

Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Information Requirements

(Revised April 2, 2014)

1. General Requirements Overview - Personally Identifiable Information (PII), Protected Health Information (PHI) and Federal Information Laws

This Section addresses the Contractor's requirements under The Privacy Act of 1974 (Privacy Act), The Freedom of Information Act (FOIA), and The Health Insurance Privacy and Accountability Act (HIPAA) as set forth in applicable statutes, implementing regulations and DoD issuances. In general, the Contractor shall comply with the specific requirements set forth in this section and elsewhere in this Contract. The Contractor shall also comply with requirements relating to records management as described herein.

This Contract incorporates by reference the federal regulations and DoD issuances referred to in this Section. If any authority is amended or replaced, the changed requirement is effective when it is incorporated under contract change procedures. Where a federal regulation and any DoD issuance govern the same subject matter, the Contractor shall first follow the more specific DoD implementation unless the DoD issuance does not address or is unclear on that matter. DoD issuances are available at <http://www.dtic.mil/whs/directives>.

For purposes of this Section, the following definitions apply.

DoD Privacy Act Issuances means the DoD issuances implementing the Privacy Act, which are DoDD 5400.11 (May 8, 2007 thru Change 1 September 1, 2011) and DoD 5400.11-R (May 14, 2007).

HIPAA Rules means, collectively, the HIPAA Privacy, Security, Breach and Enforcement Rules, issued by the U.S. Department of Health and Human Services (HHS) and codified at 45 CFR Part 160 and Part 164, Subpart E (Privacy), Subpart C (Security), Subpart D (Breach) and Part 160, Subparts C-D (Enforcement), as amended by the 2013 modifications to those Rules, 78 FR 5566-5702 (January, 25, 2013) (with corrections at 78 FR 32464 (June 7, 2013)). Additional HIPAA rules regarding electronic transactions and code sets (45 CFR Part 162) are not addressed in this Section and are not included in the term HIPAA Rules.

DoD HIPAA Issuances means the DoD issuances implementing the HIPAA Rules in the DoD 6025.18-R (January 24, 2003), DoDI 6025.18 (December 2, 2009), and DoD 8580.02-R (July 12, 2007).

DHA Privacy Office means the DHA Privacy and Civil Liberties Office. The DHA Privacy Office Chief is the HIPAA Privacy and Security Officer for DHA, including the National Capital Region Medical Directorate (NCRMD).

Service-Level Privacy Office means a privacy office of one of the military Services (Army, Navy, or Air Force). The Service-Level Privacy Offices have authority over Privacy Act and HIPAA compliance by the military Services. *[This definition is applicable to this Contract if the*

Government party to this Contract is one of the Services or a Service component. In that case, this Section may need Service-specific provisions in addition to this definition.]

Breach means actual or possible loss of control, unauthorized disclosure of or unauthorized access to PHI or other PII (which may include, but is not limited to PHI), where persons other than authorized users gain access or potential access to such information for any purpose other than authorized purposes, where one or more individuals will be adversely affected. The foregoing definition is based on the definition of breach in DoD Privacy Act Issuances as defined herein.

HHS Breach means a breach that satisfies the HIPAA Breach Rule definition of a breach in 45 CFR 164.402.

2. Records Management

When creating and maintaining official government records, the Contractor shall comply with all federal requirements established by 44 U.S.C. Chapters 21, 29, 31, 33 and 35, and by 36 CFR, Chapter XII, Subchapter B – Records Management. The Contractor shall also comply with DoD Administrative Instruction No. 15 (DOD AI-15), “OSD Records and Information Management Program” (May 3, 2013).

3. Freedom of Information Act (FOIA)

The Contractor shall comply with the following procedures if it receives a FOIA request and immediately contact the DHA FOIA Officer for evaluation/action:

The Contractor shall inform beneficiaries that DHA FOIA procedures require a written request addressed to the DHA Freedom of Information Service Center, 7700 Arlington Boulevard, Suite 5101, Falls Church, Virginia 22042-5101 (or email requests addressed to FOIARequests@tma.osd.mil), and that the request shall describe the desired record as completely as possible to facilitate its retrieval from files and to reduce search fees which may be borne by the requestor. Although the administrative time limit to grant or deny a request (ten working days after receipt) does not begin until the request is received by DHA, the Contractor shall act as quickly as possible.

In response to requests received by the Contractor for the release of information, unclassified information, documents and forms which were previously provided to the public as part of routine services shall continue to be made available in accordance with previously established criteria. All other requests from the public for release of DHA records and, specifically, all requests that reference the Freedom of Information Act shall be immediately forwarded to DHA, ATTENTION: Freedom of Information Officer, for appropriate action. Direct contact, including interim replies, between TRICARE contractors and such requestors is not authorized. The Contractor shall process requests by individuals for access to records about themselves in accordance with directions from the DHA Freedom of Information Service Center. If such a requestor specifically makes the request under the Privacy Act or does not make clear whether the request is made under FOIA or the Privacy Act, the Contractor shall process the request in accordance with directions from the DHA Privacy Office. If requestor specifically seeks PHI

under HIPAA, the Contractor shall follow paragraph 8.1.6, relating to individual rights of access to PHI.

4. Systems of Records

In order to meet the requirements of the Privacy Act and the DoD Privacy Act Issuances, the Contractor shall identify to the DHA Contracting Officer (CO) systems of records that are or will be maintained or operated for DHA where records of PII collected from individuals are maintained and specifically retrieved using a personal identifier. Upon identification of such systems to the CO, and prior to the lawful operation of such systems, the Contractor shall coordinate with the DHA Privacy Office to complete systems of records notices (SORNs) for submission and publication in the *Federal Register* as coordinated by the Defense Privacy and Civil Liberties Office, and as required by the DoD Privacy Act Issuances.

Following proper SORN publication and Government confirmation of Contractor authority to operate the applicable system(s), the Contractor shall also comply with the additional systems of records and SORN guidance, in coordination with the DHA Privacy Office, regarding periodic system review, amendments, alterations, or deletions set forth by the DoD Privacy Act Issuances, Office of Management and Budget (OMB) Memorandum 99-05, Attachment B, and OMB Circular A-130. The Contractor shall promptly advise the DHA Privacy Office of changes in systems of records or their use that may require a change in the SORN.

5. Privacy Impact Assessment (PIA)

The Contractor shall provide for the completion of a PIA for any applicable systems that collect, maintain, use or disseminate PII or PHI about members of the public, federal personnel, contractors, or in some cases foreign nationals. The Contractor shall establish practices that satisfy the requirements of DoDI 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance." (February 12, 2009).

To begin the PIA process, the Contractor shall use the DoD-approved PIA Template, DD Form 2930. The Contractor shall use the [DHA PIA Guide](#) to complete the [DD Form 2930](#). The Contractor should send completed DD Form 2930s to the DHA Privacy Office for review and approval, with a copy to the CO.

6. Data Sharing Agreement (DSA) (Applies if contract requirements involve PII/PHI or de-identified data that would be PII/PHI)

The Contractor shall consult with the DHA Privacy Office to determine if the Contractor must obtain a Data Sharing Agreement (DSA) or Data Use Agreement (DUA), when MHS data that is managed by DHA will be accessed, used, disclosed or stored, to perform the requirements of this Contract. The Contractor shall comply with requests for additional documentation by the DHA Privacy Board when requesting PHI for research.

In addition, the Contractor shall submit any research requests for MHS data that include PHI to the DHA Privacy Board in order to be reviewed for HIPAA compliance.

The Contractor shall comply with the permitted uses established in a DSA/DUA to prevent the unauthorized use and/or disclosure of any PII/PHI, in accordance with the HIPAA Rules and the DoD HIPAA Issuances. Likewise, the Contractor shall comply with the DoD Privacy Act Issuances.

To begin the data sharing request process, the Contractor shall submit a Data Sharing Agreement Application (DSAA) to the DHA Privacy Office. If the application is approved, the requestor shall enter into one of the following agreements, depending on the data involved:

- DSA for De-Identified Data
- DSA for PHI
- DSA for PII Without PHI
- Data Use Agreement for Limited Data Set.

DSAs are active for one year, or until the end of the current option year, whichever comes first. If the DSA will not be renewed, the Contractor shall provide a Certificate of Data Disposition (CDD) to the DHA Privacy Office.

7. Privacy Act and HIPAA Training

The Contractor shall ensure that its entire staff, including subcontractors and consultants that perform work on this Contract receive training on the Privacy Act, HIPAA, the Alcohol, Drug Abuse and Mental Health Administration (ADAMHA) Reorganization Act, 42 U.S.C. 290dd-2, and the ADAMHA implementing regulations, 42 CFR Part 2.

The Contractor shall ensure all employees and subcontractors supply a certificate of all training completion to the Contracting Officer's Representative (COR) within 30 days of being assigned and on an annual basis based on the trainee's birth month thereafter.

8. HIPAA Business Associate Provisions

8.1 Business Associate – General Provisions

The Contractor meets the definition of Business Associate, and DHA meets the definition of a covered entity under the HIPAA Rules and the DoD HIPAA Issuances. Therefore, a Business Associate Agreement (BAA) between the Contractor and DHA is required to comply with the HIPAA Rules and the DoD HIPAA Issuances. This paragraph 8 serves as the required BAA. As a Business Associate, the Contractor shall comply with the HIPAA Rules and the DoD HIPAA Issuances applicable to a business associate performing under this Contract.

8.1.1 Catch-All Definition: The following terms used, but not otherwise defined in paragraph 8.1, shall have the same meaning as those terms have in the DoD HIPAA Issuances: Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices (NoPP), Protected Health Information (PHI), Required

By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information (Unsecured PHI), and Use.

8.1.2 The Contractor shall not use or further disclose PHI other than as permitted or required by the Contract or as Required by Law.

8.1.3 The Contractor shall use appropriate safeguards, and comply with the HIPAA Security Rule with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Contract.

8.1.4 The Contractor shall report to DHA any breach of which it becomes aware, and shall proceed with breach response steps as required by Paragraph 9. With respect to electronic PHI, the Contractor shall also respond to any security incident of which it becomes aware in accordance with any Information Assurance provisions of this Contract. If at any point the Contractor becomes aware that a security incident involves a breach, the contractor shall immediately initiate breach response as required by paragraph 9.

8.1.5 In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), respectively, as applicable, the Contractor shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Contractor agree to the same restrictions, conditions, and requirements that apply to the Contractor with respect to such PHI.

8.1.6 With respect to individual rights of access to PHI, the Contractor shall make available PHI in a designated record set to the individual or the individual's designee as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.524. If the Contractor intends to deny the individual's request, the Contractor shall forward it (within seven working days of receipt) to the CO. The CO shall make a determination within 20 calendar days (50 calendar days for justified delays) of the request. The CO shall notify the individual, with a copy to the Contractor, of any approved or denied access determinations and the reason for any denial. The individual may appeal the denial determination to the DHA Privacy Office.

8.1.7 The Contractor shall make any amendment(s) to PHI in a designated record set as directed or agreed to by DHA, or take other measures as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.526.

8.1.8 The Contractor shall maintain and make available to the Government the information required to provide an accounting of disclosures to the MHS or to the individual as necessary to satisfy DHA's obligations under the DoD HIPAA Issuances and the corresponding 45 CFR 164.528.

8.1.9 To the extent the Contractor is to carry out one or more of DHA's obligation(s) under the HIPAA Rules, the Contractor shall comply with the requirements of the HIPAA Rules.

8.1.10 The Contractor shall make its internal practices, books, and records available to the HHS Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures

8.2 General Use and Disclosure Provisions

The Contractor may only use or disclose PHI as necessary to perform the services set forth in this Contract or as required by law. The Business Associate is not permitted to de-identify PHI under DoD HIPAA Issuances or the corresponding 45 CFR 164.514(a)-(c), nor is it permitted to use or disclose de-identified PHI, except as provided by the Contract or directed by DHA. The Contractor agrees to use, disclose and request PHI only in accordance with the HIPAA Privacy Rule “minimum necessary” standard and corresponding DHA policies and procedures as stated in the DoD HIPAA Issuances. The Contractor shall not use or disclose PHI in a manner that would violate the DoD HIPAA Issuances or HIPAA Privacy Rules if done by the covered entity, except uses and disclosures for the Contractor’s own management and administration and legal responsibilities or for data aggregation services as set forth in paragraphs 8.3.1 – 8.3.3.

8.3 Specific Use and Disclosure Provisions

8.3.1 Except as otherwise limited in this Section, the Contractor may use PHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor. The foregoing authority to use PHI does not apply to disclosure of PHI, which is covered in the next paragraph.

8.3.2 Except as otherwise limited in paragraph 8.3, the Contractor may disclose PHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor, provided that disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

8.3.3 Except as otherwise limited in this Section, the Contractor may use PHI to provide Data Aggregation services relating to DHA’s health care operations.

8.4 Contractor Compliance with DHA Notices and Restrictions

8.4.1 DHA will provide the Contractor with the notice of privacy practices that DHA produces in accordance with the DoD HIPAA Issuances and the corresponding 45 CFR 164.520.

8.4.2 Upon notification by DHA of any changes in, or revocation of, permission by an

Individual to use or disclose his or her PHI, the Contractor shall comply to the extent that such changes may affect the Contractor's use or disclosure of PHI.

8.4.3 Upon notification by DHA, the Contractor shall comply with any restriction on the use or disclosure of PHI that the Government has agreed to or is required to abide by under the DoD HIPAA Issuances or the corresponding 45 CFR 164.522 , to the extent that such restriction may affect Contractor's use or disclosure of PHI.

8.5 Permissible Requests by DHA

The Government will not request the Contractor to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules or any applicable Government regulations (including without limitation, DoD HIPAA Issuances) if done by the Government, except for providing Data Aggregation services to the Government and for management and administrative activities of the Contractor as otherwise permitted by this Contract.

8.6 Termination

8.6.1 Effect of Noncompliance

Noncompliance by the Contractor (or any of its staff, agents, or subcontractors) with any requirement in these HIPAA Business Associate Provisions (paragraph 8) may subject the Contractor to termination under any applicable default or other termination provision of this Contract.

8.6.2 Effect of Termination.

8.6.2.1 If this Contract has records management requirements, the Contractor shall handle such records in accordance with the records management requirements. If this Contract does not have records management requirements, the Contractor shall handle such records in accordance with paragraphs 8.6.2.2 and 8.6.2.3 below. If this Contract has provisions for transfer of records and PII/PHI to a successor contractor, or if DHA gives directions for such transfer, the Contractor shall handle such records and information in accordance with such Contract provisions or DHA direction.

8.6.2.2 If this Contract does not have records management requirements, except as provided in paragraph 8.6.2.3 below, upon termination of the Contract, for any reason, the Contractor shall return or destroy all PHI received from the Government, or created or received by the Contractor on behalf of the Government that the Contractor still maintains in any form. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Contractor. The Contractor shall retain no copies of the PHI.

8.6.2.3 If this Contract does not have records management provisions and the Contractor

determines that returning or destroying the PHI is infeasible, the Contractor shall provide to the Government notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Government and the Contractor that return or destruction of PHI is infeasible, the Contractor shall extend the protections of the Contract to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Contractor maintains such PHI.

8.7 Miscellaneous

8.7.1 Survival. The obligations of the Contractor under the “Effect of Termination” provision of this Paragraph 9 shall survive the termination of this Contract.

8.7.3 Interpretation. Any ambiguity in this Contract shall be interpreted in a manner to permit compliance with the HIPAA Rules and the DoD HIPAA Issuances.

9. Breach Response

In the event of a breach of PII/PHI by the Contractor, the Contractor shall follow the breach response requirements set forth in this paragraph, which are designed to satisfy both the Privacy Act and HIPAA as applicable. If a breach involves only PII, then the Contractor shall comply with DoD Privacy Act Issuance breach response requirements only; if a breach involves PHI (a subset of PII), then the Contractor shall comply with both Privacy Act and HIPAA breach response requirements. A breach involving PHI may or may not constitute an HHS Breach. If a breach is not an HHS Breach, then the Contractor has no HIPAA breach response obligations. In such cases, the Contractor must still comply with breach response requirements under the DoD Privacy Act Issuances.

If the DHA Privacy Office determines that a breach is an HHS Breach, then the Contractor shall comply with both the HIPAA Breach Rule and DoD Privacy Act Issuances, as directed by the Privacy Office, regardless of whether the breach occurs at DHA or at one of the Service components. If the Privacy Office determines that the breach does not constitute an HHS Breach, then the Contractor shall comply with DoD Privacy Act Issuances, as directed by the Privacy Office. *[If the Government party to this Contract is one of the Services or a Service component, then the applicable Service-Level Privacy Office oversees Privacy Act compliance (the only DHA Privacy Office role is to track the Service-level breach response efforts). Additional Service-specific provisions may be appropriate here.]*

The following provisions of this paragraph set forth the Contractor’s Privacy Act and HIPAA breach response requirements for DHA breaches, including but not limited to HHS breaches. For other breaches not involving the DHA Privacy Office (i.e., Privacy Act-only breaches occurring at a Service-level component), the Contractor shall follow the directions of the Service-Level Privacy Office.

The Contractor shall comply with all breach response requirements set forth in this paragraph. In general, for breach response, the Contractor shall report the breach to the government, assess the breach incident, notify affected individuals, and take mitigation actions as applicable. Because DoD defines “breach” to include possible (suspected) as well as actual (confirmed) breaches, the Contractor shall implement these breach response requirements immediately upon the Contractor’s discovery of a possible breach.

9.1 Reporting Provisions

The Contractor shall report the breach within one hour of discovery to the US Computer Emergency Readiness Team (US CERT), and, within 24 hours of discovery, to the DHA Privacy Office, and the other parties set forth below. The Contractor is deemed to have discovered a breach as of the time a breach (suspected or confirmed) is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing it) who is an employee, officer or other agent of the Contractor.

The Contractor shall submit the US-CERT report using the online form at <https://forms.us-cert.gov/report/>. Before submission to US-CERT, the Contractor shall save a copy of the on-line report. After submission, the Contractor shall record the US-CERT Reporting Number. Although only limited information about the breach may be available as of the one hour deadline for submission, the Contractor shall submit the US-CERT report by the deadline. The Contractor shall e-mail updated information as it is obtained, following the instructions at <http://www.us-cert.gov/pgp/email.html>. The Contractor shall provide a copy of the initial or updated US-CERT report to the DHA Privacy Office and the applicable Service-Level Privacy Office, if requested by either. Contractor questions about US-CERT reporting shall be directed to the DHA Privacy Office, not the US-CERT office.

The Contractor report to DHA due within 24 hours shall be submitted by completing the New Breach Reporting Form DD 2959 at the Breach Response page on the DHA Privacy Office web site and emailing that form to the DHA Privacy Office, the DHA CO and COR, and the DHA Program Office (or Service-Level Privacy Office) applicable to the Contractor. For the applicable Program Office, the Contractor shall e-mail the notice to its usual Point of Contact (POC) unless the POC specifies another addressee for breach reporting. Encryption is not required, because Breach Report Forms should not contain PII/PHI. The email address for notices to the DHA Privacy Office is provided at the Privacy Office website breach response page. If electronic mail is not available, telephone notification is also acceptable, but all notifications and reports delivered telephonically must be confirmed by email as soon as technically feasible.

If multiple beneficiaries are affected by a single event or related set of events, then a single reportable breach may be deemed to have occurred, depending on the circumstances. The Contractor shall inform the DHA Privacy Office as soon as possible if it believes that “single event” breach response is appropriate; the DHA Privacy Office will determine how the

Contractor shall proceed and, if appropriate, consolidate separately reported breaches for purposes of Contractor report updates, beneficiary notification, and mitigation. The corresponding CDRL, entitled “Breach Report,” provides further guidance on completing and updating the Breach Report Form.

When a Breach Report Form initially submitted is incomplete or incorrect due to unavailable information, or when significant developments require an update, the Contractor shall submit a revised form or forms, stating the updated status and previous report date(s) and showing any revisions or additions in red text. Examples of updated information the Contractor shall report include, but are not limited to: confirmation on the exact data elements compromised, the root cause of the incident, and any mitigation actions to include, sanctions, training, incident containment, follow-up, etc. The Contractor shall submit these report updates promptly after the new information becomes available. Prompt reporting of updates is required to allow the DHA Privacy Office to make timely final determinations on any subsequent notifications or reports. The Contractor shall provide updates to the same parties as required for the initial Breach Report Form. The Contractor is responsible for reporting all information needed by the DHA Privacy Office to make timely and accurate determinations on reports to HHS as required by the HHS Breach Rule and reports to the Defense Privacy and Civil Liberties Office as required by DoD Privacy Act Issuances.

In the event the Contractor is uncertain on how to apply the above requirements, the Contractor shall consult with the CO, who will consult with the Privacy Office as appropriate when determinations on applying the above requirements are needed.

9.2 Individual Notification Provisions

If the Privacy Office determines that individual notification is required, the Contractor shall provide written notification to individuals affected by the breach as soon as possible, but no later than 10 working days after the breach is discovered and the identities of the individuals are ascertained. The 10 day period begins when the Contractor is able to determine the identities (including addresses) of the individuals whose records were impacted.

The Contractor’s proposed notification to be issued to the affected individuals shall be submitted to the parties to which reports are submitted under paragraph 9.1 for their review, and for approval by the DHA Privacy Office. Upon request, the Contractor shall provide the DHA Privacy Office with the final text of the notification letter sent to the affected individuals. If different groups of affected individuals receive different notification letters, then the Contractor shall provide the text of the letter for each group. (PII shall not be included with the text of the letter(s) provided.) Copies of further correspondence with affected individuals need not be provided unless requested by the Privacy Office. The Contractor’s notification to the individuals, at a minimum, shall include the following:

—The individual(s) must be advised of what specific data was involved. It is insufficient to

simply state that PII has been lost. Where names, Social Security Numbers (SSNs) or truncated SSNs, and Dates of Birth (DOBs) are involved, it is critical to advise the individual that these data elements potentially have been breached.

—The individual(s) must be informed of the facts and circumstances surrounding the breach. The description should be sufficiently detailed so that the individual clearly understands how the breach occurred.

—The individual(s) must be informed of what protective actions the Contractor is taking or the individual can take to mitigate against potential future harm. The notice must refer the individual to the current Federal Trade Commission (FTC) web site pages on identity theft and the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261.

—The individual(s) must also be informed of any mitigation support services (e.g., one year of free credit monitoring, identification of fraud expense coverage for affected individuals, provision of credit freezes, etc.) that the Contractor may offer affected individuals, the process to follow to obtain those services and the period of time the services will be made available, and contact information (including a phone number, either direct or toll-free, e-mail address and postal address) for obtaining more information.

Contractors shall ensure any envelope containing written notifications to affected individuals are clearly labeled to alert the recipient to the importance of its contents, e.g., "Data Breach Information Enclosed," and that the envelope is marked with the identity of the Contractor and/or subcontractor organization that suffered the breach. The letter must also include contact information for a designated POC to include, phone number, email address, and postal address.

If the Contractor determines that it cannot readily identify, or will be unable to reach, some affected individuals within the 10 day period after discovering the breach, the Contractor shall so indicate in the initial or updated Breach Report Form. Within the 10 day period, the Contractor shall provide the approved notification to those individuals who can be reached. Other individuals must be notified within 10 days after their identities and addresses are ascertained. The Contractor shall consult with the DHA Privacy Office, which will determine the media notice most likely to reach the population not otherwise identified or reached. The Contractor shall issue a generalized media notice(s) to that population in accordance with Privacy Office approval.

The Contractor shall, at no cost to the government, bear any costs associated with a breach of PII/PHI that the Contractor has caused or is otherwise responsible for addressing.

Breaches are not to be confused with security incidents (often referred to as cyber security incidents when electronic information is involved), which may or may not involve a breach of PII/PHI. In the event of a security incident not involving a PII/PHI breach, the Contractor shall follow applicable DoD Information Assurance requirements under its contract. If at any point the

Contractor finds that a cyber security incident involves a PII/PHI breach (suspected or confirmed), the Contractor shall immediately initiate the breach response procedures set forth below. The Contractor shall also continue to follow any required cyber security incident response procedures to the extent needed to address security issues, as determined by DoD/DHA.