

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

## **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 Portability 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 (October 29, 1014) 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-E (Enforcement), as amended. 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 Military Health System (MHS). These issuances are DoD 6025.18-R (January 24, 2003), DoDI 6025.18 (December 2, 2009), and DoDI 8580.02 (August 12, 2015).

***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).

## **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) and Records Management requirements outlined in the current TRICARE Operations Manual (TOM).

### **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 [DHA.FOIA@mail.mil](mailto:DHA.FOIA@mail.mil)), and that the request shall describe the desired record as completely as possible (ideally with Contract or modification number) 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 FOIA 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, Civil Liberties, and Transparency Division, 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)**

Contractors are not required to submit PIAs to DHA.

## **6. Data Sharing Agreement (DSA)**

### **6.1 (Applies if contract requirements involve the use of DHA data (including PII/PHI, a limited data set, or de-identified data))**

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 DHA data will be accessed, used, disclosed or stored, to perform the requirements of this Contract.

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 DoD HIPAA Issuances. Likewise, the Contractor shall comply with the DoD Privacy Act Issuances.

Data use involving PHI for research purposes, as defined by HIPAA, will also be reviewed by the DHA Privacy Board. Thus, the Contractor shall comply with DHA Privacy Board requests for additional documentation.

To begin the DSA request process, the Contractor shall submit a DSA Application (DSAA) to the DHA Privacy Office. Upon approval, 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
- DUA for Limited Data Set.

DSAs executed for contract support will expire after one year, or at the end of the contract option year, whichever comes first. If the contractual use of DHA data will continue after the DSA expiration date, the Contractor shall submit a DSA Renewal Request template to the Privacy Office; however, if the DSA will not be renewed, the Contractor shall close the DSA by providing a Certificate of Data Disposition (CDD) to the DHA Privacy Office.

### **6.2 (Applies if contract requirements may include human subjects research)**

This Contract incorporates by reference the Protection of Human Subjects Research clause in the Defense Federal Acquisition Regulation Supplement (DFARS) at 48 CFR 252.235-7004. A separate DFARS provision, 48 CFR 235.072(e), requires that the clause be incorporated in contracts that include or may include research involving human subjects in accordance with 32

CFR 219, DoDI 3216.02, and 10 U.S.C. 980, including research that meets exemption criteria under 32 CFR 219.101(b), The clause applies to solicitations and contracts awarded by any DoD component, regardless of mission or funding Program Element Code. Thus, in the event a contractor participates in a study or demonstration project or other activity that involves human subjects research, then the contractor shall comply with Protection of Human Subjects Research clause. Contracting officers may not determine whether an activity is exempt from human subject research requirements. If contractor activity appears to involve human subject research, then the contractor shall consult the DHA Privacy Office, which may contact the Research Regulatory Oversight Office in the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD (P&R)).

## **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, and the federal regulations on confidentiality of alcohol and drug abuse patient records, 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 (if this Contract incorporates by reference the TRICARE Operations Manual (TOM), then all references to paragraph 9 shall be deemed to refer to the breach response provisions of the TOM, Ch. 1, Sec. 5, paragraphs 2.1-2.2). With respect to electronic PHI, the Contractor shall also respond to any security incident of which it becomes aware in accordance with any applicable DoD cybersecurity and National Institute of Standards and Technology (NIST) requirements. 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** *[This paragraph 9 is inoperative, and all references herein to “paragraph 9” shall be deemed to refer to the TOM breach responses provisions, if the contract incorporates the TOM by reference. See paragraph 8.1.4 above,]*

## **9.1 Definitions Related to Breach response**

**9.1.1 Breach** means a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than an authorized purpose have access or potential access to PII, whether physical or electronic. The foregoing definition is based on the definition of breach in DoDD 5400.11. Breaches are classified as either possible or confirmed (see the following two definitions) and as either cyber or non-cyber (i.e., involving either electronic PII/PHI or paper/oral PII/PHI).

**9.1.2 A possible breach** is an incident where the possibility of unauthorized access is suspected (or should be suspected) and has not been ruled out. For example, if a laptop containing PII/PHI is lost, and the contractor does not initially know whether or not the PII/PHI was encrypted, then the incident must initially be classified as a possible breach, because it is impossible to rule out the possibility of unauthorized access to the PII/PHI. In contrast, that possibility can be ruled out immediately, and a possible breach has not occurred, when misdirected postal mail is returned unopened in its original packaging. However, if the intended recipient informs the contractor that an expected package has not been received, then a possible breach exists until and unless the unopened package is returned to the contractor. In determining whether unauthorized access should be suspected, the contractor shall consider at least the following factors:

- How the event was discovered;
- Did the information stay within the covered entity’s control;
- Was the information actually accessed/viewed; and
- Ability to ensure containment (e.g., recovered, destroyed, or deleted).

**9.1.3 A confirmed breach** is an incident in which it is known that unauthorized access could occur. For example, if a laptop containing PII/PHI is lost and the contractor knows that the

PII/PHI is unencrypted, then the contractor should classify and report the incident as a confirmed breach, because unauthorized access could occur due to the lack of encryption (the contractor knows this even without knowing whether or not unauthorized access to the PII/PHI has actually occurred). If the laptop is subsequently recovered and forensic investigation reveals that files containing PII/PHI were never accessed, then the possibility of unauthorized access can be ruled out, and the contractor should re-classify the incident as a non-breach incident.

**9.1.4 A HIPAA breach** is an incident that satisfies the definition of breach in 45 CFR 164.402.

**9.1.5 A cybersecurity incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices, with respect to electronic PII/PHI. A cybersecurity incident may or may not involve a breach of PII/PHI. For example, a malware infection would be a possible breach if it could cause unauthorized access to PII/PHI. However, if the malware only affects data integrity or availability (not confidentiality), then a non-breach cybersecurity incident has occurred.

## **9.2 General**

**9.2.1** The breach response requirements set forth in this paragraph 9 are designed to satisfy both the DoD Privacy Act Issuances and the HIPAA Breach Rule, 45 CFR Part 164, Subpart D, as applicable. The definition of **breach** above is based on the definition of breach in the DoD Privacy Act Issuances. This Privacy Act definition is broader than a HIPAA breach as defined above. Thus, a Privacy Act breach would not constitute a HIPAA breach if the PII involved does not include PHI, or if it involves PHI but is excluded from the definition of HIPAA breach. If a breach is not a HIPAA 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, as stated in this paragraph 9.

**9.2.2** 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. These procedures focus on the first two steps (breach identification and reporting) of a comprehensive breach response program, but also require addressing the remaining steps: containment, mitigation (which includes individual notification), eradication, recovery, and follow-up.

**9.2.3** The contractor shall establish internal processes for carrying out the procedures set forth below. These processes shall assign responsibility for investigating, classifying, reporting and otherwise responding to breaches and cybersecurity incidents. The contractor should consult with the DHA Privacy Office where guidance is needed, such as when the contractor is uncertain whether a discovered breach is the contractor’s responsibility (e.g., if the contractor discovers a breach not caused by the contractor), or how the contractor is classify an incident (breach vs. non-breach, confirmed vs. possible, cyber vs. non-cyber). Under no circumstances will a contractor delay reporting a confirmed or possible breach to the DHA Privacy Office beyond the

24-hour deadline (see paragraph 9.3.2) while waiting for the DHA Privacy Office guidance or while investigating the incident. In conjunction with its initial investigation, the contractor shall immediately take steps to minimize any impact from the occurrence, proceed with further investigation of any relevant details (such as root causes, vulnerabilities exploited), and initiate further breach response steps.

**9.2.4** In the event of a cybersecurity incident not involving a PII/PHI breach, the contractor shall follow applicable DoD cybersecurity and NIST requirements, which include United States-Computer Emergency Readiness Team (US-CERT) reporting (see paragraph 9.3 below). If at any point a contractor finds that a cybersecurity incident involves a PII/PHI breach (possible or confirmed), the contractor shall immediately initiate the reporting procedures set forth below. The contractor shall also continue to follow any required cybersecurity incident response procedures and other applicable DoD cybersecurity requirements.

**9.2.5** Contractors shall require subcontractors who discover a possible breach or cybersecurity incident to initiate the incident response requirements herein by reporting the incident to the contractor immediately after discovery. The time of that report to the contractor shall trigger the contractor's DHA Privacy Office reporting deadline (24 hours) under paragraph 9.3.2. If a cybersecurity incident is involved, the contractor's deadline for US-CERT reporting (one hour) runs from the time the incident is confirmed. The contractor shall require the subcontractor to cooperate as necessary to meet these deadlines, maintain records, and otherwise enable the contractor to complete the breach response requirements herein. Alternatively, the contractor and subcontractor may agree that the subcontractor shall report directly to US-CERT and the DHA Privacy Office, and that the subcontractor shall be responsible for completing the response process, provided that such agreement requires the subcontractor to inform the contractor of the incident and the subsequent response actions.

**9.2.6** Contractors shall maintain records of all breach and cybersecurity incident investigations, regardless of the outcome. Investigations identifying unauthorized disclosures must be logged for HIPAA and Privacy Act disclosure accounting purposes, whether or not individual notification is required under the HIPAA Breach Rule.

**9.2.7** Contractors, when acting as HIPAA-covered entities (rather than as business associates), are not subject to the breach response requirements herein. However, such contractors are subject to both the HIPAA Breach Rule (applicable to them in their capacity as covered entities) and DoD cybersecurity requirements (applicable to them in their capacity as DoD contractors).

### **9.3 Reporting Provisions**

**9.3.1** Immediately upon discovery of a possible or confirmed breach or cybersecurity incident, the contractor shall initiate an investigation. If the incident involves electronic PII/PHI, and if the investigation finds a confirmed breach or cybersecurity incident, the contractor shall report it, within one hour of confirmation, to the United States-Computer Emergency Readiness Team

(US-CERT) Incident Reporting System at <https://forms.us-cert.gov/report/>, as required by the Department of Homeland Security (DHS).

**Note:** DHS no longer requires US-CERT reporting of non-cyber breaches or unconfirmed electronic breaches. However, DHS permits US-CERT reporting of unconfirmed cyber-related incidents on a voluntary basis. Thus, if a contractor is uncertain whether a possible cyber-related incident should be treated as confirmed and thus reportable, the contractor may voluntarily report the incident.

Before submission to US-CERT, the contractor shall save a copy of the on-line report. After submitting the report, the contractor shall record the US-CERT incident reporting number, which shall be included in the initial report to the DHA Privacy Office as described in paragraph 9.3.2.

**Note:** Regardless of whether or not an incident is confirmed as a breach, the contractor must also investigate whether or not the incident impacts data integrity or availability of PII/PHI. If such impact is confirmed, then the incident is reportable to US-CERT as a cybersecurity incident. For guidance on investigating the impact on data integrity and availability, refer to DoD cybersecurity and NIST guidance.

The contractor shall provide any updates to the initial US-CERT report by email to [soc@us-cert.gov](mailto:soc@us-cert.gov), with the Reporting Number in the subject line. The contractor shall provide a copy of the initial or updated US-CERT report to the DHA Privacy Office if requested. Contractor questions about US-CERT reporting shall be directed to the DHA Privacy Office, not the US-CERT office.

**9.3.2** In addition to US-CERT reporting, the contractor shall report to the DHA Privacy Office by submitting the form specified below within 24 hours of discovery of a breach (possible or confirmed), unless the breach falls within a category that the Privacy Office has determined to be not reportable. This 24 hour period runs from the time of discovery, unlike the one hour US-CERT reporting period, which runs from the time a cybersecurity incident is confirmed. Thus, depending on the time period needed to confirm, the report to the DHA Privacy Office may be due either before or after the US-CERT report.

The breach report form required within the 24 hour deadline shall be sent by e-mail to: [DHA.PrivacyOfficer@mail.mil](mailto:DHA.PrivacyOfficer@mail.mil). The contractor shall also e-mail the report to the CO, the COR and its usual point of contact at the applicable Program Office. Encryption is not required, because reports and notices shall not contain PII/PHI. If electronic mail is not available, telephone notification is also acceptable (at 703-275-6363), but all notifications and reports delivered telephonically must be confirmed in writing as soon as technically feasible.

Contractors shall prepare the breach reports required within the 24 hour deadline by completing the Breach Reporting DD Form DD 2959 (Breach of PII Report), available at the Breach Response link on the DHA Privacy Office web site, <http://www.health.mil/Military-Health->

Topics/Privacy-and-Civil-Liberties/Breaches-of-PII-and-PHI. For non-cyber incidents without a US-CERT number, the contractor shall assign an internal tracking number and include that number in Box 1.e of the DD Form 2959. The contractor shall coordinate with the DHA Privacy Office for subsequent action such as beneficiary notification, and mitigation. The contractor must promptly update the DD Form 2959 as new information becomes available.

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 promptly after the new information becomes available, stating the updated status and previous report date(s) and showing any revisions or additions in red text. The Contractor shall provide updates to the same parties as required for the initial Breach Report Form.

### **9.3 Individual Notification Provisions**

**9.3.1** If the DHA Privacy Office determines that individual notification is required, the Contractor shall provide written notification to beneficiaries 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 beneficiaries are ascertained. The 10 day period begins when the Contractor is able to determine the identities (including addresses) of the beneficiaries whose records were impacted. If notification cannot be accomplished within 10 working days, the contractor shall notify the DHA Privacy Office.

**9.3.2** The Contractor's proposed notification to be issued to the affected beneficiaries shall be submitted to the DHA Privacy Office for approval. The notification to beneficiaries shall include, at a minimum, the following:

- Specific data elements
- Basic facts and circumstances
- Recommended precautions the beneficiary can take
- Federal Trade Commission (FTC) identity theft hotline information
- Any mitigation support services offered such as credit monitoring.

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.

If media notice is required, the contractor will submit a proposed notice and suggested media outlets for the DHA Privacy Office review (which will include coordination with the DHA Communications Division) and approval.

**9.4.** 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.

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.