This Business Associate Agreement (BAA) incorporates HIPAA/HITECH Act requirements under the HHS Final Omnibus Rule (78 FR 5566, published 25 Jan 2013), effective 23 Sep 2013. This BAA is for use by MHS components outside of DHA. This BAA can serve as a separate agreement or may be used to modify an existing contract or other agreement between the MHS component and the business associate. It is also appropriate for new contracts or agreements. In each case, the MHS component should consult with the Contracting Officer or other POC and the Service-level privacy officials for completing and/or modifying this BAA as may be appropriate. At several points, bracketed language indicates where additional or different language may be needed, including specifics regarding breach response.

This BAA is NOT to be used in contracts for components of DHA. Those components should request contract language from the DHA Procurement Directorate. Contact ContractPolicyDivision@dha.mil.

Draft Business Associate Agreement

Introduction

In accordance with 45 CFR 164.502(e)(2) and 164.504(e) and paragraph C.3.4.1.3 of DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003 *[replace with corresponding paragraph in the pending successor issuance, DoDI 6025.18, Enclosure 3, when published]*, this document serves as a business associate agreement (BAA) between the signatory parties for purposes of the Health Insurance Portability and Accountability Act (HIPAA) and the "HITECH Act" amendments thereof, as implemented by the HIPAA Rules and DoD HIPAA Issuances (both defined below). The parties are a DoD Military Health System (MHS) component, acting as a HIPAA covered entity, and a DoD contractor, acting as a HIPAA business associate. The HIPAA Rules require BAAs between covered entities and business associates. Implementing this BAA requirement, the applicable DoD HIPAA Issuance (DoD 6025.18-R, paragraph C3.4.1.3) *[replace with corresponding paragraph in the pending successor issuance, DoDI 6025.18, Enclosure 3, when published]* provides that requirements applicable to business associates must be incorporated (or incorporated by reference) into the contract or agreement between the parties.

(a) **Catchall Definition**. Except as provided otherwise in this BAA, the following terms used in this BAA shall have the same meaning as those terms in the DoD HIPAA Rules: 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, and Use.

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.

Business Associate shall generally have the same meaning as the term "business associate" in the DoD HIPAA Issuances, and in reference to this BAA, shall mean *[insert name of Business Associate signatory to this BAA]*.

Agreement means this BAA together with the documents and/or other arrangements under which the Business Associate signatory performs services involving access to PHI on behalf of the MHS component signatory to this BAA.

Covered Entity shall generally have the same meaning as the term "covered entity" in the DoD HIPAA Issuances, and in reference to this BAA, shall mean *[insert name of MHS component signatory to this BAA]*.

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

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 (2003), DoDI 6025.18 (2009), and DoD 8580.02-R (2007). *[These citations should be replaced with citations to the pending successor issuances when those are published.]*

DoD Privacy Act Issuances means the DoD issuances implementing the Privacy Act, which are DoDD 5400.11 (2007) and DoD 5400.11-R (2007). *[The latter citation should be replaced with a citation to the pending successor issuance when it is published.]*

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

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, implementing the "HITECH Act" provisions of Pub. L. 111-5. See 78 FR 5566-5702 (Jan. 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 BAA and are not included in the term HIPAA Rules.

Service-Level Privacy Office means one or more offices within the military services (Army, Navy, or Air Force) with oversight authority over Privacy Act and HIPAA privacy compliance. *[This definition may need tailoring to the service-specific organizational structure.]*

I. Obligations and Activities of Business Associate

(a) The Business Associate shall not use or disclose PHI other than as permitted or required by the Agreement or as required by law.

(b) The Business Associate shall use appropriate safeguards, and comply with the DoD HIPAA Rules with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Agreement.

(c) The Business Associate shall report to Covered Entity any Breach of which it becomes aware, and shall proceed with breach response steps as required by Part V of this BAA. With respect to electronic PHI, the Business Associate shall also respond to any security incident of which it becomes aware in accordance with any Information Assurance provisions of the Agreement. If at any point the Business Associate becomes aware that a security incident involves a Breach, the Business Associate shall immediately initiate breach response as required by part V of this BAA.

(d) In accordance with 45 CFR 164.502(e)(1)(ii)) and 164.308(b)(2), respectively), as applicable, the Business Associate shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such PHI. *[When the pending successor issuances are published, then the preceding sentence should begin as follows: "In accordance with DoDI 6025.18, Enclosure 3, paragraph ___, DoDI 8580.02, Enclosure 3, paragraph __, and 45 CFR 164.502(e)(1)(ii)) and 164.308(b)(2), as applicable, the Business Associate shall …"]*

(e) The Business Associate shall make available PHI in a Designated Record Set, to the Covered Entity or, as directed by the Covered Entity, to an Individual, as necessary to satisfy the Covered Entity obligations under 45 CFR 164.524.

(f) The Business Associate shall make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526.

(g) The Business Associate shall maintain and make available the information required to provide an accounting of disclosures to the Covered Entity or an individual as necessary to satisfy the Covered Entity's obligations under 45 CFR 164.528.

(h) To the extent the Business Associate is to carry out one or more of Covered Entity's

obligation(s) under the HIPAA Privacy Rule, the Business Associate shall comply with the requirements of HIPAA Privacy Rule that apply to the Covered Entity in the performance of such obligation(s); and

(i) The Business Associate shall make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

II. Permitted Uses and Disclosures by Business Associate

(a) The Business Associate may only use or disclose PHI as necessary to perform the services set forth in the Agreement 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 Agreement or directed by the Covered Entity.

(b) The Business Associate 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.

(c) The Business Associate 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 Business Associate's own management and administration and legal responsibilities or for data aggregation services as set forth in the following three paragraphs.

(d) Except as otherwise limited in the Agreement, the Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. The foregoing authority to use PHI does not apply to disclosure of PHI, which is covered in the next paragraph.

(e) Except as otherwise limited in the Agreement, the Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or the Business Associate 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 Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(f) Except as otherwise limited in the Agreement, the Business Associate may use PHI to provide Data Aggregation services relating to the Covered Entity's health care operations.

III. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) The Covered Entity shall provide the Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with 45 CFR 164.520 and the corresponding provision of the DoD HIPAA Issuances.

(b) The Covered Entity shall notify the Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes affect the Business Associate's use or disclosure of PHI.

(c) The Covered Entity shall notify the Business Associate of any restriction on the use or disclosure of PHI that the Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

IV. Permissible Requests by Covered Entity

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

V. Breach Response

(a) In general.

In the event of a breach of PII/PHI held by the Business Associate, the Business Associate shall follow the breach response requirements set forth in this Part V, which is designed to satisfy both the Privacy Act and HIPAA as applicable. If a breach involves PII without PHI, then the Business Associate shall comply with DoD Privacy Act Issuance breach response requirements only; if a breach involves PHI (a subset of PII), then the Business Associate 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 Business Associate has no HIPAA breach response obligations. In such cases, the Business Associate 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 Business Associate shall comply with both the HIPAA Breach Rule and DoD Privacy Act Issuances, as directed by the DHA Privacy Office, regardless of whether the breach occurs at DHA or at one

of the Service components. If the DHA Privacy Office determines that the breach does not constitute an HHS Breach, then the Business Associate shall comply with DoD Privacy Act Issuances, as directed by the applicable Service-Level Privacy Office. *[The Service-Level Privacy Office may wish to add more specific provisions here and below addressing what is required when the incident is not an HHS Breach. The only DHA Privacy Office role in that situation is to track the Service-level breach response.]* The following provisions of Part V set forth the Business Associate's Privacy Act and HIPAA breach response requirements for all breaches, including but not limited to HHS breaches.

This Part V is designed to satisfy the DoD Privacy Act Issuances and the HIPAA Breach Rule as implemented by the DoD HIPAA Issuances. In general, for breach response, the Business Associate shall report the breach to the Covered Entity, 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 Business Associate shall implement these breach response requirements immediately upon the Business Associate's discovery of a possible breach.

(b) Government Reporting Provisions

The Business Associate 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 Business Associate 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 Business Associate.

The Business Associate shall submit the US-CERT report using the online form at https://forms.us-cert.gov/report/. Before submission to US-CERT, the Business Associate shall save a copy of the on-line report. After submission, the Business Associate 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 Business Associate shall submit the US-CERT report by the deadline. The Business Associate shall e-mail updated information as it is obtained, following the instructions at http://www.us-cert.gov/pgp/email.html. The Business Associate 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. Business Associate questions about US-CERT reporting shall be directed to the DHA or Service-Level Privacy Office, not the US-CERT office.

The Business Associate report 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, as applicable, the DHA Privacy Office, the Service-Level Privacy Office, the Contracting Officer (CO) and Contracting Officer's Representative (COR) *[if the Agreement is not a contract, delete these references to the CO and COR]*, and the Business

Associate's DoD 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 Business Associate 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 Business Associate shall proceed and, if appropriate, consolidate separately reported breaches for purposes of Business Associate report updates, beneficiary notification, and mitigation.

When a Breach Report Form initially submitted is incomplete or incorrect due to unavailable information, or when significant developments require an update, the Business Associate 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 Business Associate shall report include, but are not limited to: confirmation on the exact data elements involved, the root cause of the incident, and any mitigation actions to include, sanctions, training, incident containment, follow-up, etc. The Business Associate 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 Business Associate shall provide updates to the same parties as required for the initial Breach Reporting Form. The Business Associate 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 Business Associate is uncertain on how to apply the above requirements, the Business Associate shall consult with the DHA Privacy Office (or the Service-Level Privacy Office, which will consult with the Privacy Office as appropriate) when determinations on applying the above requirements are needed.

(c) Individual Notification Provisions

If the DHA Privacy Office determines that individual notification is required, the Business Associate 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 Business Associate is able to determine the identities (including addresses) of the individuals whose records were impacted.

The Business Associate's proposed notification to be issued to the affected individuals shall be submitted to the parties to which reports are submitted under paragraph V(a) for their review, and for approval by the DHA Privacy Office. Upon request, the Business Associate 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 Business Associate 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 Business Associate'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 Business Associate 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 Business Associate 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.

Business Associates 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 Business Associate 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 Business Associate 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 Business Associate shall so indicate in the initial or updated Breach Report Form. Within the 10 day period, the Business Associate 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 Business Associate shall consult with the DHA Privacy Office, which will determine which media notice is most likely to reach the population not otherwise identified or reached. The Business Associate shall issue a generalized media notice(s) to that population in accordance with Privacy Office approval.

The Business Associate shall, at no cost to the government, bear any costs associated with a breach of PII/PHI that the Business Associate 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 Business Associate shall follow applicable DoD Information Assurance requirements under its Agreement. If at any point the Business Associate finds that a cyber security incident involves a PII/PHI breach (suspected or confirmed), the Business Associate shall immediately initiate the breach response procedures set forthhere. The Business Associate 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.

VI. Termination

(a) Termination. Noncompliance by the Business Associate (or any of its staff, agents, or subcontractors) with any requirement in this BAA may subject the Business Associate to termination under any applicable default or other termination provision of the Agreement.

(b) Effect of Termination.

(1) If the Agreement has records management requirements, the Business Associate shall handle such records in accordance with the records management requirements. If the Agreement does not have records management requirements, the records should be handled in accordance with paragraphs (2) and (3) below. If the Agreement has provisions for transfer of records and PII/PHI to a successor Business Associate, or if DHA gives directions for such transfer, the Business Associate shall handle such records and information in accordance with such Agreement provisions or DHA direction.

(2) If the Agreement does not have records management requirements, except as provided in the following paragraph (3), upon termination of the Agreement, for any reason, the Business Associate shall return or destroy all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity that the Business Associate still maintains in any form. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The

Business Associate shall retain no copies of the PHI.

(3) If the Agreement does not have records management provisions and the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide to the Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Covered Entity and the Business Associate that return or destruction of PHI is infeasible, the Business Associate shall extend the protections of the Agreement 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 Business Associate maintains such PHI.

VII. Miscellaneous

(a) Survival. The obligations of Business Associate under the "Effect of Termination" provision of this BAA shall survive the termination of the Agreement.

(b) Interpretation. Any ambiguity in the Agreement shall be resolved in favor of a meaning that permits the Covered Entity and the Business Associate to comply with the HIPAA Rules and the DoD HIPAA Rules.

_____	_____
[Business Associate]	[MHS Covered Entity component]
_____	_____
Date	Date