A. EXCLUSION FROM PARTICIPATION IN FEDERAL HEALTH CARE PROGRAMS (OCTOBER 2015)

1. The Contractor shall not employ or contract with any individual or entity (hereinafter collectively referred to as "person") to provide items or services that will be included in invoices submitted to the Government under this contract if such person is listed on the Department of Health and Human Services (HHS) Office of the Inspector General (OIG) List of Excluded Individuals and Entities (LEIE) or the TRICARE Sanctioned Provider List. The Government is legally prohibited from paying for provision of items or services by such persons. The prohibition extends to services beyond direct patient care, such as services of persons in executive or leadership roles and administrative and management services, whether or not such services are billed separately. The LEIE may be found at http://oig.hhs.gov/fraud/exclusions.asp, and the TRICARE Sanctioned Provider list at http://www.health.mil/Military-Health-Topics/Access-Cost-Quality-and-Safety/Quality-And-Safety-of-Healthcare/Program-Integrity/Sanctioned-Providers. The LEIE and TRICARE Sanctioned Provider List are hereinafter collectively referred to as "the Lists."

2. Prior to start of contract performance, the Contractor shall (a) query the Lists to determine whether the name of any person the Contractor employs or contracts with to provide services or items for which payment may be made under this contract appears on the Lists, and (b) certify to the Contracting Officer that the Contractor has queried the Lists and no such names appear on either of the Lists.

3. During performance of the contract, and prior to persons other than those whose names were queried in accordance with paragraph 2, above, (hereinafter "new persons") providing services or items under the contract, the Contractor shall (a) query the Lists as in paragraph 2, and (b) certify to the Contracting Officer that the names of such new persons do not appear on either of the Lists.

4. The Contractor is advised that during performance of the contract, MTF personnel will periodically recheck of the names of contractor personnel working in the MTF against the Lists. The Government will notify the Contractor in the event any contractor personnel working in the MTF appear on either of the Lists.

5. Should any person providing items or services under the contract appear on either of the Lists at any time during contract performance, the Contractor shall promptly remove that person from the contract.

6. Violation of any aspect of the above paragraphs shall be considered a material breach of the contract and may result in termination of the contract.

7. The Contractor is further advised that, in accordance with Civil Monetary Penalties Law [CMP] (codified at 42 USC § 1320a-7a):

a. There are steep civil monetary penalties associated with billing the Government for providing items or services by a person on either of the Lists, and with failing to return to the Government any overpayments received for provision of such items or services.

b. Billing under the contract for provision of items or services by a person on either List may also result in exclusion of the person that employs or contracts with such person.

8. HHS OIG has issued a Special Advisory Bulletin on the Effect of Exclusion from Participation in Federal Health Care Programs with additional information on the CMP. The Special Advisory Bulletin may be found at http://oig.hhs.gov/exclusions/files/sab-05092013.pdf.

B. PERSONALLY IDENTIFIABLE INFORMATION, PROTECTED HEALTH INFORMATION, AND FEDERAL INFORMATION REQUIREMENTS (REVISED 10/27/2020)

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 Department of Defense (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 DoDI 5400.11, DoD Privacy and Civil Liberties Programs, January 29, 2019 and DoDI 5400.11-R, Department of Defense Privacy Program, 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 Code of Federal Regulations (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 DoDM 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019, DoDI 6025.18, Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs, March 13, 2019, and DoDI 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs, August. 12, 2015.

Defense Health Agency (DHA) Privacy Office is the DHA Privacy and Civil Liberties Office. The DHA Privacy Office Chief is the HIPAA Privacy and Security Officer for DHA.

2. Records Management

When creating and maintaining official government records, the Contractor shall comply with all federal requirements established by 44 United States Code (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 preferably sent via the National FOIA Portal at: www.FOIA.gov. However, requesters may also submit requests via email at

DHA.FOIA@mail.mil; or via postal delivery addressed to the DHA Freedom of Information Service Center, 7700 Arlington Boulevard, Suite 5101, Falls Church, Virginia 22042-5101. All FOIA requests 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. Contract and/or Modification numbers must be included in all FOIA requests seeking DHA procurement records. 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 and respond to DHA within ten working days.

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, OMB Circular A-130, and Privacy Act of 1974 requirements applicable to contractors operating systems of records on behalf of federal agencies. 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)

If DHA data is stored on a Contractor owned system, a PIA is required from the Contractor.

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 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.

Prior to using any data involving PHI for research purposes, as defined by HIPAA, the Contractor must gain approval from 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 1 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 subject research)

This Contract incorporates by reference the Protection of Human Subject 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 subject research, then the contractor shall comply with Protection of Human Subject Research clause. COs 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 substance use disorder patient records, 42 CFR Part 2. Refer to FAR 52.224-3 regarding specific requirements for Privacy Training appropriate to the Contractor's scope of involvement with DHA's PHI and its regulatory responsibilities as either a Covered Entity, or Business Associate.

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. The contractor shall use the DoD BAA, which shall be used by all organizational entities within the DoD, referred to collectively as the "DoD Components", located at, https://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Contract-Language/HIPAA-Compliant-Business-Associate-Agreement-for-the-MHS. b.i. and (3)b.ii

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]

9.1. Definitions Related to Breach response

9.1.2 Breach means a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses PII; or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. The foregoing definition is based on the definition of breach in DoDM 6025.18. 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).

9.1.3 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).

9.1.4. 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.

9.1.5. A HHS breach is an incident that satisfies the definition of breach in Section 164.402 of the HIPAA Breach Rule. The text of the HHS definition states:

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part [i.e. the HIPAA Privacy Rule] which compromises the security or privacy of the PHI.

HHS breach excludes:

Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a DoD covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

Any inadvertent disclosure by a person who is authorized to access PHI at a DoD covered entity or business associate to another person authorized to access PHI at the same DoD covered entity or business associate, or organized health care arrangement in which the DoD covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted the HIPAA Privacy Rule.

A disclosure of PHI where a DoD covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Except as provided in this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under this issuance is presumed to be a breach unless the DoD covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

The unauthorized person who used the PHI or to whom the disclosure was made;

Whether the PHI was actually acquired or viewed; and

The extent to which the risk to the PHI has been mitigated.

9.1.6. 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 shall be followed for all unauthorized use or disclosure of information regardless of whether the information is PHI or solely PII.

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 to 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. 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). 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 (1 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, and not 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 1 hour of confirmation, to the 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, 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 1 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. 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 Department of Defense Form DD 2959 (Breach of PII Report), available at https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2959.pdf. 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.

9.4 Individual Notification Provisions

9.4.1 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 and addresses 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.

9.4.2. 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, and
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 and approval (which will include coordination with the DHA Communications Division).

9.5 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.