 “sent” e-mails were arbitrarily selected for review at each of the 5 departments visited for a total of 40 reviewed e-mails. Only the sent e-mails containing PII/PHI were further evaluated. From the 40 sent e-mails, 10 contained PII/PHI. We found 8 of the 10 sent e-mails with PII/PHI did not include “FOUO” in the subject line of the message, and 7 of 7⁴ e-mails had attachments containing PII/PHI information that did not include the required FOUO statement. Also, 4 of 9⁵ e-mails sent with PII/PHI were not encrypted.

f. **Breach Reporting.** NAVMED Policy 09-016 requires reporting within 1 hour of the discovery of a known or suspected incident of a PII/PHI breach. In four of the four departments assessed at NMCP, personnel were unaware of the timeframe to report a breach. At each of the departments assessed, personnel interviewed gave incorrect answers that did not match the reporting timeframe requirement.

g. **Disposal of Medical Equipment.** The disposal process for medical equipment potentially containing PII and PHI needed improvement at NMCP and NHJAX. We judgmentally selected a sample of 111 items of equipment that the command determined had been disposed of in FYs 2013 or 2014; 80 items were from NMCP, and 31 were from NHJAX. We then determined, through discussion with the command, that a total of 56 equipment sample items that we assessed had hard drives capable of storing PII/PHI: 38 from NMCP and 18 from NHJAX. The sample selection for our assessment of disposal documentation is summarized in Table 1.

³ Three e-mails were not assessed for FOUO on attachments because it was determined the attachments were generated externally.

⁴ Three e-mails were not assessed for this element because it was determined the attached forms were generated externally.

⁵ One e-mail was not assessed for encryption because NHJAX was unable to send encrypted e-mails to that specific recipient at the time.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

Table 1: Sample Selection for Disposal Documentation Assessment

111 Items of Equipment	NMCP	NHJAX
Equipment Disposed of by Command in FYs 2013 and 2014	80	31
Equipment Having Hard-drives (56 total)	38	18
Proof of final disposition/destruction	0	16

(1) **Disposal Review.** We requested relevant disposal documentation for each sample item. This included the (1) DD Form 1348-1A (Issue Release/Receipt Document), (2) Excess Property Turn-In Document (used at NMCP) or DD Form 1149 (Requisition and Invoice/Shipping Document used at NHJAX), and (3) Defense Medical Logistics Standard Support (DMLSS)⁶ screenshots. We reviewed the documentation for the following elements as required by the Navy Medicine Equipment Management Manual or BUMED FY 2014 Logistics Guidance:

- Existence of a signed DD Form 1348-1A Turn-In Document;
- Existence of an Excess Property Turn-In Document (used at NMCP) or a DD Form 1149 (used at NHJAX) for transfer of custody;
- Annotation of a condition code in DMLSS;
- Annotation of the date of destruction in DMLSS;
- Annotation of the method of destruction in DMLSS;
- Annotation of the name of the sanitizer (individual performing destruction) in DMLSS;
- Annotation of the rank/grade of the sanitizer in DMLSS;
- Annotation that equipment meets the disposition requirements in accordance with DoD memo, “Disposition of Unclassified Computer Hard Drives,” dated 4 June 2001, on DD Form 1348-1A, Box 27; and
- Documentation showing final disposition of the hard drives (both forms of documentation below are acceptable per guidance):

⁶ The DMLSS information technology system delivers an automated and integrated information system with a comprehensive range of medical materiel, equipment, war reserve materiel, and facilities management functions.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL, JACKSONVILLE (AUDIT REPORT N2016-0013)**

- Documentation showing that the hard drive was degaussed and destroyed by Information Management Department personnel at NHJAX; or
- NMCP receiving documentation from the National Security Agency (NSA) showing that the hard drive was sent to NSA and subsequently destroyed by NSA.

(2) **Disposal Review Results.** Both NMCP and NHJAX did not fully comply with guidance governing the destruction of equipment containing PII/PHI. The results for each element at both locations are summarized in Table 2. We reviewed 38 sample items at NMCP and 18 sample items at NHJAX.

Table 2: Results of Disposal Documentation Assessment

Elements Assessed	NMCP	NHJAX
Signed DD Form 1348-1A	37	17
Excess Property Turn-In Document (NMCP)/DD Form 1149 (NHJAX)	38	16
Annotation of condition code	37	18
Annotation of date of destruction	0	14
Annotation of method of destruction	0	14
Annotation of name of sanitizer	3	14
Annotation of rank/grade of sanitizer	3	14
DD Form 1348-1A annotated that equipment disposition requirements met	12	14
Proof of final disposition/destruction	N/A	16 ⁷

(a) Both NMCP and NHJAX could not provide a signed DD Form 1348-1A for one of their sampled pieces of equipment. Additionally, NHJAX could not provide a DD Form 1149 for two of their sampled pieces of equipment, and NMCP did not annotate the condition code in DMLSS for one sampled piece of equipment.

(b) NMCP did not annotate in DMLSS the date and method of destruction for any of the 38 sampled pieces of equipment, and did not annotate the name and rank/grade of the sanitizer for 35 sampled pieces of equipment. This occurred because the

⁷ For one sample, destruction of the hard drive was pending at the time of review.

**Subj: MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

equipment is deactivated in DMLSS once it is transferred to the Defense Logistics Agency (DLA). At the time of transfer, NMCP did not want the equipment to continue being counted in their inventory, so they closed it out in DMLSS. However, once a piece of equipment is removed from DMLSS, it cannot be updated further without reactivating the equipment record in the inventory. The receipt of the date and method of destruction is often provided months later by NSA after they perform the destruction, and it is not a priority to input this information into the DMLSS records. Because of this, required elements of disposition are not documented in DMLSS as required by the FY 2014 Logistics Guidance. NMCP processes hard drive disposal to NSA in batches. The NMCP procedures do not specify timing of hard drive disposals. Management agreed that a quicker transfer schedule would help alleviate this problem and suggested a weekly transfer, when applicable. Also, the Information Management Department at NMCP did not provide the Equipment Management Department with a listing of serial numbers from the removed hard drives and the corresponding serial numbers of the equipment from which the hard drives were removed. The Equipment Manager needs this information to do the required DMLSS updates. Information Management should update the policy to include sending hard drives to NSA for destruction on a more frequent basis to expedite the return information on destruction. These actions will help alleviate the time gap between disposition and proof of destruction and allow NMCP to match the pieces of equipment that have had their hard drives removed. In addition, the Equipment Department should document in DMLSS, the date, rank, and name of person that destroyed the hard drive in each instance and the method of destruction for each piece of disposed equipment with the capability of storing PII.

(c) NMCP did not annotate that the equipment met the disposition requirements on the DD Form 1348-1A for 26 of the sampled pieces of equipment, because the NMCP Biomedical Engineering Division was unaware of this requirement. NMCP personnel had interpreted the requirements for medical and computer equipment as separate even though that was not the Naval Medical Logistics Command's intent in their guidance. The annotation did not occur on any of the sampled items of medical equipment. The FY 2014 Logistics Guidance gives specific requirements for disposal of hard drives and specific references for Automated Data Processing equipment. At the staff level, this equipment was deemed to be computer equipment only and separate from medical equipment. Due to this erroneous interpretation, the policy regarding the disposition of hard drives in the FY 2014 Logistics Guidance was not applied to hard drives found within medical equipment. NMCP should coordinate with Naval Medical Logistics Command to update the Logistics Guidance to ensure the DD Form 1348-1A is properly annotated for medical equipment.

(d) NMCP's noncompliance with guidance requiring the annotation of all the required elements in DMLSS and on the DD Form 1348-1A could result in their being

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

unable to verify that equipment was sanitized of PII and PHI, thus increasing the risk of a PII breach.

(e) NHJAX did not annotate in DMLSS the date and method of destruction, or the name and rank/grade of the sanitizer for four pieces of sampled equipment. NHJAX also did not annotate that the equipment met the disposition requirements on the DD Form 1348-1A for the same four samples. Corrective action has been taken by the command.

(f) NHJAX could not verify the destruction of one hard drive because their Biomedical Engineering Division initially did not indicate that the equipment had PII or computer hard drive elements. The equipment was submitted for normal disposal to DLA since there was no indication that PII or PHI was present. Based on the survey results, NHJAX processed the equipment for transfer to DLA without completing required documentation regarding the proof of hard drive removal. NHJAX's inability to prove destruction of the hard drive presents a risk that the hard drive is still intact and could be acquired outside of DON. This could cause a violation of Health Insurance Portability and Accountability Act regulations regarding confidentiality of PHI. The Material Management Department, which is responsible for equipment disposal at NHJAX, should amend their disposal process to ensure that: (1) equipment is tested for the capability of storing PII; (2) equipment capable of storing PII is marked as such in DMLSS; and (3) DMLSS is checked for the capability of storing information at the beginning of the disposal process.

9. Recommendations and Corrective Actions. Our recommendations, summarized management responses, and our comments on the responses are below. The complete management responses are in Enclosures 6 and 7.

We recommend that Commander, Naval Medical Center, Portsmouth:

Recommendation 1. Provide training and awareness to personnel to ensure that forms used to collect personally identifiable information are formally reviewed and approved prior to use, as required by Department of the Navy Bureau of Medicine and Surgery Instruction 5210.9B.

Management response to Recommendation 1. Concur. Forms Management personnel currently interact with clinical and administrative areas through the "Executive Officer (XO) Rounds" process. Through this process, which includes an outbrief of findings with the Division Officer and often the Department Head as well as other key personnel, the Forms Management Officer can provide training and awareness on discrepancies in the collection of personally identifiable information (PII). In addition, in order to ensure Forms and Reports requirements

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL, JACKSONVILLE (AUDIT REPORT N2016-0013)**

are being met, the Naval Medical Center Portsmouth (NMCP) intranet will be updated to include a simple set of directions to follow for assistance with the submission of forms. Plan of the Day and All Hands notices will be utilized to direct to NMCP staff to the revised NMCP intranet page and provide Forms Management point of contact information. The target completion date for the Forms Management intranet site is April 2016.

Naval Audit Service comment on response to Recommendation 1. Actions taken and planned by Commander, Naval Medical Center, Portsmouth, meet the intent of the recommendation, which is considered open pending completion of the agreed-to actions.

Recommendation 2. Provide oversight to ensure that the Forms Manager Officers review forms in their control for the required Privacy Act statements, as required by Secretary of the Navy Instruction 5211.5E.

Management response to Recommendation 2. Concur. A Tiger Team is inspecting the case files of all NMCP internal forms. The estimated rate of inspection is 25 case files per month out of 416 total case files. Through these inspections, discrepancies for the proper display of Privacy Act statements on forms can be documented. Addressing Privacy Act statement discrepancies will be coordinated through the Department Heads and Division Officers. All forms found to be noncompliant with Secretary of the Navy Instruction 5211.5E will be revised or cancelled with the proper corresponding action utilizing DD Form 67. The estimated completion date of the case file audit is April 2017.

Naval Audit Service comment on responses to Recommendation 2. Actions taken and planned by Commander, Naval Medical Center, Portsmouth, meet the intent of the recommendation, which are considered open pending completion of the agreed-to actions. In subsequent communication, management provided a new estimated completion date of 1 October 2016.

Recommendation 3. Provide training and awareness for personnel to ensure that personally identifiable information on e-mail is properly safeguarded in accordance with Navy Medicine Policy 08-005.

Management response to Recommendation 3. Concur. NMCP will:
(a) increase the publication of messages to staff personnel on the Plan of the Day, All Hands and Intranet Home Page concerning the Navy Medicine Policy 08-005 on safeguarding requirements; (b) distribute Awareness Briefs to Share Point managers to publish for their staffs' situational awareness about this requirement (Share Point managers will maintain records documenting when their staff

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

reviewed Awareness Briefs); (c) implement quarterly (or more frequently, if necessary) spot checks for compliance with this standard and maintain written records documenting the outcome of these reviews; (d) report all noncompliant safeguarding practices to the appropriate office immediately upon detection; and (e) continue to educate staff during command assessments, XO Rounds, command orientation, audits, spot-checks, and during semiannual performance reviews when standards are established and/or reviewed. The target completion date is 30 September 2016.

Recommendation 4. Review the current computer access policy and educate shared folder owners so that they ensure only those with a “need to know” have access in accordance with Department of the Navy Chief Information Officer Message 201839Z.

Management response to Recommendation 4. Concur. NMCP will publish a local instruction regarding a new shared information access policy and will be working with departments to ensure that only those with a “need to know” have access. The target completion date is 1 March 2016.

Recommendation 5. Provide additional training to ensure that personnel know the proper timeframe to report a breach in accordance with Navy Medicine Policy 09-016.

Management response to Recommendation 5. Concur. NMCP will: (a) increase the publication of Plan of the Day and all hands messages to staff concerning Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules; and (b) continue to educate staff during command assessments, XO Rounds, command orientation, annual required training, and during semiannual performance reviews when standards are established and/or reviewed. The target completion date is 30 November 2016.

Recommendation 6. Provide oversight to ensure that the Equipment Management Department documents, in Defense Medical Logistics Standard Support, include the date, rank, and the name of the person who destroyed a hard drive in each instance, and the method of destruction for each piece of disposed equipment with the capability of storing personally identifiable information, as required by Navy Bureau of Medicine and Surgery Fiscal Year 2014 Logistics Guidance.

Management response to Recommendation 6. Concur. Equipment Management Division is working with Information Management Division to ensure that the date, rank, and name of the person who destroyed a hard drive in each instance, and the method of destruction for each piece of disposed equipment with the capability of storing PII, are included and documented in Defense

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL, JACKSONVILLE (AUDIT REPORT N2016-0013)**

Medical Logistics Standard Support (DMLSS). If using the National Security Agency (NSA) for hard drive destruction, the date, shippers tracking number, and the rank and name of the person who shipped the hard drive will be included and documented in DMLSS. A standard operating procedure is being written between Equipment Management Division and Information Management Division to implement the recommendation. Target completion date is 1 February 2016.

Naval Audit Service comment on responses to Recommendations 3 through 6. Actions taken and planned by Commander, Naval Medical Center, Portsmouth, meet the intent of the recommendations, which are considered open pending completion of the agreed-to actions.

Recommendation 7. Update policy to include sending hard drives to the National Security Agency for destruction on a weekly basis to expedite receipt of confirmation of hard drive destruction.

Management response to Recommendation 7. Concur. NMCP will update the policy to include sending hard drives to NSA for destruction on a weekly or as-needed basis to expedite receipt of confirmation of hard drive destruction. Equipment Management Division will work with Information Management Division to complete a standard operating procedure for this process, with a target completion date of 1 February 2016.

Naval Audit Service comment on response to Recommendation 7. Actions planned by the Commander, Naval Medical Center, Portsmouth, meet the intent of the recommendation, which was to expedite the receipt of confirmation of hard drive destruction. This recommendation is considered open pending completion of the agreed-to actions.

Recommendation 8. Provide oversight to ensure the Information Management Department provides the Equipment Management Department with a listing of hard drives that have been removed that includes the hard drive serial number and the equipment serial numbers.

Management response to Recommendation 8. Concur. Information Management Division will provide Equipment Management Division with a listing of hard drives that have been removed that includes the hard drive and equipment serial numbers along with the shipping tracking number verifying delivery to NSA. Equipment Management Division will ensure that the information is entered into DMLSS. Equipment Management Division will work with Information Management Division to include this recommendation in the

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL, JACKSONVILLE (AUDIT REPORT N2016-0013)**

Excess standard operating procedures, with a target completion date of 1 February 2016.

Naval Audit Service comment on response to Recommendation 8. Actions planned by Commander, Naval Medical Center, Portsmouth, meet the intent of the recommendation, which is considered open pending completion of the agreed-to actions.

Recommendation 9. Coordinate with Naval Medical Logistics Command to update Fiscal Year 2014 Logistics Guidance to ensure that the DD Form 1348-1A is properly annotated for medical equipment.

Management response to Recommendation 9. Concur. NMCP coordinated with Naval Medical Logistics Command to update Fiscal Year 2014 logistics guidance to ensure that the DD Form 1348-1A is properly annotated for medical equipment. Fiscal Year 2015 logistics guidance was updated with the correct information. Action considered complete.

Naval Audit Service comment on response to Recommendation 9. Actions taken by Commander, Naval Medical Center, Portsmouth, meet the intent of the recommendation. This recommendation is considered closed as of 14 December 2015 (the date of the management response package).

We recommend that Commander, Naval Hospital, Jacksonville:

Recommendation 10. Provide training and awareness to personnel to ensure that forms used to collect personally identifiable information are formally reviewed and approved prior to use, as required by Department of the Navy Bureau of Medicine and Surgery Instruction 5210.9B.

Management response to Recommendation 10. Concur. The command published a Forms Management Program Instruction dated 13 August 2015. It specifically outlines procedures for use and approval of forms using PII. The command's Forms Control Committee has a representative from each directorate that monitors all forms used for version control and updates. The command has bi-monthly meetings in which each directorate representative will present all forms for revision/approval, at which time the documents are screened for PII/HIPAA compliance. The notes concerning the precedence of forms are well understood by the Forms Control Committee, and higher echelon forms are used whenever possible. Our legal office is included in the routing of all forms when PII is involved and there is also a legal representative who sits on the Forms Control Committee. The Committee will ensure the "For Official Use Only"

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

statement is annotated on all forms containing PII. The command is currently in the process of screening all forms and has an estimated completion date of March 2016.

Naval Audit Service comment on response to Recommendation 10. In subsequent communication, the command provided a copy of the published Forms Management Program Instruction dated 13 August 2015, which included training and awareness of the requirement for formal review and approval of forms used to collect PII. The instruction, combined with actions planned by Commander, Naval Hospital, Jacksonville, meet the intent of the recommendation, which is considered open pending completion of the agreed-to actions.

Recommendation 11. Establish controls and provide oversight to ensure that staff assistance visits are conducted and documented in accordance with Secretary of the Navy Instruction 5211.5E.

Recommendation 12. Establish controls and provide oversight at the lower echelons (i.e., branch clinics, dental clinics) to ensure that staff assistance visits are conducted and documented in accordance with Secretary of the Navy Instruction 5211.5E.

Management response to Recommendations 11 and 12. Partially concur. Secretary of the Navy Instruction 5211.5E specifically requires “Navy Echelon 2 and 3 Commands and Marine Corps Major Subordinate Commands” to, among other things, “(11) Conduct staff assistance visits or program evaluations within their command and lower echelon commands to ensure compliance with the Privacy Act (PA).” Naval Hospital Jacksonville is an Echelon 4 command. Currently, staff assist visits that conduct “program evaluations” are tracked and documentation collected through our Command Evaluation Program Coordinator to ensure compliance with the Privacy Act Instruction. Our last evaluation was completed in the 4th quarter, Fiscal Year 2015. Navy Medicine East is scheduled to provide assist visit the week of 25-29 January 2016.

Naval Audit Service comment on responses to Recommendations 11 and 12. Although documentation of assistance visits was not provided to us during the audit visit, we subsequently learned there was a reorganization and Naval Hospital Jacksonville is now an Echelon 4 activity and is no longer required to conduct staff visits. With the reorganization, Navy Medicine East will conduct the staff assistance visits as the Echelon 3, and we saw documentation of staff assistance visits done at Navy Medicine East. These actions, combined with Naval Hospital Jacksonville’s tracking of program evaluations and the

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

completion of such an evaluation in the 4th quarter of Fiscal Year 2015, meet the intent of the recommendations. The recommendations are considered closed as of as of 14 December 2015 (the date of the management response package).

Recommendation 13. Establish controls and provide oversight to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with the Secretary of the Navy Message 042232Z of October 2007.

Recommendation 14. Establish controls and provide oversight at the lower echelons (i.e., branch clinics, dental clinics) to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with the Secretary of the Navy Message 042232Z of October 2007.

Management response to Recommendations 13 and 14. Concur on both. Naval Hospital Jacksonville Instruction 5211.5D has been revised and is currently routing for signature by the Commanding Officer. This will specifically annotate the requirement to conduct semiannual spot checks throughout the hospital and at each of our branch health clinics. Our most recent semiannual spot checks were conducted at Naval Hospital Jacksonville and all our branch health clinics between 30 July and 4 September, and addressed all areas and items delineated in Secretary of the Navy message 042232Z of October 2007. Document file is retained in the Command legal office.

Naval Audit Service comment on responses to Recommendations 13 and 14. Actions planned by Commander, Naval Hospital, Jacksonville, meet the intent of the recommendations. In subsequent communication, management indicated that Naval Hospital Jacksonville Instruction 5211.5D is expected to be approved and signed by 29 January 2016. Recommendations 13 and 14 are considered open pending completion of the agreed-to actions.

Recommendation 15. Update the Naval Hospital, Jacksonville Instruction 5211.7A, "Health Insurance Portability and Accountability Act (HIPAA)," to align with current disposal processes to render personally identifiable information records unrecognizable or beyond reconstruction as required by Secretary of the Navy Instruction 5211.5E.

Management response to Recommendation 15. Concur. Navy Hospital Jacksonville Instruction 5211.7A Change Transmittal 1 signed 15 April 2015

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL, JACKSONVILLE (AUDIT REPORT N2016-0013)**

outlines the current disposal policy using contracted services with onsite crosscut shredding.

Recommendation 16. Remove shredders that do not render personally identifiable information/protected health information unrecognizable from departments, as required by Secretary of the Navy Instruction 5211.5E.

Management response to Recommendation 16. Concur. Naval Hospital Jacksonville Operations Management Department is constantly conducting rounds to ensure all unauthorized shredders have been removed from the facility. A current sweep of the facility and its outlying buildings was performed the week of 5 October 2015, and resulted in the removal of 10 unauthorized shredders. Every space has been inspected within the facility and is 100 percent compliant. We will perform spot checks to ensure continued compliance.

Recommendation 17. Provide training and awareness for personnel to ensure that personally identifiable information is properly safeguarded in accordance with Navy Medicine Policy 08-005.

Management response to Recommendation 17. Concur. Naval Hospital Jacksonville was 100 percent compliant with the annual HIPAA and PII training. Also Naval Hospital Jacksonville Instruction 5211.7A CH-1 dated 15 April 2015 specifically addressed items in Navy Medicine Policy 08-005. This was passed via command postmaster and through the Executive Steering Council.

Recommendation 18. Provide oversight to ensure that: (1) the Material Management Department amends the disposal process; (2) equipment is tested for capability of storing personally identifiable information; (3) equipment capable of storing personally identifiable information is marked as such in Defense Medical Logistics Standard Support; and (4) Defense Medical Logistics Standard Support is checked for the capability of storing personally identifiable information at the beginning of the disposal process.

Management response to Recommendation 18. Concur. We recognized in 2013 that we were not in compliance with Naval Medicine Logistics Command Fiscal Year 2014 logistics guidance with reference to disposal and documentation of equipment with hard drives that have the capability of storing PII. We corrected ourselves and since the spring of 2013 have been in compliance with NMLC's annual guidance.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL, JACKSONVILLE (AUDIT REPORT N2016-0013)**

Our process since spring 2013: Step (1): When a piece of equipment is presented to Equipment Management for transfer to Defense Reutilization Marketing Office, Biomedical Repair conducts the assessment to determine if the equipment is capable of storing PII/PHI and removes any hard drives. The equipment is transferred to Equipment Management Division and the hard drive is presented to Management Information Department for destruction. Steps (2) and (3) are completed by Biomedical Repair once a new piece of equipment arrives at the Command as part of the acceptance check. If a piece of equipment has the capability of storing PII/PHI, the “Contains Patient Data” indicator in DMLSS is checked. Step (4) is completed by Biomedical Repair once a piece of equipment has been identified for transfer to the Defense Reutilization Marketing Office. The Biomedical Repair Technician codes the equipment and assesses the equipment for capability of storing PII on the DD 1149 (transfer document).

The Naval Audit Service team visit triggered us to streamline the disposal process of equipment with PII/PHI. Effective 10 March 2015, Biomedical Repair is now required to surrender the equipment with hard drive to Equipment Management. Equipment Management is now required to surrender the hard drive to Management Information Department for disposal. This ensures the chain of custody, the destruction and the proper documentation required in DMLSS with regards to equipment PII/PHI. The same procedures also apply to the outlying branch clinics.

Naval Audit Service comment on responses to Recommendations 15 through 18. Actions taken by Commander, Naval Hospital, Jacksonville meet the intent of the recommendations. These recommendations are considered closed as of 14 December 2015 (the date of the management response package).

10. Followup and Additional Information.

a. Actions taken and planned by Naval Medical Center, Portsmouth meet the intent of Recommendations 1 through 9. Recommendations 1 through 8 are closed. Recommendation 9 is considered open pending completion of the planned corrective actions.

b. Actions taken and planned by Naval Hospital, Jacksonville meet the intent of Recommendations 10 through 18. Recommendations 11, 12, and 15 through 18 are closed. Recommendations 10, 13, and 14 are considered open pending completion of the planned corrective actions.

c. All open recommendations are subject to monitoring in accordance with reference (b). Management should provide a written status report on the

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT
NAVAL MEDICAL CENTER, PORTSMOUTH AND NAVAL HOSPITAL,
JACKSONVILLE (AUDIT REPORT N2016-0013)**

recommendations within 30 days after target completion dates. Please provide all correspondence to the Assistant Auditor General for Financial Management and Comptroller Audits, Ms. Ellen Smith, XXXXXXXXXXXX, with copies to the Director, Policy and Oversight, XXXXXXXXXXXX, XXXXXXXXXXXX and the Naval Audit Service Followup Coordinator, XXXXXXXXXXXX, XXXXXXXXXXXX. Please submit correspondence in electronic format (Microsoft Word or Adobe Acrobat file), and ensure that it is on letterhead and includes a scanned signature.

FOIA
(b)(6)

d. Any requests for this report under the Freedom of Information Act must be approved by the Auditor General of the Navy as required by reference (b). This audit report is also subject to followup in accordance with reference (b).

e. In order to protect privacy and other sensitive information included in this report, we request that you do not release this report outside the Department of the Navy, post on non-Naval Audit Service Web sites, or in Navy Taskers without the prior approval of the Auditor General of the Navy.

f. We appreciate the cooperation and courtesies extended to our auditors.



ELLEN L. SMITH
Assistant Auditor General
Financial Management and Comptroller Audits

FOIA
(b)(6)

Copy to:
UNSECNAV
DCMO
OGC
ASSTSECNAV FMC
ASSTSECNAV FMC (FMO)
ASSTSECNAV EIE
ASSTSECNAV MRA
ASSTSECNAV RDA
CNO (VCNO, DNS-33, N40, N41)
CMC (DMCS, APMC)
BUMED
DON CIO
NAVINSGEN (NAVIG-14)
AFAA/DO

Status of Recommendations

Recommendations							
Finding ⁸	Rec. No.	Page No.	Subject	Status ⁹	Action Command	Target or Actual Completion Date	Interim Target Completion Date ¹⁰
1	1	10	Provide training and awareness to personnel to ensure that forms used to collect personally identifiable information are formally reviewed and approved prior to use, as required by Department of the Navy Bureau of Medicine and Surgery Instruction 5210.9B.	O	Commander, Naval Medical Center, Portsmouth	4/30/16	
1	2	11	Provide oversight to ensure that the Forms Manager Officers review forms in their control for the required Privacy Act statements, as required by Secretary of the Navy Instruction 5211.5E.	O	Commander, Naval Medical Center, Portsmouth	10/1/16	
1	3	11	Provide training and awareness for personnel to ensure that personally identifiable information on e-mail is properly safeguarded in accordance with Navy Medicine Policy 08-005.	O	Commander, Naval Medical Center, Portsmouth	9/30/16	
1	4	12	Review the current computer access policy and educate shared folder owners so that they ensure only those with a "need to know" have access in accordance with Department of the Navy Chief Information Officer Message 201839Z.	O	Commander, Naval Medical Center, Portsmouth	3/1/16	
1	5	12	Provide additional training to ensure that personnel know the proper timeframe to report a breach in accordance with Navy Medicine Policy 09-016.	O	Commander, Naval Medical Center, Portsmouth	11/30/16	
1	6	12	Provide oversight to ensure that the Equipment Management Department documents, in Defense Medical Logistics Standard Support, include the date, rank, and the name of the person who destroyed a hard drive in each instance, and the method of destruction for each piece of disposed equipment with the capability of storing personally identifiable information, as required by Navy Bureau of Medicine and Surgery Fiscal Year 2014 Logistics Guidance.	O	Commander, Naval Medical Center, Portsmouth	2/1/16	

⁸ / + = Indicates repeat finding.

⁹ / O = Recommendation is open with agreed-to corrective actions; C = Recommendation is closed with all action completed; U = Recommendation is undecided with resolution efforts in progress.

¹⁰ If applicable.

Recommendations							
Finding ⁸	Rec. No.	Page No.	Subject	Status ⁹	Action Command	Target or Actual Completion Date	Interim Target Completion Date ¹⁰
1	7	13	Update policy to include sending hard drives to the National Security Agency for destruction on a weekly basis to expedite receipt of confirmation of hard drive destruction.	O	Commander, Naval Medical Center, Portsmouth	2/1/16	
1	8	13	Provide oversight to ensure the Information Management Department provides the Equipment Management Department with a listing of hard drives that have been removed that includes the hard drive serial number and the equipment serial numbers.	O	Commander, Naval Medical Center, Portsmouth	2/1/16	
1	9	14	Coordinate with Naval Medical Logistics Command to update Fiscal Year 2014 Logistics Guidance to ensure that the DD Form 1348-1A is properly annotated for medical equipment.	C	Commander, Naval Medical Center, Portsmouth	12/14/15	
1	10	14	Provide training and awareness to personnel to ensure that forms used to collect personally identifiable information are formally reviewed and approved prior to use, as required by Department of the Navy Bureau of Medicine and Surgery Instruction 5210.9B.	O	Commander, Naval Hospital, Jacksonville	3/31/16	
1	11	15	Establish controls and provide oversight to ensure that staff assistance visits are conducted and documented in accordance with Secretary of the Navy Instruction 5211.5E.	C	Commander, Naval Hospital, Jacksonville	12/14/15	
1	12	15	Establish controls and provide oversight at the lower echelons (i.e., branch clinics, dental clinics) to ensure that staff assistance visits are conducted and documented in accordance with Secretary of the Navy Instruction 5211.5E.	C	Commander, Naval Hospital, Jacksonville	12/14/15	
1	13	16	Establish controls and provide oversight to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with the Secretary of the Navy Message 042232Z of October 2007.	O	Commander, Naval Hospital, Jacksonville	1/29/16	

Recommendations							
Finding ⁸	Rec. No.	Page No.	Subject	Status ⁹	Action Command	Target or Actual Completion Date	Interim Target Completion Date ¹⁰
1	14	16	Establish controls and provide oversight at the lower echelons (i.e., branch clinics, dental clinics) to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with the Secretary of the Navy Message 042232Z of October 2007.	O	Commander, Naval Hospital Jacksonville	1/29/16	
1	15	16	Update the Naval Hospital, Jacksonville Instruction 5211.7A, "Health Insurance Portability and Accountability Act (HIPAA)," to align with current disposal processes to render personally identifiable information records unrecognizable or beyond reconstruction as required by Secretary of the Navy Instruction 5211.5E.	C	Commander, Naval Hospital, Jacksonville	12/14/15	
1	16	17	Remove shredders that do not render personally identifiable information/protected health information unrecognizable from departments, as required by Secretary of the Navy Instruction 5211.5E.	C	Commander, Naval Hospital, Jacksonville	12/14/15	
1	17	17	Provide training and awareness for personnel to ensure that personally identifiable information is properly safeguarded in accordance with Navy Medicine Policy 08-005.	C	Commander, Naval Hospital, Jacksonville	12/14/15	
1	18	17	Provide oversight to ensure that: (1) the Material Management Department amends the disposal process; (2) equipment is tested for capability of storing personally identifiable information; (3) equipment capable of storing personally identifiable information is marked as such in Defense Medical Logistics Standard Support; and (4) Defense Medical Logistics Standard Support is checked for the capability of storing personally identifiable information at the beginning of the disposal process.	C	Commander, Naval Hospital, Jacksonville	12/14/15	

Pertinent Guidance

Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA) of 1996. This Act in part improves portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery. The Act specifies that confidentiality of consumers is to be protected and that procedures shall be set up that protects the confidentiality of the information and the privacy of individuals receiving health care services and items.

Secretary of the Navy (SECNAV) Instruction 5211.5E, “Department of the Navy (DON) Privacy Program,” dated 28 December 2005.

- (1) Privacy Act Coordinator conducts staff assistance visits or program evaluation within his or her command and lower echelon commands to ensure compliance with the Privacy Program;
- (2) Disposal methods are considered sufficient if the records are rendered unrecognizable or beyond reconstruction; and
- (3) DON activities are responsible for establishing appropriate administrative, technical, and physical safeguards to ensure that the documents in every system of records are protected from unauthorized alteration or disclosure. They are also responsible for ensuring that confidentiality is protected.

When an individual is requested to furnish PII for possible inclusion in a system of records, a Privacy Act Statement (PAS) must be provided to the individual, regardless of the method used to collect the information. A PAS shall include: The Federal law or Executive Order that authorizes collection of information; whether or not it is mandatory for the individual to provide the requested information; the principal purposes for collecting the information; the routine uses that will be made of the information; and the possible effects on the individual if the requested information is not provided. The PAS must appear on the form used to collect the information or on a separate form that can be retained by the individual collecting the information. When forms are used to collect information about individuals for a system of records, the PAS shall appear as follows (listed in the order of preference):

- (a) Immediately below the title of the form;
- (b) Elsewhere on the front page of the form (clearly indicating it is the PAS);
- (c) On the back of the form with a notation of its location below the title of the form; or
- (d) On a separate form, which the individual may keep.

SECNAV Instruction 5210.16, “Department of the Navy Forms Management and Information Requirements (Reports) Management Programs,” dated 31 December 2005. When a DON command requires a form, they shall use, in order of precedence, General Services Administration Standard or Optional forms, then Department of Defense (DoD) forms and finally, existing DON forms. The last option is to create a new DON form. This option requires approval and assignment of a form number from the Service Forms Manager. The authorization of an information requirement shall require the assignment of a report control symbol or the citing of the authority that exempts the report from requiring a symbol.

SECNAV Message 042232Z of October 2007, “DON PII [Personally Identifiable Information] Annual Training Policy.” Spot checks will be conducted on a semi-annual basis. Auditable records will be maintained by the command Privacy Act coordinator or other designated official. Corrective action should be taken immediately where weaknesses are identified.

DON CIO Naval Message 201839Z, “PII on DON Shared Drives and Application Based Portals,” dated November 2008. This requires that command leadership must ensure proper controls and permissions are in place to safeguard PII found on shared drives and portals. Only those personnel with a need to know should have access to these privacy-sensitive files.

DON CIO Message 032009Z of October 2008, “DON Policy Updates for Personal Electronic Devices Security and Application of E-mail Signature and Encryption.” Users must digitally sign e-mail messages requiring either message integrity and/or non-repudiation, and encrypt messages containing sensitive information.

Bureau of Medicine and Surgery Instruction 5210.9B, “Forms and Reports Management Program and Survey Coordination,” dated 16 June 2009. This instruction provides the precedence order for higher authority forms. It lists the duties of the Activity Forms Management Officer, which include the following:

- Administration of the Forms and Reports Management Program at the Navy Medical Department Activity;
- Management of all Activity-created forms used by Navy Medical Department personnel within the Activity;
- Review of program requirements and assessment of compliance to ensure requirements are being executed;
- Ensuring Activity forms do not duplicate higher authority forms in any way; and
- Ensuring all Activity forms used by Navy Medical Department personnel have an associated requiring document, form title, form number, form edition date, and follow the guidance established.

Navy Medicine (NAVMED) Policy 08-005, “E-Mailing PII and PHI [Protected Health Information],” dated 28 January 2008. When PHI or PII is transmitted by e-mail, Navy Medicine personnel shall only use Government-furnished equipment and software, and encrypt the sensitive information with DoD-approved encryption methods prior to transmission. This requires authorized, non-DoD recipients to use a DoD-approved digital certificate to encrypt and decrypt sensitive e-mail. All documents containing PHI or PII shall be marked as “FOR OFFICIAL USE ONLY (FOUO) - PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties.” When transmitting PHI or PII by e-mail, the subject line of the message should include “FOUO.” This sensitivity marking apprises the receiver of the need to properly protect the information.

NAVMED Policy 09-016, “Personally Identifiable Information Incident Reporting Requirements,” dated 6 July 2009. An incident or “breach” involving PII 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. The policy requires reporting within 1 hour of the discovery of a known or suspected incident involving PII/PHI.

NAVMED P-5132, “Equipment Management Manual,” dated 7 April 2014. The purpose of this manual is to reiterate DON policy and provide equipment management procedures, including disposal. Requirements for equipment marked for disposal listed in this guidance include condition coding, coordinating transfer to the Defense Logistics Agency with a signed DD Form 1348-1A, and reporting in Defense Medical Logistics Standard Support.

Navy Bureau of Medicine and Surgery Fiscal Year 2014 Logistics Guidance, Revised October 2013. This policy covers topics in Clinical Engineering and Procurement Support, Equipment and Technology Management, and Business Logistics Systems. This includes procedures on disposal of computer equipment. It states that the Information Technology Department is responsible for the sanitization or destruction of computer hard drives. The date and method of destruction, as well as the name and rank/grade of the person who conducted the sanitization process, is to be included in the Notes section of Defense Medical Logistics Standard Support. The guidance also requires the following remark in Block 27 of the DD Form 1348-1A:

“The Equipment described by this document meets the disposition requirements in accordance with the DoD Memorandum, “Disposition of Unclassified Computer Hard Drives,” dated 4 June 2001.”

Naval Medical Center, Portsmouth Standard Operating Procedures for Property Disposal/Redistribution Program, dated January 2012. The purpose of the Standard Operating Procedures, which are specific to Naval Medical Center, Portsmouth only, is to

provide guidance regarding receipt, advertisement, redistribution, and disposal of Government-owned durable equipment identified as idle, underused, or excess. These procedures require Biomedical Engineering to condition code the medical equipment, and provide the hard drives to Information Management for disposal. The hard drives are then sent to National Security Agency for destruction.

Scope and Methodology

We conducted this audit of managing personally identifiable information (PII), including PII on medical treatment equipment, at Naval Medical Center, Portsmouth (NMCP), VA and Naval Hospital, Jacksonville (NHJAX), FL from 30 September 2014 to 19 November 2015. These commands were selected because they had the largest number of disposed pieces of medical equipment in Fiscal Years (FYs) 2013 and 2014.

To determine whether the commands' internal controls were operating effectively to protect PII from unauthorized disclosure, we reviewed policies and procedures related to PII. We reviewed matters related to the Privacy Act program: semi-annual spot checks, disposal method, internal PII/protected health information (PHI) forms, safeguarding PII, and PII breach reporting. To determine whether commands sufficiently disposed of medical treatment equipment containing PII, we requested relevant disposal documentation for each sample item. This included the (1) DD Form 1348-1A; (2) Excess Property Turn-In Document (used at NMCP); or DD Form 1149 (used at NHJAX); and (3) Defense Medical Logistics Standard Support screenshots.

We arbitrarily selected departments from both medical and administrative departments in order to capture information from the widest variety of environments at each. We reviewed a total of 10 departments at NMCP and NHJAX.

We evaluated procedures, monitoring practices, and safeguarding measures by conducting physical visits to verify proper safeguarding and disposal of PII. To test the safeguarding of PII/PHI on computers, we arbitrarily selected two departments with computers for review. We reviewed computers to determine whether: (a) e-mails sent containing PII/PHI had "FOUO" [for official use only] included in the subject line of the message; (b) documents containing PII/PHI in e-mails sent are marked, "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE. Any misuse or unauthorized disclosure can result in both civil and criminal penalties," (c) e-mails sent with PII/PHI were encrypted, and (d) there were sufficient controls and permissions over shared drives.

We looked at internally generated forms used to collect PII/PHI at both NMCP and NHJAX to determine whether they were reviewed and approved by a command Forms Manager.

We interviewed Privacy Act Coordinators, Health Insurance Portability and Accountability Compliance Officers, and personnel responsible for implementing the Privacy Act Program at NMCP and NHJAX.

We received a universe of 1,309 pieces of medical equipment determined to have been disposed of by Navy Medicine East in FYs 2013 and 2014. Of this, 1,086 pieces were disposed of by NMCP and 45 pieces were disposed of by NHJAX. From this universe, we randomly selected a sample of 111 pieces of equipment: 80 items from NMCP and 31 from NHJAX. We then determined through discussions with the command, which pieces contained hard drives, potentially making them capable of storing PII/PHI. This left a total of 56 samples that we assessed (38 from NMCP and 18 from NHJAX). The results are not projected because not all items were applicable. We did not test the reliability of the Defense Medical Logistics Standard Support system because this is a Department of Defense (DoD) system.

We assessed compliance with applicable laws and regulations, including DoD and Department of the Navy regulations applicable to PII/PHI. We also reviewed prior Naval Audit Service, DoD Inspector General, and Government Accountability Office audit reports. There were no previous audit reports directly covering PII on medical treatment equipment at DON East Coast Commands on which to follow up.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Enclosure 4:

Activities Visited

Bureau of Medicine and Surgery, Falls Church, VA

Navy Medicine East, Portsmouth, VA

Naval Medical Center, Portsmouth, VA

Naval Hospital, Jacksonville, FL

Naval Medical Logistics Command, Fort Detrick, MD

Glossary of Acronyms

BUMED	Bureau of Medicine and Surgery
CIO	Chief Information Officer
DLA	Defense Logistics Agency
DMLSS	Defense Medical Logistics Standard Support
DoD	Department of Defense
DON	Department of the Navy
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers' Financial Integrity Act
FOUO	For Official Use Only
FY	Fiscal Year
HIPAA	Health Insurance Portability and Accountability Act
NAVMED	Navy Medicine
NHJAX	Naval Hospital, Jacksonville
NMCP	Naval Medical Center, Portsmouth
NMLC	Naval Medicine Logistics Command
NSA	National Security Agency
PAC	Privacy Act Coordinator
PHI	Protected Health Information
PII	Personally Identifiable Information
SECNAV	Secretary of the Navy

Enclosure 6:

Management Response from Naval Medical Center, Portsmouth



DEPARTMENT OF THE NAVY
NAVY MEDICINE EAST
620 JOHN PAUL JONES CIRCLE
PORTSMOUTH, VIRGINIA 23708-2106

7510
Ser M3/151298
14 Dec 15

FIRST ENDORSEMENT on Commanding Officer, Naval Medical Center, Portsmouth, VA ltr
7510 Ser 00/500055 of 7 Dec 15

From: Commander, Navy Medicine East
To: Assistant Auditor General for Financial Management and Comptroller Audits, Naval
Audit Service
Via: Chief, Bureau of Medicine and Surgery

Subj: MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT NAVAL
MEDICAL CENTER PORTSMOUTH (DRAFT AUDIT REPORT (2014-070))

1. Forwarded. Concur with managerial responses from Naval Medical Center Portsmouth. The
Command has developed an effective plan to address recommendations from the Naval Audit
Service listed in reference (a).

2. Navy Medicine East point of contact for this matter is [REDACTED], USN,
Comm: [REDACTED], E-mail: [REDACTED].

[REDACTED]
Acting

FOIA
(b)(6)

FOIA
(b)(6)



DEPARTMENT OF THE NAVY
NAVAL MEDICAL CENTER
620 JOHN PAUL JONES CIRCLE
PORTSMOUTH, VIRGINIA 23708-2197

7510
Ser 00/500055
7 Dec 2015

From: Commanding Officer, Naval Medical Center, Portsmouth
To: Assistant Auditor General for Financial Management and
Comptroller Audits, Naval Audit Service
Via: (1) Commander, Navy Medicine East
(2) Chief, Bureau of Medicine and Surgery

Subj: MANAGING PERSONALLY IDENTIFIABLE INFORMATION AT NAVAL
MEDICAL CENTER, PORTSMOUTH (DRAFT AUDIT REPORT 2014-070)

Ref: (a) NAVAUDSVC Draft Audit Report 2014-070 of 19 Nov 15

Encl: (1) NAVMEDCEN Portsmouth Response to Recommendations

1. Enclosure (1) is submitted in accordance with reference (a).
It is submitted to provide proposed corrective actions to
recommendations 1 through 9.



Acting

FOIA
(b)(6)

"FIRST AND FINEST"

**Response to Managing Personally Identifiable Information at
Naval Medical Center, Portsmouth (Draft Audit Report 2014-070):**

Recommendation 1. Provide training and awareness to personnel to ensure that forms used to collect personally identifiable information are formally reviewed and approved prior to use, as required by Department of the Navy Bureau of Medicine and Surgery Instruction 5210.9B.

NMCP Response: Concur. Forms Management personnel currently interact with clinical and administrative areas through the "Executive Officer (XO) Rounds" process. Through this process, which includes an out brief of findings with the Division Officer and often the Department Head as well as other key personnel, the Forms Management Officer can provide training and awareness on discrepancies in the collection of PII. In addition, in order to ensure Forms and Reports requirements are being met the NMCP intranet will be updated to include a simple set of directions to follow for assistance with the submission of forms. Plan of the Day and All Hands notices will be utilized to direct the NMCP staff to the revised NMCP intranet page and provide Forms Management point-of-contact information. The target date for the Forms Management intranet site is April 2016.

Recommendation 2. Provide oversight to ensure that the Forms Manager Officers review forms in their control for the required Privacy Act statements, as required by Secretary of the Navy Instruction 5211.5E.

NMCP Response: Concur. A Tiger Team is currently inspecting the Case Files of all NMCP internal forms. The estimated rate of inspection is 25 Case Files per month out of 416 total Case Files. Through the inspection of the Case Files, discrepancies for the proper display of Privacy Act statements on forms can be documented. Addressing Privacy Act statement discrepancies will be coordinated through the Department Heads and Division Officers. All Forms found to be non-compliant with SECNAVINST 5211.5E will be revised or cancelled with the proper corresponding action utilizing DD Form 67. The estimated completion date of the Case File audit is April 2017.

Recommendation 3. Provide training and awareness for personnel to ensure that personally identifiable information on e-mail is properly safeguarded in accordance with Navy Medicine Policy 08-005.

NMCP Response: Concur. Naval Medical Center Portsmouth will:
(a) increase the publication of messages to staff personnel on the Plan of the Day, All Hands and Intranet Home page concerning the Navy Medicine Policy 08-005 on safeguarding requirements;
(b) distribute Awareness briefs to Share Point managers to publish for their staff's situational awareness about this requirement. Share Point managers will maintain records documenting when their staff reviewed Awareness Briefs; (c) implement quarterly (or more frequently, if necessary) spot checks for compliance with this standard and maintain written records documenting the outcome of these reviews; (d) report all non-compliant safeguarding practices to the appropriate Office immediately upon detection; and (e) continue to educate staff during Command Assessments, XO Rounds, Command Orientation, Audits, Spot-Checks and during semi-annual performance reviews when standards are established and/or reviewed. The target completion date is 30 September 2016.

Recommendation 4. Review the current computer access policy and educate shared folder owners so that they ensure only those with a "need to know" have access in accordance with Department of the Navy Chief Information Officer Message 201839Z.

NMCP Response: Concur. Naval Medical Center Portsmouth will publish a local instruction regarding a new shared information access policy and will be working with departments to ensure that only those with a "need to know" have access. The target completion date is 1 March 2016. (See Attachment A for Draft Instruction)

Recommendation 5. Provide additional training to ensure that personnel know the proper timeframe to report a breach in accordance with Navy Medicine Policy 09-016.

NMCP Response: Concur. Naval Medical Center Portsmouth will (a) increase the publication of Plan of the Day and All Hands messages to staff concerning HIPAA Privacy and Security Rules; and (b) continue to educate staff during Command Assessments, XO Rounds, Command Orientation, Annual Required Training, and during semi-annual performance reviews when standards are established and/or reviewed. The target completion date is 30 November 2016. (See Attachment B for POD/All Hands Notice, Attachment C for Annual Required Training Matrix, and Attachment D for HIPAA Privacy Command Assessment)

Recommendation 6. Provide oversight to ensure that the Equipment Management Department documents, in Defense Medical Logistics

Standard Support, include the date, rank, and the name of the person who destroyed a hard drive in each instance, and the method of destruction for each piece of disposed equipment with the capability of storing personally identifiable information, as required by Navy Bureau of Medicine and Surgery Fiscal Year 2014 Logistics Guidance.

NMCP Response: Concur. Equipment Management Division (EMD) is working with Information Management Department (IMD) to ensure that the date, rank, and the name of the person who destroyed a hard drive in each instance, and the method of destruction for each piece of disposed equipment with the capability of storing personally identifiable information are included and documented in Defense Medical Logistics Standard Support (DMLSS). If using the NSA for hard drive destruction, the date, shippers tracking number, and the rank and name of the person who shipped the hard drive will be included and documented in DMLSS. A Standard Operating Procedure (SOP) is being written between EMD and IMD to implement the above recommendation. Target completion date of 1 February 2016.

Recommendation 7. Update policy to include sending hard drives to the National Security Agency for destruction on a weekly basis to expedite receipt of confirmation of hard drive destruction.

NMCP Response: Concur. Naval Medical Center Portsmouth will update the policy to include sending hard drives to the National Security Agency (NSA) for destruction on a weekly or as needed basis to expedite receipt of confirmation of hard drive destruction. EMD will work with IMD to complete an SOP for this process with a target completion date of 1 February 2016.

Recommendation 8. Provide oversight to ensure the Information Management Department provides the Equipment Management Department with a listing of hard drives that have been removed that includes the hard drive serial number and the equipment serial numbers.

NMCP Response: Concur. IMD will provide EMD with a listing of hard drives that have been removed that includes the hard drive serial number and the equipment serial numbers along with the FEDEX tracking number verifying delivery to the NSA. EMD will ensure that the information is entered into DMLSS. EMD will work with IMD to include this recommendation in the Excess SOP with a target completion date of 1 February 2016.

Recommendation 9. Coordinate with Naval Medical Logistics Command to update Fiscal Year 2014 Logistics Guidance to ensure that the DD Form 1348-1A is properly annotated for medical equipment.

NMCP Response: Concur. Naval Medical Center Portsmouth coordinated with Naval Medical Logistics Command to update Fiscal Year 2014 Logistics Guidance to ensure that the DD Form 1348-1A is properly annotated for medical equipment. Fiscal Year 2015 Logistics Guidance was updated with the correct information. Action considered complete. (See Attachment E for the FY15 Logistics Guidance Section 2.3.13 pages 59-60).

NAVMEDCEN

NAVMEDCEN

Subj: Naval Medical Center Portsmouth Command (NMCP) Information Management Shared files and folder plan.

1. Purpose. Establishes an instruction which will provide guidance, and direction on how users store business information on NAVAL MEDICAL CENTER PORTSMOUTH information systems available for use on NMCP domain environment.

2. Scope. The Information Management (IM) Plan applies to Naval Medical Center Portsmouth

4. Policy. The policy contained herein is effective upon receipt.

5. Administration and Maintenance. Additions, corrections, or changes to the manual will be published annually, if necessary. Any correspondence concerning this document should be addressed to:

Commander

Attachment A

Breach Definition

Lost, Stolen, or Compromised of Personal Identifiable Information (PII) and Protected Health Information (PHI). 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, whether physical or electronic, to such information for an other than authorized purposes where one or more individuals will be adversely affected. Such incidents also are known as breaches.

A breach should be report to the United States Computer Emergency Readiness Team (US-CERT) within 1 hour of the discovery of the breach.

Please contact the HIPAA Privacy Officer at [REDACTED] or HIPAA Security Officer at [REDACTED] for additional questions or concerns.

FOIA
(b)(6)

Attachment B



**NMCP REQUIRED TRAINING CHECKLIST
FY-2016**



Navy Medicine Learning Management System (Swank Healthcare) <https://navy.swankhealth.com>

Training Type	Required for	Frequency/Due Date
Newcomer Training (To include all applicable BUMED Required Training not previously completed in FY 16)	All New NMCP Staff	Once upon check-in
Nursing Learning Resource Guides (LRG)	Identified Nursing and Corpsmen staff (in conjunction with Nursing Orientation)	Once Upon Check-in
Command/Departmental Updates HMSB Program (Performance Checklist's)	Identified staff per the training requirement All 's, E-6 and Below (excluding IDC's)	Varies by topic
BUMED Required Training		
1. Constitution and Citizenship Day	All Hands	1 Jan 2016
2. Diversity Training	All Hands	1 Jan 2016
3. Prevention of Unauthorized Commitments	Active Duty and GS (every 2 years)	1 Jan 2016
4. Navy Medicine Anti-Fraud Program	All Hands	1 Jan 2016

The BUMED Required Training will be automatically assigned to you by BUMED. Please do not enroll or complete the above training as an elective.
Navy Medicine LMS assignments are assigned based upon staff demographics to ensure the training is only assigned to individuals that are required by regulating instruction

Local Command Delivered Required Training **SEAT Department**

Course Title	Required For	Frequency/Due Date
Command Orientation	All Hands	One Time
Nursing Orientation	Identified Nursing and Corpsmen staff (in conjunction with Nursing LRG's)	
Tactical Combat Casualty Care (TCCC)	HM's/PA's Deploying with 180 days	As Required
Hospital Corpsman Skills Basic (HMSB)	All HM's, E-6 and Below (Excluding IDC's)	PCL's must be completed via Navy Medicine LMS
Basic Life Support	All Clinical Staff	24 Months
Advanced/Pediatric Cardiac Life Support (ACLS/PALS)	As Required	
Advanced Trauma Life Support (ATLS)	MD/PA/CRNA/Deploying Personnel	48 Months
Trauma Nurse Core Course (TNCC)	RN Personnel Deploying	
General Military Training Category 1 Face to Face Topics	All Military Personnel	1 Jan 2016
Counter Intelligence Awareness and Reporting NAVADMIN Requirements (as identified by Navy Regulations)	Active Duty and GS Identified Staff	1 Jan 2016 Varies

FOIA
(b)(6)

Navy Knowledge Online (NKO) www.nko.navy.mil

Course Title	Course Code	Required For	Due Date
No Fear Act	OCHR-NFA-2.1	Active Duty and GS (every 2 years)	1 Jan 2016
DOD Cyber Awareness Challenge	DOD-IAA-V12.0	All Hands	1 Jan 2016
Personally Identifiable Information	DOD-P11-2.0	All Hands	1 Jan 2016
Combating Trafficking in Persons General Awareness	DOD-CTIP-1.0	Active Duty and GS	1 Jan 2016
Antiterrorism Level 1 Awareness Training	CENSECFOR-AT-010-1.0	All Hands	1 Jan 2016
Records Management in the DON: Everyone's Responsibility	DOR-RM-010-1.1	Active Duty and GS	1 Jan 2016
Operations Security (Uncle Sam's OPSEC)	NIOC-USOPSEC-2.0	All Hands	1 Jan 2016

Joint Knowledge On-Line <https://jkodirect.jten.mil>

Course Type	Required for	Frequency/Due Date
ERPC - Clinician, Operator/Responder, Executive, or Basic Awareness	All Hands	Every 3 years
HIPAA and Privacy Training	All Hands	1 Jan 2016

Safety (ESAMS) <https://esams.enic.navy.mil>

Course Type	Required for	Frequency
Various courses-Determined by your Dept. Leadership and Safety Representative	All Hands	As Required

Emergency Management (FEMA) <http://www.training.fema.gov/EMIWeb/IS/is100HCb.asp>

Course Title	Required for	Frequency
IS-100.HCB - ICS 100 for Healthcare/Hospitals	All Hands	As Required

Attachment C

Naval Medical Center Portsmouth				
HIPAA Privacy Assessment Check List				
Location:			Surveyor:	
Date:				
Administration Observations	Yes	No	Guidelines/Resources	Comments
1 Does the department or clinic have a Standard Operating Procedure for handling PHI?			Each Department should have a SOP specific to their area for handling PHI. NAVMEDCENTPTS HIPAA INSTRUCTION 6150.3C	
2 What is the procedure for reporting a breach of PHI (lost, stolen or a compromise of PHI)?			A Breach of PHI must be reported to the United States Computer Electronics Recovery Team (US-CERT) within 1 hour of the the breach. Report the Breach to the Privacy Officer ASAP.	
3 Do faculty/staff know who the HIPAA Privacy and Security Officers are?			HPO [redacted] @ [redacted] HSO [redacted] @ [redacted]	
4 Do faculty/staff know where they should refer questions regarding patient privacy?			HPO @ [redacted] or https://webapps.mar.med.navy.mil/training/hipaa/index.asp .	
5 Are faxes limited to urgent (NON-ROUTINE)?			Transmission of PHI by fax should be limited to urgent and non-routine situations IAW NAVMEDCENTPTS HIPAA INSTRUCTION 6150.3C	
6 Is the HIPAA Program Office (HPO) approved Fax coversheet available and being used?			Obtain from HPO website. Keep at fax machines.	
7 Do staff members verify fax numbers prior to use?			Sending PHI to the wrand destination is a breach	
8 Do staff members routinely contact an individual to alert him or her a fax is being sent containing PHI?			Staff should routinely contact the individual to alert him or her a fax is being sent containing PHI	
9 Do staff members routinely contact the individual to verify receipt of fax containing PHI?			Staff members should routinely contact the individual to verify receipt of fax containing PHI.	
10 Have all staff and faculty completed HIPAA training?			Required to go through MHS Learn to complete computer-based training (CBT). Contact HPO at [redacted] to assist with training needs. IAW NAVMEDCENTPTS HIPAA INSTRUCTION 6150.3C	
11 Does the location have a process and designated Point of Contact for logging, tracking, reporting and resolving PII/PHI disclosures?			We must maintain an accounting of all disclosures for at least 6 years per NAVMEDCENTPTS HIPAA INSTRUCTION 6150.3C. See Question # 27.	
12 Are faculty/staff aware that they should only access PHI that they need to know to perform their work related duties?			Emphasize during staff meetings. Violators can face sanction and/or lose their job. HPO is available to attend mtg.	
13 Do faculty/staff know what to do if a patient requests amendments to their medical records?			Contact the HPO. Patient needs to complete NAVMEDCENTPTSVA 6150/21 forms	

FOIA (b)(6)
FOIA (b)(6)

FOIA (b)(6)

FOR OFFICIAL USE ONLY

ENCLOSURE 6: MANAGEMENT RESPONSE FROM NAVAL MEDICAL CENTER, PORTSMOUTH

14	Do faculty/staff know what to do when patients request copies of their medical records?			<i>Direct patient to the Out Patient Records to complete the authorization DD 2870 form.</i>	
15	Do staff members use Guard Mail?			<i>Every effort should be made to send PHI via a courier. The PHI is double sealed, once in an envelope addressed to the intended individual and marked "sensitive information, for recipient's eyes only" and a second time in a guard mail envelope. The outside of the guard mail envelope will be addressed to an individual person and their department.</i>	
16	Are Guard Mail boxes secured?			<i>Departments will ensure their guard mail boxes are in a secure area to ensure control of PHI being sent through the guard mail. Boxes or cabinets not in a secure area must be relocated or locked.</i>	
	Department/ Clinic Observations	Yes	No	Guidelines/Resources	Comments
17	Is the department compliant with not placing PHI in the regular trash receptacle?			<i>Check every wastebasket. PHI should be placed in PHI bins or shredded.</i>	# of Cans
18	Are shredder containers or other PHI disposal bins available and easily accessible by staff members?			<i>Contact facilities department at [redacted] to order containers or to notify that containers are overflowing.</i>	
19	Are documents containing PHI (e.g. appointment schedules, census lists, physician orders) secure? (not visible to unauthorized individuals - including the public)			<i>Check work areas (registration desks, nurses station) for PHI visible to others. Use a "Confidential" cover page, place in drawers, or turn over even if department personnel are present.</i>	
20	Are materials removed from printers and fax machines in a timely manner?			<i>Verify there is a process where staff regularly remove printed material in a timely manner.</i>	
21	Do faculty/staff log-off computers before leaving their workstations?			<i>Remind faculty/staff of Information Assurance requirements.</i>	
22	Are computer monitors and printers located and positioned so that visitors can't access or view the PHI on them?			<i>If computer screens are visible to patients or visitors, they should be repositioned or screen protectors should be purchased.</i>	
23	All computers located in areas where visitors are left unattended?			<i>Computers should never be left logged on and unattended.</i>	
24	Is the waiting room configured to prevent visitors from overhearing the registration process?			<i>Observe dialogue/exchanges and identify need for staff to lower voices. Should conversations be held in a more private area?</i>	
25	Does the location have a whiteboard, patient tracker (electronic), x-ray boards or other posting mechanism that contains only the minimum amount of information necessary and is it located in a secure area (staff only or quasi-public area)?			<i>The incidental uses and disclosure rule does not excuse non-compliance due to mistakes, neglect, failure to have in place appropriate safeguards, or failure to make reasonable efforts to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.</i>	# of boards

FOIA (b)(6)

ATTACHMENT D

FOR OFFICIAL USE ONLY

ENCLOSURE 6: MANAGEMENT RESPONSE FROM NAVAL MEDICAL CENTER, PORTSMOUTH

Records Maintenance	Yes	No	Guidelines/Resources	Comments
26 Does the location have a process for identifying and issuing patients who need to receive Notice of Privacy Practices (NOPP) information/pamphlet? Does the location have a process for collecting and documenting the patient's signed acknowledgment of receiving the NOPP?			Implementation of the Requirements of HIPAA at NMCP (NMCPINST 6150.3C) states: Patients must receive notification about use of their private medical information and their rights regarding their PHI. When patients present to NAVMEDCEN clinics or wards for the first time, the staff member checking them in will ask if they received the NOPP. If not, they will be provided with a copy. The staff member will then ask the patient to acknowledge receipt by signing the medical record label, which will become a permanent record of acknowledgement of receipt of the NOPP. Acknowledgement labels can be obtained by contacting the Forms Control Division at [REDACTED]. NOPP brochures can be obtained by contacting the Privacy Office at [REDACTED].	
27 Is the Department/Clinic using an accepted process for documenting all patient approved PHI disclosures?			<i>The Department of Defense Health Information Privacy Regulation (DODINST 6025.18R) states that we must be able to provide documentation of patient approved PHI disclosures for the past 6 years. To help comply with these requirements, the TRICARE Management Activity (TMA) created an electronic disclosure-tracking tool. The Protected Health Information Management Tool (PHIMT) stores information about all disclosures, authorizations, and restrictions that are made for a particular patient. Methods available to comply with this requirement include: (1) Keeping a log book of the disclosure and copies of the signed authorization (DD Form 2870). (2) Entering a copy of the authorization form in the patient's AHLTA record. (3) Taking the authorization form to Outpatient Medical Records where it will be entered in the Protected Health Information Management Tool (PHIMT), or (4) placing a copy in the out-patient medical record.</i>	
28 Are patient charts maintained/stored in a secure area?			<i>Records should be stored in a secure area and locked if area when area is unattended..</i>	
29 Are records locked in a secure area during periods when clinic/Department is closed?			<i>Records should be stored in a secure area and locked when area is unattended.</i>	

FOIA (b)(6)

Department / Clinic POC Name (Printed)

Surveyor's Name (Please Print)

Signature

Surveyor's Signature

(Rev 4/2015)



DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH, VA 22042

IN REPLY REFER TO
7000
Ser M42/15UM40084
26 May 15

MEMORANDUM FOR COMMANDER, NAVY MEDICINE EAST
COMMANDER, NAVY MEDICINE WEST
COMMANDING OFFICER, NAVAL MEDICAL LOGISTICS
COMMAND
COMMANDING OFFICER, NAVAL MEDICAL RESEARCH
CENTER
COMMANDING OFFICER, NAVY MEDICINE EDUCATION AND
TRAINING COMMAND
COMMANDING OFFICER, NAVY MEDICINE INFORMATION
SYSTEMS SUPPORT ACTIVITY
COMMANDING OFFICER, NAVY AND MARINE CORPS
PUBLIC HEALTH CENTER

Subj: FY15 LOGISTICS GUIDANCE CHANGE TRANSMITTAL I

Ref: (a) BUMED Memo 6700 Ser M42/AT-0286242 of 7 Oct 13
(b) CONTRACT HEALTHCARE SERVICES VALIDATION AND FORECASTING
FOR FISCAL YEARS 2015 and 2016

Encl: (1) FY15 Logistics Guidance CH-1

1. The FY15 Logistics Guidance is the most current guidance in the areas of Equipment and Maintenance Management, Business Systems, and Logistics processes. This document provides information to support standardization across Navy Medicine, as described in reference (a). This document is accessible at https://gov_only.nmhc.med.navy.mil/guidance.asp.
2. FY15 acquisition-specific guidance is provided in reference (b). This document is accessible at https://gov_only.nmhc.med.navy.mil/guidance/CHCS%20Validation%20and%20Forecasting%20Memo%20FY1415_SIGNED%2018%20June.pdf
3. Key FY15 due dates are included in the appendix of enclosure (1), starting on page 80.
4. The BUMED Logistics Director (M42) will disseminate updates to the logistics guidance as necessary to the Regional Logisticians and Comptrollers for forwarding within their Area of Responsibility (AOR). My point of contact for Logistics Guidance is [REDACTED], [REDACTED].

[REDACTED]
Deputy Chief
Installations and Logistics

ATTACHMENT E

FOIA
(b)(6)

FOIA
(b)(6)



NAVY BUREAU OF MEDICINE AND SURGERY

FY15 LOGISTICS GUIDANCE

Revised: April 2015

Enclosure (1)

ATTACHMENT E

b. For equipment traded-in to a private organization or replacements provided by a vendor as part of product recalls, use transaction reason, "TRADE-IN EQUIPMENT."

3. Asset Requiring Repair. This is applicable to a non-medical asset needed to be sent out for repair and should not be transferred. Use the "Temporary Location" field and the "Notes" tab in DMLSS to indicate to which vendor the asset will be shipped to. For all medical equipment needed to be sent for repair, coordinate the tracking with the BIOMED by following the guidance provided in Section 2.2 of this document.

2.3.13 Equipment Loss (End-Item Decrease)

1. Termination of Accountability. Personal property that has been transferred-out, disposed, lost, stolen, or destroyed should be properly documented and removed from the APSR at the time the property leaves the activity or it is determined the item no longer exists. Substantiating documentation must be retained indefinitely. The following transaction reasons should be used when performing a loss in DMLSS:

a. "Component Loss." Use for the loss of a system's component. For example, if a repair was done and a single component was replaced.

b. "Equipment Inventory Adjustment Loss." Use for equipment removed as a result of inventory. This includes equipment for which a DD Form 200 was initiated for causative research, but no Financial Liability Investigation was conducted.

c. "Financial Liability Investigation." Use when a DD Form 200 was initiated upon discovery of lost, damaged, or destroyed equipment for which it resulted in a Financial Liability Investigation and involved individual(s) was (were) found financially liable.

d. "Item Changed to Not Accountable." Use when accountability requirements change. For example, the user can use this transaction reason when removing non-medical computer monitors from DMLSS.

e. "Loss to Deployment." Use for equipment that was deployed and could not be recovered.

f. "Loss to Natural Disaster." Use for equipment damaged/destroyed as a result of a natural disaster. For example, if there was flooding in a facility and equipment was damaged beyond repair.

g. "Ship to Another MTF." Use for transfers to the Navy, Army, and Air Force facilities using DMLSS. The user must use this transaction reason in order to complete the lateral transfer process in DMLSS.

h. "Trade-In Equipment." Transfer to vendor outside of the Federal Government.

i. "Turn-in to DLA-DS." Use this transaction reason for items turned in to DLA-DS. DMLSS will automatically generate a DD Form 1348-1A when using this transaction reason. Do not use this DD Form 1348-1A as disposal documentation because the signed or stamped Electronic Turn-In Document (ETID) or Disposal Turn-In Document (DTID) should have already been returned before performing a loss in DMLSS.

2. Disposal Procedures

a. The CEM should ensure that equipment with condition code "A" and Maintenance Assessment of "Excellent, Good, or Fair" are first reported as excess before turn-in to DLA-DS. The BIOMED will be responsible for condition coding medical equipment and MID will be responsible for condition coding ADP equipment. Excess reporting must be done via DMLSS. Medical equipment hard drives which may potentially store PHI must be removed and disposed following the procedures in section 2.3.14.7, "Disposal of ADP Equipment."

b. Equipment for disposal will be coordinated with the nearest DLA-DS using a signed DD Form 1348-1A DTID or ETID with the appropriate Disposition Authority Code or processed as a receipt-in-place. Navy Medicine activities that rely on another DoD activity, such as installation supply, to coordinate turn-ins to DLA-DS may use the DD Form 1149 to substantiate termination of accountability and control.

c. Secondary review/approval is required for all property disposition. Accordingly, two authorized command staff signatures are required on the appropriate disposition form (DD Form 1348 or DD Form 1149) before the tri-wall container is sealed or when the property is dropped-off at DLA-DS or installation supply.

d. For property turned-in to DLA-DS, the CEM should acquire the official stamped/signed DD Form 1348 before completing the loss transaction in DMLSS. For property turned-in to installation supply, loss may be performed in DMLSS upon receipt of signed DD Form 1149.

e. While waiting for a stamped or signed receipt from DLA-DS or installation supply, the property should be transferred to "HOLD" customer in DMLSS. Once the stamped/signed receipt is received, the CEM should perform a loss in DMLSS using the transaction reason "Turn-in to DLA-DS" or "Turn-in to Installation Supply." The DMLSS-generated DD Form 1348 will have the transaction document number and as such, the CEM must ensure that the stamped/signed DD Form 1348 or the DD Form 1149 is attached and maintained with the DMLSS-generated DD Form 1348.

2.3.14 Accounting for Information Technology (IT) Equipment

1. All IT equipment should be assigned to the IT Department (ITD). Accordingly, the Head of the ITD will be assigned as the Custodian for all IT equipment owned by the activity. Since ITD has the sole responsibility of overseeing the issuance, replacement, repair, and reissue of all IT equipment at the activity, ITD will be responsible for the life

Enclosure 7:

Management Response from Naval Hospital, Jacksonville



DEPARTMENT OF THE NAVY
NAVY MEDICINE EAST
620 JOHN PAUL JONES CIRCLE
PORTSMOUTH, VIRGINIA 23708-2106

7510
Ser M09/151297
14 Dec 15

FIRST ENDORSEMENT on Commanding Officer, Naval Hospital, Jacksonville, FL ltr 7510
Ser 00F0ZZ/1886 of 7 Dec 15

From: Commander, Navy Medicine East
To: Assistant Auditor General for Financial Management and Comptroller Audits, Naval Audit Service
Via: Chief, Bureau of Medicine and Surgery

Subj: NAVAL AUDIT SERVICE DRAFT REPORT ON PERSONALLY IDENTIFIABLE INFORMATION AND MEDICAL TREATMENT EQUIPMENT AT NAVAL HOSPITAL JACKSONVILLE

1. Forwarded. Concur with managerial responses from Naval Hospital Jacksonville. The Command has developed an effective plan to address recommendations from the Naval Audit Service listed in reference (a).

2. Navy Medicine East point of contact for this matter is [REDACTED], [REDACTED], USN,
Comm: [REDACTED], E-mail: [REDACTED].

[REDACTED]
Acting

FOIA
(b)(6)

FOIA
(b)(6)



DEPARTMENT OF THE NAVY
NAVAL HOSPITAL
2080 CHILD STREET
JACKSONVILLE, FLORIDA 32214-5000

IN REPLY REFER TO
7510
Ser 00F0ZZ/1886
07 Dec 2015

From: Commanding Officer, Naval Hospital Jacksonville
To: Naval Audit Service, Assistant Auditor General for Research, Development, Acquisition and Logistics Audits
Via: (1) Commander, Navy Medicine East
(2) Chief, Bureau of Medicine and Surgery
Subj: NAVAL AUDIT SERVICE DRAFT REPORT ON PERSONALLY IDENTIFIABLE INFORMATION AND MEDICAL TREATMENT EQUIPMENT AT NAVAL HOSPITAL JACKSONVILLE, FL

Ref: (a) NAVAUDSVC Memo 2014-070 of 19 Nov 2015

Encl: (1) Naval Hospital Jacksonville command response to subject draft report

1. Reference (a) forwarded the subject draft report for review and comments. Accordingly, enclosure (1) contains our response.

2. My point of contact for additional information is [REDACTED], Director for Administration, at [REDACTED] or email [REDACTED].



FOIA
(b)(6)

FOIA
(b)(6)

Naval Hospital Jacksonville Command Response to Subject Draft Report

Recommendation 10. Provide training and awareness to personnel to ensure that forms used to collect personally identifiable information are formally reviewed and approved prior to use, as required by the Department of the Navy Bureau of Medicine and Surgery Instruction 5210.9B.

NHJAX response to 10: Concur. The command published a Forms Management Program Instruction (NAVHOSPJAXINST 5213.1F) dated 13 August 2015. It specifically outlines procedures for use and approval of forms using personally identifiable information (PII). The command's Forms Control Committee (FCC) has a representative from each directorate that monitors all forms used for version control and updates. The command has bi-monthly meetings in which each directorate representative will present all forms for revision/approval at which time the documents are screened for PII/HIPAA compliance. The notes concerning the precedence of forms are well understood by the FCC, and higher echelon forms are used whenever possible. Our Legal office is included in the routing of all forms when PII is involved and there is also a legal representative that sits on the FCC. The FCC will ensure the For Official Use Only statement is annotated on all forms containing PII. The command is currently in the process of screening all directorate forms and has an estimated completion date of March 2016.

Recommendation 11. Establish controls and provide oversight to ensure that staff assistance visits are conducted and documented in accordance with Secretary of the Navy Instruction (SECNAVINST) 5211.5E.

Recommendation 12. Establish controls and provide oversight at the lower echelons (i.e., branch clinics, dental clinics) to ensure that staff assistance visits are conducted and documented in accordance with SECNAVINST 5211.5E.

NHJAX response to 11 and 12: Partially Concur. SECNAVINST 5211.5E specifically requires "Navy Echelon 2 and 3 Commands and Marine Corps Major Subordinate Commands" to, among other things, "(11) Conduct staff assistance visits or program evaluations within their command and lower echelon commands to ensure compliance with the Privacy Act (PA)." NHJAX is an Echelon 4 command. Currently staff assist visits that conduct "program evaluations" are tracked and documentation collected through our Command Evaluation Program Coordinator to ensure compliance with the Privacy Act Instruction. Our last evaluation was completed in the 4th Quarter, FY15. Navy Medicine East is scheduled to provide assist visit the week of 25-29 January 2016.

Recommendation 13. Establish controls and provide oversight to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with the Secretary of the Navy (SECNAV) Message 042232Z of October 2007.

Recommendation 14. Establish controls and provide oversight at the lower echelons (i.e., branch clinics, dental clinics) to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with the SECNAV Message 042232Z of October 2007.

Enclosure (1)

Naval Hospital Jacksonville Command Response to Subject Draft Report

NHJAX response to 13 and 14: Concur on both. NAVHOSPJAXINST 5211.5D has been revised and is currently routing for signature by the Commanding Officer. This will specifically annotate the requirement to conduct semi-annual spot checks throughout the Hospital and at each of our branch health clinics (BHC). Our most recent semiannual spot checks were conducted at NHJAX and all our BHCs between 30 July and 4 September, and addressed all areas and items delineated in SECNAV message 042232Z OCT 2007. Document file is retained in the Command Legal Office.

Recommendation 15. Update the NAVHOSPJAXINST 5211.7A, "Health Insurance Portability and Accountability Act (HIPAA)," to align with current disposal processes to render personally identifiable information records unrecognizable or beyond reconstruction as required by SECNAVINST 5211.5E.

NHJAX response to 15: Concur. NAVHOSPJAXINST 5211.7A CHANGE TRANSMITTAL 1 signed 15 April 2015 outlines the current disposal policy using contracted services with onsite crosscut shredding.

Recommendation 16. Remove shredders from departments that do not render personally identifiable information/protected health information unrecognizable, as required by SECNAVINST 5211.5E.

NHJAX response to 16: Concur. NHJAX Operations Management Department is constantly conducting rounds to ensure all unauthorized shredders have been removed from the facility. A current sweep of the facility and its outlying buildings was performed the week of 5 Oct 15 and resulted in the removal of 10 unauthorized shredders. Every space has been inspected within the facility and is 100% compliant. We will perform spot checks to ensure continued compliance. The only spaces currently authorized to have shredders are the following: MID (SIPR Room), Legal, and Security Manager's Office.

Recommendation 17. Provide training and awareness to personnel to ensure that forms used to collect personally identifiable information are formally reviewed and approved prior to use, as required by SECNAVINST 5210.16.

NHJAX Response to 17: Concur. The command published a Forms Management Program Instruction (NAVHOSPJAXINST 5213.1F) dated 13 August 2015. It specifically outlines procedures for use and approval of forms using personally identifiable information (PII). The command's Forms Control Committee (FCC) has a representative from each directorate that monitors all forms used for version control and updates. The command has bi-monthly meetings in which each directorate representative will present all forms for revision/approval at which time the documents are screened for PII/HIPAA compliance. The notes concerning the precedence of forms are well understood by the FCC, and higher echelon forms are used whenever possible. Our Legal office is included in the routing of all forms when PII is involved and there is also a legal representative that sits on the FCC. The FCC will ensure the For Official Use Only statement is annotated on all forms containing PII. The command is currently in the process of screening all directorate forms and has an estimated completion date of March 2016.

Because this recommendation is duplicative to Recommendation 10, we have deleted it from the final report and renumbered the subsequent recommendations in the body of the report.

Naval Hospital Jacksonville Command Response to Subject Draft Report

Recommendation 18. Provide training and awareness for personnel to ensure that PII is properly safeguarded in accordance with Navy Medicine Policy 08-005.

NHJAX response to 18: Concur. NHJAX was 100% compliant with the annual HIPAA and PII training. Also, NHJAXINST 5211.7A CH-1 dated 15 Apr 15 specifically addressed items in NAVMED Policy 08-005. This was passed via command postmaster and through the Executive Steering Council.

Recommendation 19. Provide oversight to ensure that: (1) the Material Management Department amends the disposal process; (2) equipment is tested for capability of storing PII; (3) equipment capable of storing PII is marked as such in Defense Medical Logistics Standard Support; and (4) Defense Medical Logistics Standard Support is checked for the capability of storing PII at the beginning of the disposal process.

NHJAX response to 19: Concur. We recognized in 2013 that we were not in compliance with NMLC FY14 Logistics guidance with reference to disposal and documentation of equipment with hard drives that have the capability of storing PII. We corrected ourselves and since the Spring of 2013 have been in compliance with NMLC's annual guidance. This was articulated to the Navy Audit Service team during their visit; therefore, it is no surprise that 4 out of 18 records did not have the proper documentation in Defense Medical Logistics Standard Support (DMLSS) or on the DD Form 1348-1A. However, all 4 hard drives were recorded on the destruction log, kept by the Information Assurance Officer, with date, method of destruction, name and grade of the person performing the destruction.

Our process since Spring 2013 in response to recommendation 19 (which was/is in compliance with NMLC annual FY guidance): Step (1): When a piece of equipment is presented to Equipment Management for transfer to Defense Reutilization Marketing Office (DRMO), Biomedical Repair conducts the assessment to determine if the equipment is capable of storing PII/PHI and removes any hard drives. The equipment is transferred to Equipment Management Division and the hard drive is presented to Management Information Department (MID) for destruction. Steps (2) and (3) are completed by Biomedical Repair once a new piece of equipment arrives at the Command as part of the acceptance check. If a piece of equipment has the capability of storing PII/PHI, the "Contains Patient Data" indicator in DMLSS is checked. Step (4) is completed by Biomedical Repair once a piece of equipment has been identified for transfer to DRMO. The Biomedical Repair Technician condition codes the equipment and assesses the equipment for capability of storing PII on the DD 1149 (transfer document).

However, the Navy Audit Service Team visit triggered us to streamline the disposal process of equipment with PII/PHI. Effective 10 March 2015, Biomedical Repair is now required to surrender the equipment with hard drive to Equipment Management. Equipment Management is now required to surrender the hard drive to MID for disposal. This ensures the chain of custody, the destruction and the proper documentation required in DMLSS with regards to equipment with PII/PHI. The same procedures also apply to the outlying branch health clinics.

Naval Hospital Jacksonville Command Response to Subject Draft Report

Finding	Rec No.	Page No.	Subject	Status	Action Command	Target or Actual Completion Date	Interim Target Completion Date
1	10		Provide training and awareness to personnel to ensure that forms used to collect personally identifiable information are formally reviewed and approved prior to use, as required by Department of the Navy Bureau of Medicine and Surgery Instruction 5210.9B.	Working	Commander, Naval Hospital, Jacksonville	Will be complete Mar 16	
1	11	1	Establish controls and provide oversight to ensure that staff assistance visits are conducted and documented in accordance with Secretary of the Navy Instruction (SECNAVINST) 5211.5E.	Complete	Commander, Naval Hospital, Jacksonville		
1	12	1	Establish controls and provide oversight at the lower echelons (i.e., branch clinics, dental clinics) to ensure that staff assistance visits are conducted and documented in accordance with SECNAVINST 5211.5E.	Complete	Commander, Naval Hospital, Jacksonville		
1	13	1	Establish controls and provide oversight to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with the Secretary of the Navy (SECNAV) Message 042232Z of October 2007.	Working	Commander, Naval Hospital, Jacksonville	Will be complete Feb 16	
1	14	1	Establish controls and provide oversight at the lower echelons (i.e., branch clinics, dental clinics) to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with the SECNAV Message 042232Z of October 2007.	Working	Commander, Naval Hospital, Jacksonville	Will be complete Feb 16	
1	15	2	Update the NAVHOSPJAXINST 5211.7A, "Health Insurance Portability and Accountability Act (HIPAA)," to align with current disposal processes to render personally identifiable information records unrecognizable or beyond reconstruction as required by SECNAVINST 5211.5E.	Complete	Commander, Naval Hospital, Jacksonville		
1	16	2	Remove shredders from departments that do not render personally identifiable information/protected health information unrecognizable, as required by SECNAVINST 5211.5E.	Complete	Commander, Naval Hospital Jacksonville		
1	17	1	Provide training and awareness to personnel to ensure that forms used to collect personally identifiable information are formally reviewed and approved prior to use, as required by SECNAVINST 5210.16.	Working	Commander, Naval Hospital, Jacksonville	Will be complete Mar 16	

Naval Hospital Jacksonville Command Response to Subject Draft Report

1	18	3	Provide training and awareness for personnel to ensure that PII is properly safeguarded in accordance with Navy Medicine Policy 08-005.	Complete	Commander, Naval Hospital, Jacksonville		
1	19	3	Provide oversight to ensure that: (1) the Material Management Department amends the disposal process; (2) equipment is tested for capability of storing PII; (3) equipment capable of storing PII is marked as such in Defense Medical Logistics Standard Support; and (4) Defense Medical Logistics Standard Support is checked for the capability of storing PII at the beginning of the disposal process.	Complete	Commander, Naval Hospital, Jacksonville		

~~FOR OFFICIAL USE ONLY~~

Use this page as

BACK COVER

for printed copies

of this report

~~FOR OFFICIAL USE ONLY~~